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

Digital Asset Depository Nebraska Payment System Risk Examination Manual

Nebraska Department of Banking and Finance

Version 2.0 – July 2023

Table of Contents

1. INTRODUCTION

The Nebraska Department of Banking and Finance ("the Department") Digital Asset Depository Institution ("DD") Payment System Risk ("PSR") Examination Manual (or, "DD PSR Manual" or "Manual") provides guidance to the Department bank examiners for carrying out examinations and supervision of digital asset payment systems and related activities.

Financial institutions accept, collect, and process a variety of payment instruments and participate in clearing and settlement systems. In some cases, financial institutions perform all of these tasks. Financial institutions, acting either in consortiums or independently, remain the core providers to businesses and consumers for most retail payment instruments and services. Federal government-affiliated providers and operators, such as the Federal Reserve Banks (Reserve Banks), also compete with numerous financial institutions and private sector firms in providing various services in support of retail payments.

Recently, a number of new payment instruments have emerged that are largely or wholly electronic. Electronic payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants. Another trend associated with emerging payments is the increased participation of nonbank third parties in retail payment systems and a lengthened transaction chain, which may increase risk in payment processes. Management of retail payments risk is increasingly difficult and requires diligent oversight of third-party service providers.

Additionally, a number of new payment instrument technologies have emerged and may be considered permissible activities for Nebraska financial institutions, including DDs. Such payment systems offer efficiency gains by allowing for rapid and convenient transmission of payment information among system participants, improving both access to collateral and collateral velocity. However, the emergence of a new payment mechanism can also enable the propagation of fraud, money laundering, and operational disruption if sufficient controls are not in place or if data is compromised.

The guidance in this Manual addresses traditional payment systems where applicable to the permissible activities allowed for DDs, in alignment with the FFIEC Retail Payment Systems Examination Handbook, FFIEC Wholesale Payment systems Examination Handbook and Federal Reserve Policy on Payment System Risk.

Additionally, the DD PSR Manual focuses on the emerging risks and considerations presented by digital assets and new payment instruments and is intended to supplement the existing guidance on traditional payment systems.

The DD PSR Manual is divided into four sections:

Payment Systems Overview. The first section of the Manual presents an overview of retail payment systems and wholesale payment systems, grouping payment instruments in various categories, including: Fedwire and the Clearing House Interbank Payments System ("CHIPS"), and other electronic payments.

DD's Role in the Payment System. This section of the Manual provides an overview of the DD's potential role in payment systems, introduces the emerging new payment instruments, and highlights key risks associated with new digital assets payment instruments.

Risk Management. The third section of the Manual describes the risks associated with DD payment systems and instruments, including considerations presented by new digital asset payment instruments using the regulatory risk categories: reputation, strategic, credit, liquidity, settlement, legal/compliance, and operational/transaction risk. This section also presents the risk management practices DDs should implement in order to mitigate the risks described.

Examination Procedures. The fourth section of the Manual provides detailed processes examiners should follow to evaluate the effectiveness of the internal controls and risk management processes implemented by DDs.

1.1. DD Background

On May 26, 2021, Nebraska became the second state to pass a bill authorizing the chartering of digital asset (commonly known as cryptocurrency) depositories ("DDs").[1] LB649, also known as the Nebraska Financial Innovation Act ("NFIA"), became effective on October 1, 2021 and provides guidelines on the charter, operation, supervision and regulation of digital asset depositories. NFIA is the "statutory framework Nebraska has chosen to encourage the creation of Nebraska Digital Asset Depositories, protect digital asset consumers, preserve confidence in Nebraska Financial Institutions, and promote FinTech innovation."[2]

NFIA allows two ways to create a DD:[3]

(1) A business may be organized and apply for a Nebraska Digital Asset Depository Institution Charter (similar to a Bank/Financial Institution organizing and applying for its initial Nebraska Charter); or
(2) A Nebraska Chartered Financial Institution, as defined by the Act, may apply for authority from the Nebraska Director of Banking and Finance ("the Director") to operate a Digital Asset Depository "Department" (an amendment to a Nebraska Bank's/Financial Institution's existing Charter).

The Nebraska Department of Banking and Finance is responsible for enforcing and administering the Act, which includes the drafting of rules, regulations, and other guidance documents for the emerging industry.[4]

Permissible Activities

[1] Neb. Stat. §§ 8-3001 to 8-3031 (LB649, 2021)

[2] The Nebraska Department of Banking and Finance Website.

[3] Neb. Stat. § 8-3004 (LB649, 2021) and Neb. Stat. § 8-3014 (LB649, 2021)

[4] The Nebraska Department of Banking and Finance, "Digital Assets."

Consistent with Nebraska law and subject to the approval of the Director, a DD may operate a (non-lending/non-demand deposit of US dollars) digital asset banking business for digital asset customers, with authority including the following:[5]

- Provide custodial services for digital assets,
- Issue stablecoins and hold reserves for stablecoins at Federal Deposit Insurance Corporation ("FDIC") insured Nebraska Financial Institutions,
- Use independent node verification networks and stablecoins for payment activities,
- Apply to become a member bank of the Federal Reserve,
- Participate in and perform digital asset exchange,
- Participate in and perform staking,
- Facilitate limited digital asset lending and borrowing through exchange networks, and
- Purchase certain debt obligations.

In the context of payment activities, DDs may be permitted to issue and redeem electronic payment instruments and facilitate payment activities. (see *3. DD's Role In the Payment System* for more details). If a Nebraska Chartered Financial Institution applies to operate as a Digital Asset Depository "Department", the Financial Institutions can engage in other traditional payment activities such as demand deposit, among others.

A DD should consult with the Director and seek any necessary approval, before engaging in a substantially new activity or line of business. The activities of a particular DD will be evaluated for their consistency with law and supervisory guidance and safety and soundness, including institution management, earnings, information technology, operational controls, and CFT/AML and OFAC compliance.

2. PAYMENT SYSTEM OVERVIEW

Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Wholesale payments are typically made between businesses. Although there is no definitive division between retail and wholesale payments, retail payment systems generally have higher transaction volumes and lower average dollar values than wholesale payment systems. The following are examples of typical retail payments. These retail payments may involve the use of various retail payment instruments or access devices (e.g., checks, ACH, card, phones, etc.).

Purchase of Goods and Services. Purchase of goods and services can occur at the point-of-sale ("POS") (e.g., in person at a merchant location, through the Internet, or by telephone). These payments include attended POS payment transactions for goods or services, such as with traditional retailers, and unattended payment transactions, as with vending machines. Increasingly, traditional retailers such as grocers and home improvement stores are using unattended payment

[5] Neb. Rev. Stat. § 8-3024 (LB707, 2022)

systems at the POS as well. As technology advances, the consumer can purchase goods and services remotely without physical presence at the POS, such as via the Internet or a telephone/mobile phone. Payment instruments for retail purchases of goods and services have expanded beyond traditional vehicles (i.e., cash, checks, and credit and debit cards) to prepaid cards, contactless debit and credit cards, and other contactless devices such as key fobs, mobile phones. In addition, merchants may convert checks to electronic form at the POS, and use the ACH system for clearing and settlement.

Bill Payment. Consumers may elect to pay (or provide payment instructions for) recurring or nonrecurring bills and invoices via electronic bill payment. A particular biller's periodic recurring invoices can be electronically paid individually or set up to be paid automatically to a payment schedule. In recent years, there has been a growing trend toward payment of recurring and nonrecurring bills using Internet-based bill payment services.

P2P Payments. The vast majority of consumer-to-consumer payments are conducted with checks and cash, with some transactions using electronic P2P payment systems. The expansion of systems that permit customers to conduct P2P payments is anticipated through account-to-account ("A2A") transfers, which use either the ACH or Automated Teller Machine ("ATM") networks for movement of funds.

A2A Payments. With A2A payments, the consumer moves funds from his or her account at a financial institution to the account of another individual or business at the same or a different financial institution. The emerging use of the ATM networks for movement of funds may allow same day availability of funds at a cost far less than traditional wire transfer systems.

Cash Withdrawals and Advances. Consumers use retail payment instruments to obtain cash from merchants or ATMs. For example, consumers can use a credit card to obtain a cash advance through an ATM or an ATM or debit card to withdraw cash from an existing account. Consumers can also use personal identification number ("PIN")-based debit cards to withdraw cash at an ATM or receive cash back at some POS locations.

Retail payment systems continue to evolve with advances in technology. These advances enable financial institutions to develop new products and services, lower the barriers to business entry for smaller institutions, and exploit economies of scale.

In addition to retail payments, a Nebraska-chartered financial institution may engage in large-value wholesale payments such as wire transfers. [6] Wire transfers are usually initiated to facilitate transfers among businesses. There are two primary networks for interbank, or large-value, domestic, funds transfer payment orders. The first, Fedwire® Funds Service, is operated by the Federal Reserve Banks, and is an important participant in providing interbank payment services as well as safekeeping and transfer services for U.S. government and agency securities, and

[6] Note that DDs are not allowed to accept demand deposits.

mortgage-backed securities.[7] Funds Service and the Federal Reserve's National Settlement Service ("NSS") are critical components used in other payment systems' settlement processes. The Clearing House Interbank Payments Company L.L.C. ("CHIP Co.") operates the second, the Clearing House Interbank Payments System.[8] In addition to the Fedwire and CHIPS, the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") provides secure electronic financial messaging services to financial institutions. In contrast to Fedwire and CHIPS, SWIFT is a messaging system for funds transfer instructions, rather than a financial settlement system. In contrast to Fedwire and CHIPS, a SWIFT message may travel directly from a U.S. financial institution to a foreign institution or vice versa. In practice, SWIFT is the primary method for international funds transfer messages.

Note that a digital asset depository established as a separate entity should not accept demand deposits of United States currency or United States currency that may be accessed or withdrawn by check or similar means for payment to third parties.[9] However, if formed as a Digital Asset Depository "Department", the Nebraska-chartered Financial Institution can engage in traditional payment activities described in the sections above. Department examiners should refer to FFIEC Retail Payment Systems Examination Handbook and FFIEC Wholesale Payment Systems Examination Handbook for detailed direction and examination procedures when conducting examinations. This Manual is aimed to focus only on permissible payment activities for DDs.

In accordance with the NFIA, DDs may be permitted to issue and redeem electronic payment instruments and facilitate payment activities. For example, certain stablecoins (e.g., stablecoins) have many of the features of virtual currency but seek to stabilize prices by linking their value to a pool of assets, with the aim of being considered as capable of serving as a means of payment and store of value. More recently, certain institutions, including both non-banks and banks, have started to experiment with the new stablecoin payment network to conduct interbank payment transfers, among others for both retail and wholesale payment transfers.

[7] In addition, Fedwire® is a registered service mark of the Federal Reserve Banks. See http://www.frbservices.org/ for further information on Fedwire Funds and Securities Service, and NSS.

[8] CHIPS is a private multilateral settlement system operated by CHIP Co., a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).

[9] Neb. Rev. Stat. § 8-3005(2)(b) (LB707, 2022)

3. DD's ROLE IN THE PAYMENT SYSTEM

3.1. Stablecoin Payment Network

Technological innovations are transforming the provision of financial services and products. Payment services in particular have seen significant changes through the introduction of new payment methods, instruments, and interfaces.

Asset-backed tokens (sometimes referred to as "stablecoins"), for example, are a new means of payment permitted under the NFIA. An asset-backed token is a type of digital asset whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of one or several fiat currencies, one or several commodities or one or several digital assets, or a combination of such assets. Asset-backed tokens may present in several forms, including stablecoins, electronic money ("e-money") or commercial bank e-money.

Stablecoin: Stablecoin[10] is a type of digital asset with internal mechanisms designed to reduce price volatility.[11] While other digital assets have historically had significant price fluctuations, the relative price stability of some stablecoins facilitates their everyday use as a store of value or as a means for clearance and settlement.

E-Money: The European Central Bank and the Bank of England define e-money as "an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer." [12] When an asset-backed token is pegged to a single fiat currency and represents a direct claim on the issuer by the token holder, it may potentially be defined as e-money. Essentially, e-money is one type of asset-backed tokens, but it carries more stringent requirements in terms of pegging to the underlying asset and redemption rights.

Commercial Bank E-Money: If a form of "e-money" is issued by a commercial bank in the United States and the asset-backed tokens holders directly hold claims against the commercial bank for the high-quality liquid assets functioning as a reserve for the token, this type of asset-backed tokens

---

[10] The Financial Stability Board defines a stablecoin as "as a crypto-asset designed to maintain a stable value relative to another asset (typically a unit of currency or commodity) or a basket of assets. These may be collateralized by fiat currency or commodities or supported by algorithms. The term is used to describe a particular set of crypto-assets with certain design characteristics or stated objectives, but the use of this term should not be construed as any endorsement or legal guarantee of the value or stability of these tokens." See FSB. "Regulatory issues of stablecoins" (18 October 2019).

[11] The NFIA defines stablecoin as a cryptocurrency designed to have a stable value that is backed by a reserve asset. See Neb. Stat. § 8-3003(19) (LB649, 2021)

[12] See the European Central Bank "Definition of Electronic Money". This term has been used in recent legislation. For instance, see Singapore Monetary Authority Singapore. "Consultation on the Payment Services Act 2019: Scope of E-money and Digital Payment Tokens" (23 December 2019), which defines e-money as "denominated in currency", "pegged" to a currency, and is intended to serve as a "medium of exchange." See also the European Commissions, "2009 Directive on Electronic Money", which defines e-money as "a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions."

can be defined as "commercial bank e-money" because the ultimate obligor is the bank that issues the token.

From a legal perspective, commercial bank e-money may be considered an electronic negotiable instrument issued by a bank under UCC Article 3.

Nebraska is mindful of the different terms (e.g., stablecoin, e-money, commercial bank e-money) currently used to describe the various products on the market and recognizes the rapidly evolving applications of such products. For the purpose of this Manual, Nebraska uses the term "stablecoins" to categorically refer to the digital asset used as a means of exchange and that purports to maintain a stable value through an inherent and relative claim on a fully funded reserve of liquid assets.

These forms have different features and regulatory implications, but in general they adopt the same underlying technology and serve as a means of exchange and innovative payment instrument designed to promote more efficient payments and financial inclusion.

The NFIA requires DDs 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 digital asset depository, were DDs to issue its own stablecoins.[13]

Stablecoin Price Stability Models

1. Fiat/Commodity-Collateralized

i. **Single fiat asset-collateralized**: In the single fiat asset-collateralized model, stablecoins are wholly backed by a single fiat currency, such as the U.S. dollar. Such single fiat asset-collateralized token has a fixed redemption value, such as Gemini's "Gemini Dollar" (GUSD[14]), where the token is fully redeemable (or "pegged") for one USD. As noted above, when a stablecoin is pegged to a single fiat currency and represents a direct claim on the issuer by the token holder, it may potentially be defined as e-money. In this model, a central governing entity (or entities) issues the stablecoin and guarantees an asset's redeemability for its collateral "off-chain". The central governing entity (or entities) is required to maintain the stability of the stablecoin's value, meaning these digital assets are typically not fully decentralized.

ii. **Others:** Stablecoins can also be backed by multiple fiat currencies,[15] commodities, or by a basket of fiat currencies or other instruments such as U.S. Treasury securities. Such tokens

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

[14] See Gemini's Gemini Dollar. https://gemini.com/dollar/.

[15] Stablecoins are often associated with central bank digital currency (CBDC); since in principal, both stablecoins and CBDCs should have a (relatively) stable value with respect to a fiat currency. However, as FATF explains: CBDCs "are digital representation of fiat currencies and issued by a national government, they should be differentiated from commercial so-called stablecoin proposals." FATF standards treat commercial stablecoins as a form of virtual assets whereas, "FATF Standards cover and apply to central bank digital currencies similar to any other form of fiat currency issued by a central bank."

may have variable redemption value. Similar to the single fiat asset-collateralized model, in this model, a central governing entity (or entities) issues the stablecoins and guarantees an asset's redeemability for its collateral "off-chain".

2. **Digital Asset-Collateralized** – In the digital asset-collateralized model, stablecoins are collateralized by another digital asset (such as The MakerDao's Dai [DAI] digital asset[16]) or by a basket of digital assets. In the example of Dai, the digital asset is pegged to the dollar but it is collateralized via "smart contracts"[17] to Ether on the Ethereum network (as an ERC-20 token[18]); mechanisms within the smart contract reduce and expand supply of DAI in response to price fluctuations relative to the USD to maintain the asset's price stability. Digital asset-collateralized tokens are typically collateralized "on-chain" through the use of "smart contracts" enabling the model to be completely decentralized.

3. **Non-Collateralized –** In addition to the two models described above, a token may also take the form as non-collateralized tokens (also known as "Seigniorage-style"), which is stabilized through the use of an algorithm that expands and contracts the stablecoin supply similar to how central banks maintain the value of fiat currencies. Non-collateralized tokens have the potential to be completely decentralized. An example of a non-collateralized token is the TerraUSD.[19]

Stablecoin Network Features

Stablecoin networks describe the use of the cryptography and distributed ledger technology to facilitate transfers of value. In general, a stablecoin payment network can be divided into two categories: a private payment network and a public payment network, depending on the network's design and/or access criteria.

- **Private Stablecoin Network:** Private stablecoin networks describe networks where access is limited to entities approved by the network administrator.

  Private stablecoin networks can focus on individuals (retail) and limit access to individuals who have met certain access criteria (such as verification of identity) or legal entities (wholesale) and limit access to an established consortium (such as a group of financial institutions). In private stablecoin networks, access criteria ascertained during, "the on-

[16] See MakerDao's Dai digital assets. https://makerdao.com/en/.

[17] A "smart contract" can be defined as "an automated transaction, or any substantially similar analogue, which is comprised of code, script or programming language that executes the terms of an agreement, and which may include taking custody of and transferring an asset, or issuing executable instructions for these actions, based on the occurrence or nonoccurrence of specified conditions.

[18] Cointelegraph. "ERC-20 is a standard for creating tokens on the Ethereum network" (12 May 2018).

[19] See Terra. https://www.terra.money/.

boarding process may support a 'gatekeeping' role that assists in preventing criminal or illegal trading activity."[20]

Illustrative Example: Private Network (see Figure 1)

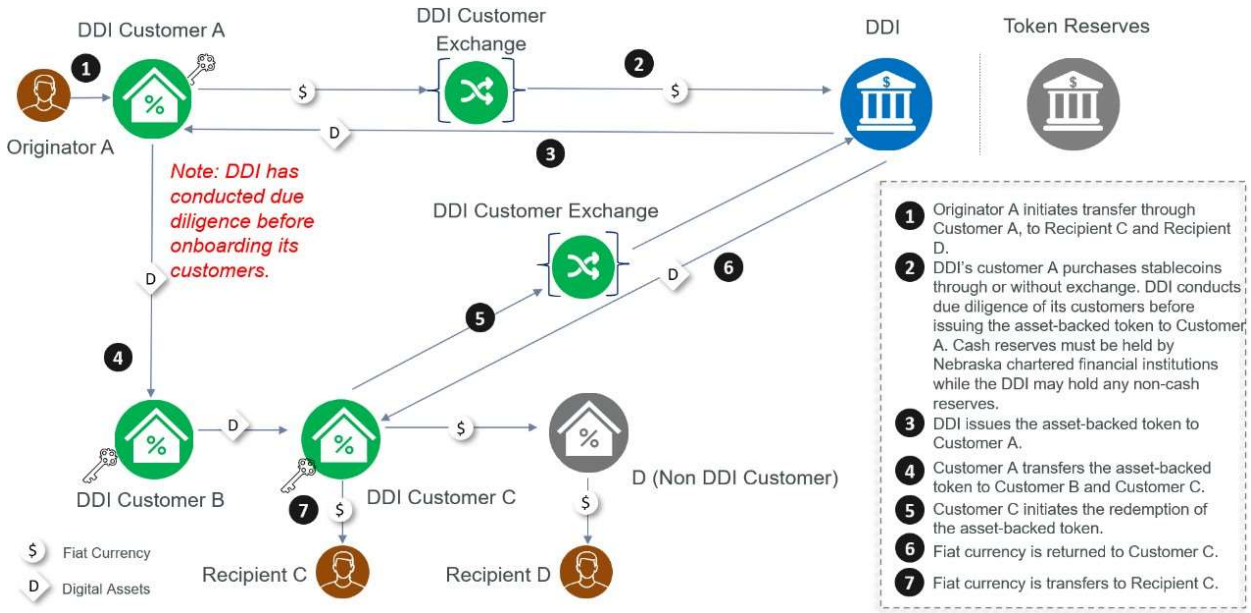

Figure 1

- **Public Stablecoin Network:** Public stablecoin networks describe networks where anyone can access the network and execute transactions. The central authority/issuing and redemption authority still has ability to put in place controls around issuance and redemption of the stablecoin but has limited ability to control who can participate in such network because assets are negotiable and may be traded freely among members of the public.

  Notably certain public (retail) stablecoin networks (such as Tether [USDT] [21]) permit pseudonymous (or potentially anonymous transactions if anonymity-enhancing coins are used) peer-to-peer transactions via non-custodial wallets.[22]

[20] For additional considerations around access rights, see OICV-IOSCO. "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms" (February 2020).

[21] See https://tether.to/.

[22] See https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. Also called a non-custodial wallet. A wallet that is directly maintained by the wallet owner, as opposed to being custodied by a third-party. The wallet owner holds the wallet's private key in this case.

Illustrative Example: Public Network (see Figure 2)

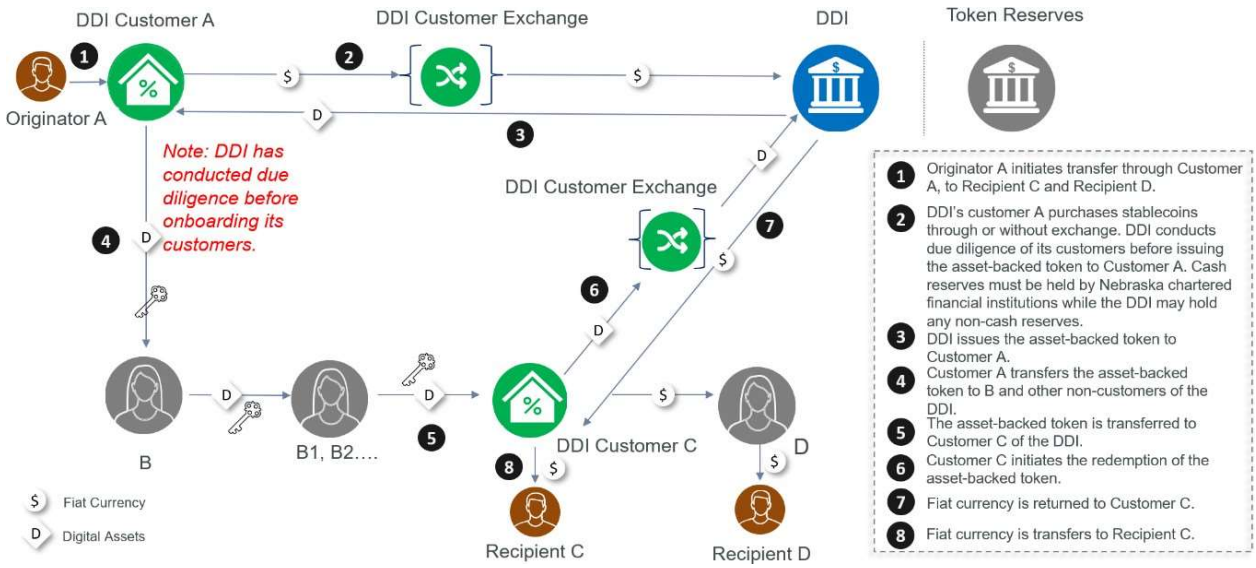

Figure 2

Role of a DD in a Stablecoin Payment Network

A DD may engage in different activities in a stablecoin payment network. In general, the activities can be summarized into four major activities:

1. **Governance of the Stablecoin Arrangement** – DDs involved in this activity would establish rules that govern the stablecoin arrangement. Rules may include, but are not limited to, setting access criteria, defining roles and responsibilities for different network participants, clarifying the ownership of the assets, or providing documented guidance on risk management principles.

2. **Issuance, Redemption and Stabilization of the Value of the Stablecoins –** As issuers of stablecoins, DDs are responsible for issuing, creating, and destroying stablecoins in accordance with its stabilization mechanisms. In addition, even though DDs are not directly managing the underlying cash reserves of the stablecoins, they are responsible for providing oversights on the selection of institutions, and the monitoring of the key decisions in managing the reserves, including designing the composition of the underlying reserve, maintaining and managing the reserve in a safe and sound manner, ensuring the issuance and redemption processes are efficient and effective, among other factors. For non-US dollar fiat reserves (e.g., Treasuries, agency bonds, etc.), the DD will be responsible for selecting the assets, managing payments and redemptions (or selecting third-party custodians for these functions) and ensuring that there are no quality or price concerns that would negatively impact overall reserve adequacy.

3. **Transfer of Stablecoins** – DDs may also be responsible for overseeing the transfer of stablecoins, including ensuring the operation of the underlying infrastructure is smooth and

efficient in coordination of third-party vendors, as well as providing clear rules for transaction validation and settlement finality.

4. **Interaction with Stablecoin Users for Storing and Exchanging Coins** – Lastly, the interaction with users typically occurs through "devices or applications that operate as 'wallets', which store the private keys providing access to stablecoins, as well as applications that enable the exchange of coins against fiat currencies or other crypto-assets."[23] DDs may directly provide such services or may work with third-party service providers to provide such services.

Given the novelty of permissible activities associated with stablecoin networks and DDs' role in administering and operating the stablecoin payment network, the Department expands upon certain federal standards with respect to its examination approach, as well as other international standards around the payment systems infrastructure.

Where financial market infrastructures are involved, for instance, expectations are highest for infrastructures that play an important role in the financial system. These expectations include risk provisioning in accordance with the *Principles for Financial Market Infrastructures* ("PFMI") established by the Committee on Payment and Settlement Systems ("CPSS") and International Organization of Securities Commissions ("IOSCO"). Among other things, the principles stipulate that legal, liquidity and credit risk be appropriately mitigated. Operational risk – cyber risk in particular – should also be fully taken into account. In a similar vein, the Department has identified the high-level risk factors for stablecoins summarized below. Department examiners should refer to *4. Risk Management* for detailed descriptions and mitigation controls.

Risk Factors

Liquidity Risk. Liquidity risk is the current and potential risk to earnings or capital arising from a financial institution's inability to meet its obligations when they come due without incurring unacceptable losses. DDs need to consider the liquidity risks related to issuance and redemption of the stablecoins. For example, the quality of the collateral (cash vs other assets) and availability of the stablecoins' reserve (segregated account vs omnibus account vs single account) determine the robustness of the liquidity risk control by DDs. The type of assets that back a stablecoin may have different liquidity risk implications, as do significant changes in the composition of reserve assets and the transparency of disclosing such information to customers.

Additionally, how DDs cope with large-scale redemption under stress scenarios also have direct implications on the liquidity risk. The PFMI specifically states that an FMI should "maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the

[23] Financial Stability Board. "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" (13 October 2020).

participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme[,] but plausible market conditions."

Credit Risk. Credit risk arises when a party cannot or will not settle an obligation for full value. This applies to DDs when they engage in traditional payment activities such as ACH or Wire, for example. The Nebraska statutes limit the credit risk that DDs can assume by requiring 100% stablecoin reserve backing of fiat deposits or defined liquid assets.[24] However, certain operations of a stablecoin payment network may result in incidental credit risk. For a stablecoin payment network, DDs need to consider both issuance/redemption activities as well as payment transfer activities to identify potential credit risks and execute proper controls accordingly. For example, DDs should have processes to identify sources of credit risk and have monitoring tools in place to ensure the digital asset reserve requirements meet the requirements stipulated in Nebraska statutes. DDs should also establish explicit rules and procedures to address credit losses resulting from counterparty default.[25]

Operational Risk. Similar to traditional payment systems, stablecoin payment networks pose a range of operational risks depending on the design and access criteria of the network. In particular, the maintenance and operational resilience of the underlying infrastructure as well as the governance of the stablecoin arrangement determine the DD's ability to monitor and mitigate the operational risks. For example, the clarity of the roles and responsibilities of the stablecoin arrangement, including setting and enforcing the rules on establishing the stablecoin's value and the functioning of the infrastructure may heavily impact the users' confidence. An ineffective third-party risk management framework may also negatively impact the operation of the stablecoin payment network. Having a strong operational resilience strategy is considered essential for DDs. For example, DDs should have a robust business continuity program in place to formalize its operational resilience strategy, given the need for stablecoin payment networks to maintain a high level of availability.

Compliance Risk. If not effectively regulated and supervised, digital assets, including stablecoins, may create new opportunities for money laundering, terrorist financing and other illicit financing activities. DDs need to understand its regulatory compliance obligations, including, for example, AML/CFT and OFAC requirements as outlined in the *4.4 Stablecoin Networks – Overview* section of the DD AML/CFT and OFAC Examination Manual.

Governance Risk. In addition to DDs issuing stablecoins, the arrangement may also include other participants on which DDs' customers rely to store private keys and exchange stablecoins. The failure of such participants may create various levels of disruption to the normal function of the arrangement. The vulnerability to shocks also depends on the operational resilience arrangements of those participants, including "stand-in and fallback arrangements that ensure continuity of service to users, and on the continued liquidity of the secondary market for coins."[26] The

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

[25] CPSS and IOSCO. "Principles for Financial Market Infrastructures" (2012)

[26] Financial Stability Board. "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" (23 October 2020)

governance of the stablecoin arrangement is therefore essential to ensure a shared understanding of the compliance and controls taken by each participant.

Others. Other relevant risk factors include legal risk, reputation risk, and strategic risk, among others. DDs should establish an appropriate risk management process that identifies, measures, monitors, and limits such risks. Refer to *4. Risk Management* for detailed information.

4. RISK MANAGEMENT

4.1. Federal Reserve Master Account Guidance and Payment System Risk Policy

Even though the DD is not allowed to establish fiat-based demand deposit accounts, under the Nebraska law, the DD is eligible to apply for a master account from the Federal Reserve System to clear payments and access other Federal Reserve services, subject to prudential standards relating to payment system risk and other applicable factors.[27] International standards explicitly call on payment systems to settle in central bank money when possible and where that is not possible, to settle in commercial bank money and to strictly limit any credit and liquidity risk of the instrument being transferred and settled.[28] A DD may only maintain a single Master Account with its Administrative Reserve Bank[29] unless a specific exception applies as described in Section 2.3 of the *Federal Reserve Banks Operating Circular 1*.[30]

Subject to Federal Reserve approval[31] and consistent with Nebraska law and rules, in order to obtain or retain access to a Federal Reserve account or a Federal Reserve financial service, a DD must demonstrate that it satisfies factors that allow the Federal Reserve to assess, manage and mitigate the risks that arise in connection with its provision of accounts or services[32]. In particular, such factors include but may not be limited to the following,[33] the requirements of which are described in further detail in following sections:

- **Applicable Law**: A DD must at a minimum, and at all times, be eligible under all applicable law to access each Federal Reserve account or a Federal Reserve financial service it uses.

- **Effective Risk Management Framework**: A DD must have an effective risk management framework that includes policies, procedures, systems and qualified staff to manage applicable risks. The framework should be further supported by internal testing and internal audit reviews,

---

[27] Neb. Rev. Stat. 8-3005(1)(vi) (LB707, 2022)

[28] *PFMI*, Principle 9, "An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money."

[29] "Administrative Reserve Bank" means the Reserve Bank in the Federal Reserve District in which the Financial Institution is located. See Federal Reserve Banks Operating Circular 1 (2013).

[30] Federal Reserve Banks Operating Circular 1 (2013)

[31] Federal Reserve System. "Guidelines for Evaluating Account and Service Requests" (1 March 2022)

[32] The Federal Reserve Board is currently assessing the tiered application requirement. Detailed requirements may be subject to changes upon finalization of the tiered application guidance.

[33] Federal Reserve Bank of New York. "Account and Financial Service Handbook" (25 February 2020)

as well as be subject to oversight by a board of directors, in addition to oversight by state and/or federal banking supervisor(s).[34]

- **Compliance Risk Management**: A DD must have a risk-based compliance framework in place that is designed to achieve compliance with all applicable U.S. laws and regulations. A DD must be able to demonstrate that its AML/CFT and OFAC compliance programs adequately identify, assess, respond to, communicate, escalate, and monitor compliance risks associated with money-laundering, terrorist financing, and U.S. economic sanctions, respectively.[35] The DD's programs must be flexible to account for potential risks posed by its customers, intermediaries, transactions, products and services, and geographic locations. In addition, the DD's programs must include methods to monitor, analyze, and report suspicious activity and address such risks when identified.

- **Operational Risk Management**: A DD must have an operational risk framework in place designed to strengthen operational resiliency against events that may impair activities associated with processes, people, and systems. The operational risk framework must consider internal and external factors, including operational risk inherent in a DD's business model, risks that might arise in connection with its use of any Federal Reserve account or Federal Reserve financial service, and cyber-related risks. The operational risk framework should include at minimum a business continuity plan and policies/procedures for identifying risks that external parties may pose to sound operations, including interdependencies with affiliates, service providers, and others. A DD must have a framework in place to support compliance with electronic access requirements, including security measures, set forth in *Federal Reserve Banks Operating Circular 5: Electronic Access*. In addition, DDs should establish an appropriate risk-based third-party risk management process, tailored to its unique profile and its third-party relationships, including relationships with affiliates.

- **Credit Risk Management**: A DD must not pose undue credit risk to the Federal Reserve System. In addition, a DD that has a Federal Reserve account or access to Federal Reserve financial services is subject to the Federal Reserve Policy on Payment System Risk (the "PSR Policy"),[36] which may require the pledging of collateral and/or special credit risk management monitoring in conjunction with the use of Federal Reserve financial services.

- **Capital and Liquidity Risk Management**: A DD must be in sound financial conditions and ensure adequate capital on an ongoing basis. In particular, a DD should evaluate the sufficiency of capital in both normal scenario and stress scenarios. A DD should also have in place liquidity risk management processes to maintain liquid resources sufficient to meet obligations to the Reserve Bank.

---

[34] Federal Reserve System. "Guidelines for Evaluating Account and Service Requests" (1 March 2022)

[35] Refer to the DD BSA/AML and OFAC Examination Manual for more details.

As part of the Master Account application, the Administrative Reserve Bank may require DDs to submit, among others, business plans[37] that are consistent with the Business Plan Guidelines set forth in the Interagency Charter and Federal Deposit Insurance Application (the "Interagency Application")[38] to assess potential credit risk. Due to the de novo nature of DDs and the heightened risks of the business activities DDs conduct, the Administrative Reserve Bank may expect DDs to review and comply with *SR 20-16: Supervision of De Novo State Member Banks* released by the Board of Governors of the Federal Reserve System. In particular, the Federal Reserve explains that "a de novo should maintain capital ratios commensurate with its risk profile and, generally, well in excess of regulatory minimums." Among other requirements, de novo banks are generally required to maintain a tier 1 leverage ratio of at least 8 percent for the first three years of their existence.[39] Lastly, under the Federal Reserve's proposed *Guidelines for Evaluating Account and Services Requests*, DDs may be categorized as Tier 3 candidates (i.e., eligible institutions that are not federally insured and that are not subject to federal prudential supervision at the institution and holding company level) and thus would be subject to the strictest level of review.[40]

The Federal Reserve Board has developed the PSR Policy to address risks that payments and securities settlement systems present to the financial system and to the Reserve Banks. The Reserve Banks are exposed to credit risk when they process wholesale and retail payments for financial institutions holding reserve accounts, just as financial institutions assume credit risk when offering retail payments to their customers. Part of the Federal Reserve's PSR Policy seeks to control and reduce credit risk to the Reserve Banks by controlling financial institutions' use of Federal Reserve daylight overdrafts.

According to the *Federal Reserve Banks Operating Circular 1*, an account holder of the Master Account does not have a right to incur an overnight draft in its account. An account holder may incur daylight overdrafts in its account only to the extent permitted by its Administrative Reserve Bank.

A daylight overdraft occurs when there are insufficient funds in a DD's Federal Reserve account to cover the institution's payment activity, such as outgoing Fedwire® funds transfers or ACH credit originations, as outgoing payments are posted during the day.

To control daylight overdrafts, the PSR Policy establishes limits, or net debit caps, on the amount of Reserve Bank daylight credit that a depository institution may use during a single day and over a two-week reserve maintenance period. These limits are determined jointly through assessments

---

[37] Federal Reserve Bank of New York. "Account and Financial Service Handbook" (25 February 2020)

[38] https://www.fdic.gov/formsdocuments/interagencycharter-insuranceapplication.pdf.

[39] Board of the Governors of the Federal Reserve System. "SR 20-16: Supervision of De Novo State Member Banks" (24 June 2020)

[40] Federal Reserve System. "Guidelines for Evaluating Account and Service Requests" (1 March 2022)

by the depository institution and its Reserve Bank. The limits reflect the overall financial condition and operational capacity of each institution using Reserve Bank payment services.

DDs may be monitored on an ex-post (i.e., end of day) or real-time basis. Under the Federal Reserve's ex post monitoring procedures, a DD with a daylight overdraft in excess of its maximum daylight overdraft capacity or net debit cap may be contacted by its Reserve Bank. The Reserve Bank may counsel the DD and discuss ways to reduce its excessive use of intraday credit. Each Reserve Bank retains the right to protect its risk exposure from individual institutions by unilaterally reducing net debit caps, imposing collateralization or clearing balance requirements, rejecting or delaying certain transactions, or, in extreme cases, taking the institution off-line or prohibiting it from using Fedwire. In addition, the Reserve Banks assess fees for daylight overdrafts above a certain deductible amount. [41] A Reserve Bank will monitor an institution's position in real time when the Reserve Bank believes that it faces excessive risk exposure, for example, from institutions with chronic overdrafts in excess of what the Reserve Bank determines is prudent. In addition, the Reserve Bank will reject or delay certain transactions that would exceed the institution's maximum daylight overdraft capacity or net debit caps, and take other prudential action, including requiring collateral.

Subject to Federal Reserve approval, DDs may also serve as a correspondent to a respondent if both parties provide the respondent's Administrative Reserve Bank with a properly executed *Transaction and Service Fee Settlement Authorization Form* to instruct the Administrative Reserve Bank of the respondent and the correspondent to settle some or all of the respondent's transactions in the correspondent's Master Account. However, the *Federal Reserve Banks Operating Circular 1* specifically notes that "Custodial Inventory Program transactions, Fed Funds check and Fedwire Funds and Securities transactions may not be settled in a Correspondent's account." [42] Such services must settle in the financial institution's own Master Account.

The DD's board of directors is responsible for PSR Policy compliance and should ensure that management establishes sound internal operating practices, including compliance with applicable banking laws, and carefully manages retail payment system-related financial risks. At a minimum, the DD's board of directors and senior management should:

- Understand the financial institution's practices and controls regarding the risks of processing transactions for both its own account and the accounts of its customers and respondents;

- Manage its Federal Reserve account effectively and use daylight credit prudently in accordance with the PSR Policy;

[41] For more details, see https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

[42] Federal Reserve Banks Operating Circular 1 (2013).

- Establish prudent limits on the daylight overdraft or net debit position in its Reserve Bank reserve account and any private sector clearing and settlement system; and

- Review periodically the institution's daylight overdraft activity to ensure the institution operates within the established guidelines.

For each payment instrument or mechanism employed by DDs, the Department expands upon the existing PSR Policy to include additional risk factors for examiners to consider as detailed in the following sections. Some heightened standards for DDs include:

- Governance arrangements that are clear and transparent and promote the safety and efficiency of the instrument or mechanism, and support the stability of the broader financial system, as needed.

- Effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the DDs can take timely action to contain losses and liquidity pressure and continue to meet its obligations.

- Objective and risk-based criteria for network participation, which permit fair and open access.

- Processes to identify, monitor and manage risks before entering into payment network agreement with other payment networks, or third-party vendors.

4.2. Strategic Risk

Strategic risk is associated with the DD's mission and future business plans. This risk category includes plans for entering new business lines, expanding existing services through mergers and acquisitions, and enhancing infrastructure (e.g., physical plant and equipment, IT, and networking). For DDs specifically, the evolving technology and solutions around digital assets demands integration of payment strategies into the DD's overall strategic planning processes. DDs also compete with innovative nonbank entities as well as other banks to provide retail or wholesale payment services. As such, competition places pressure on DDs to protect profitability through the development of new products and services while managing additional marketing, research, and development costs.

Strategic plans that include significant market expansion or the addition of new products and services may expose DDs to increased risks. For example, the design of a payment instrument and network development may increase DDs' potential risk given the inherent risks associated with new activities. Business plans for specific products and services should demonstrate that management has assessed the risks and documented relevant controls in the DDs' policies and procedures to mitigate them. Such plans should address the DD's capability to provide the service. Innovative products and services are emerging quickly and early stages of market introduction may expose DDs to undefined and unanticipated risks. In addition, as new payment instruments may have global reach, the potential jurisdictions DDs operate in present different risk implications, especially with regard to legal risk.

To mitigate strategic risk, management should have a strategic planning process that addresses its payment business goals and objectives, including supporting IT components. Because the operations of DDs are increasingly reliant upon third-party service providers for payment system products and services, the strategic plan should also address comprehensive vendor management.

4.3. Reputation Risk

Reputation risk occurs when negative publicity regarding a DD's business practices leads to a loss of revenue or litigation. For example, stablecoin payment network design mechanisms and price stabilization models vary, and the price of a stablecoin may be subject to fluctuations.[43] Customers of DDs will be willing to hold the stablecoin only if they are convinced of its reliability and security.

DDs are responsible for risks associated with the activities of third-party service providers with which they contract. Deficiencies in security and privacy policies that result in the release of customer information by a service provider can damage the reputation of client financial institutions. Operational failures could significantly impact a DD's reputation if systems are disrupted for extended periods. Management oversight of third-party service providers is a critical component of reputation risk management. DDs should establish an appropriate risk-based third-party risk management process, tailored to its unique profile and its third-party relationships, including relationships with affiliates.

4.4. Credit Risk

Credit risk arises when a party will not settle an obligation for full value. Each traditional payment instrument (e.g., ACH, debit card, wire) has a specific settlement process and underlying technology that would incur credit risk to a different degree as outlined in *The FFIEC Retail Payment Systems IT Examination Handbook and The FFIEC Wholesale Payment Systems IT Examination Handbook*.

Aside from the credit risks originating from traditional payment instruments in both retail and wholesale payment systems, for DDs, the stablecoin payment network, as a new payment instrument, also presents unique challenges to mitigate credit risks.

Stablecoin Issuance and Redemption

The design of a stablecoin payment network will define how stablecoins will be issued (i.e., the generation of new individual stablecoins into the network) as well as how stablecoins can be redeemed (how they can be exchanged for the underlying collateral, as applicable). Issuance and redemption will be dependent on the price stability model of the stablecoins.

[43] See "MakerDao Users Sue Stablecoin Issuer Following 'Black Thursday' Losses" for a historic case study (April 2020).

Credit Risk Factors

The stablecoin price stabilization model described in *3.1. Stablecoin Payment Network* section of the Manual directly determines the potential credit risk factors DDs may undertake:

- Collateralization Mechanism: Whether the stablecoin is backed with off-chain collateral (e.g., commercial bank money; central bank money) or on-chain collateral (e.g., digital assets), directly determines DDs' potential credit risk exposure. Off-chain models backed with fiat currency face credit risk if the collateral held in reserve is less than the full reserve backed for the issuance. Nebraska law does not permit a DD to maintain less than 100% backing of any issued payment instrument. The on-chain collateralization model relies on the price stability of the underlying digital assets. Despite the fact that most on-chain collateralization models ensure a certain degree of "overbacking" - the amount of collateral is structured in a way that the value of reserves is larger than the value of the outstanding stablecoins - the underlying collateral still faces the risk of being lost due to technical issues or smart contract failures. The algorithm model does not have underlying collateral as reserves but faces the key challenge of demonstrating that the algorithm can accurately respond to changing market forces and cannot be manipulated. Similar to the on-chain collateralization model, the algorithm model may also face technical failure, causing the loss of tokens. Given the risks listed above, Nebraska only permits stablecoins backed by fiat currencies and highly liquid debt securities (treasuries, agencies, etc.).[44]

- Off-Chain Collateral Location and Availability: Among the models discussed above, the off-chain collateral model (particularly the single fiat asset-collateralized model) may have less credit risk exposure due to the stability of the underlying collateral, if managed appropriately. If the collateral is in the form of liquid deposits held with commercial banks, there remains an inherent credit risk dependent on the safety and soundness of the associated commercial bank. If the collateral is backed with central bank money, the credit risk would be greatly mitigated, although it would not eliminate all credit risk stemming from the DD itself if the issuer is insolvent upon redemption.[45]

Payment Transfers Among Network Participants

In addition to potential credit risk exposures during the stablecoins issuance and redemption stage, the DD is also responsible for identifying potential credit risk exposures as the stablecoin further circulates within the network.

Credit Risk Factors

- Contract Risk: As a large number of stablecoins models are built on smart contacts, stablecoin payment networks are subject to a loss or price fluctuation due to a smart contract bug or

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

[45] Refer to the DD Supervision Handbook for more information related to resolution planning.

failure. For example, certain stablecoins may live within smart contracts protocols like Ethereum or Stellar, and there is a risk the algorithm which keeps the currency stable fails or is manipulated by a third-party. Updates to the network can have an impact on previous smart contracts, which could cause significant disruption to the existing operation. As such, the Department require that a stablecoin will be backed by a reserve of a single asset.

- Subcustodians: A DD is always required to act as the legal custodian of stablecoin. A DD may partner with another custody firm or its affiliates under appropriate circumstances. In such case, the DD faces subcustodian operational, IT, and credit risk, among others. If such a partnership occurs, it is crucial for DDs to understand the controls and processes in place in the subcustodian. Refer to the DD Custody and Fiduciary Examination Manual for more information.

Risk Mitigation:

DDs should measure, monitor, and manage its credit exposures to network participants and those arising from its issuance, redemption, payment, clearing and settlement processes. Key considerations include:

- **Governance.** DD should have a robust framework to manage its credit exposures to its participants and credit risks arising from its payment, clearing, and settlement processes. Key processes need to be in place to identify sources of credit risk, measure and monitor the credit risk exposures. Additionally, explicit rules and procedures are required to address credit losses from any potential default.[46]

- **Ensure Full Reserve of Collateral.** At minimum, DDs should have proper monitoring and reporting in place to ensure the reserve is indeed 100% backed and have sufficient transparency to allow regulators and the public to have full confidence in the obligations issued by the DDs.[47] DDs should also have in place proper auditing procedures to conduct periodic review by auditors or external third parties to avoid potential fraud. Refer to *4.5 Liquidity Risk* for more details.

- **Ability to Determine the Access Criteria for Network Participants.** DDs should have objective and risk-based criteria for network participants when DDs act as stablecoin issuers. At a minimum, DDs should have the ability to determine the access criteria for participating in the payment network and have processes in place to monitor, identify, and block/freeze illicit activities. For example, stablecoins that allow for peer-to-peer transfers reduce the ability to conduct appropriate transaction monitoring. Stablecoin payment networks should be supported by blockchain digital asset analytics to facilitate the identification of unusual activities. See

[46] CPSS and IOSCO. "Principles for Financial Market Infrastructures" (2012)

[47] See "Attorney General James Announced Court Order Against "Crypto" Currency Company Under Investigation for Fraud" for historic case study (April 2019).

also *3.6 Digital Asset Analytics* section in the DD AML/CFT and OFAC Examination Manual for more information.

- **Subcustodian Relationship.** In circumstances where the DD partners with a subcustodian, the DD needs to clearly identify the subcustodian risk associated with such partnerships and have in place procedures and appropriate controls to ensure the safety and soundness of the relevant activities conducted by its partners. It should provide appropriate disclosures regarding the custody of underlying reserves for the stablecoin holders. Refer to the DD Custody and Fiduciary Examination Manual for more information.

4.5. Liquidity Risk

Liquidity risk is the current and potential risk to earnings or capital arising from a financial institution's or DDs inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity risk related to payment systems is the risk that the financial institution cannot settle an obligation for full value when it is due but rather at some unspecified time in the future. Liquidity problems can result in opportunity costs, defaults on other obligations, and costs associated with obtaining the funds from an alternative source for possibly extended periods of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period.

Stablecoin payment networks particularly should consider the liquidity risks related to issuance and redemption of tokens.

Underlying Reserve Liquidity. Depending on the liquidity of the underlying assets that secure stablecoin issuance and redemption, the stablecoin payment network may incur various levels of liquidity risks. If the underlying assets are highly liquid, the DD will have sufficient funds to conduct the transaction, limiting the liquidity risk. If the underlying reserve consists of medium or long-term investment products, DDs may face the risk of not being able to settle the obligation for full value upon request. However, the liquidity of the underlying assets should also be considered in tandem with the price volatility of the asset when evaluating its sound and safeness, as they may be contradictory in certain cases.

Account Segregation. A DD is always required to maintain the stablecoin reserves in a FDIC-insured financial institution which has a main-chartered office in Nebraska, any branch thereof in this state, or any branch of the financial institution which maintained a main-chartered office in this state prior to becoming a branch of such financial institution that serve as reserves for stablecoins. DDs may face potential operational and credit risks from the selected financial institutions that host the reserves. Therefore, it is crucial for DDs to understand the financial institution’s controls and processes and provide ongoing monitoring to ensure the reserves are maintained and managed in compliance with the DDs requirement. For example, DDs should fully understand the account structure of stablecoin reserves. If the reserve is kept in a Federal Reserve Master Account, due to the fungible nature of the account, the selected financial institutions may face challenges in separating the reserve from the operational fund of the bank

and should mitigate these risks with strong, appropriate controls.[48] If the reserve is managed by the financial institution in another account structure, DDs should expect the selected financial institutions to clarify account segregation options and requirements and evaluate if appropriate monitoring is in place to ensure the dedicated reserve assets remain safe and sound.

Settlement Mechanism. Liquidity risks could exist depending on the settlement mechanism. Generally speaking, the settlement usually occurs through two major models: real-time gross settlement ("RTGS") such as the FedWire system used by the Federal Reserve in the United States, or TARGET2 used by the European Central Bank. RTGS settles the transactions real-time within set operating hours or 24/7 depending on the design. The other model is deferred settlement payment, which normally functions within a set operating hour and settles the transactions on a net basis. The deferred settlement payment usually implicates a settlement lag. Both settlement mechanisms may incur liquidity risk related to issuance and redemption of tokens. For example, if the token arrangement operating hours do not fully overlap with the availability and operating hours of connected infrastructures, DDs may face liquidity risks. In addition, the stablecoin payment systems are funded using account-based deposits held by the payer with the settlement institution or intraday credit extended by that settlement institution. In the absence of intraday credit, if the available intraday balance in the payers' account is insufficient to execute its payments, this could also result in liquidity risk in the payment system.

Risk Mitigation

DDs need to have a robust framework to manage liquidity risks from its participants, nostro agents, custodian banks, liquidity providers, or other entities, and regularly assess its design and operations to manage liquidity risk in the system. In the context of stablecoin payment network, Department examiners should particularly evaluate the following liquidity risk controls of the DDs:

Reserve Management and Oversight. Based on the NFIA, DDs must select a separate FDIC-insured financial institution in which to deposit the asset-backed fiat-based token reserves[49]. Even though DDs are not directly responsible for maintaining the reserves, DDs must apply appropriate oversight of the reserve management process to ensure sufficient understanding of the reserve structure and disclosure terms. As part of the examination, Department examiners should evaluate the following key elements when reviewing the stablecoin reserve management.

- **Structure of the Reserve.** The structure of the stablecoin reserve must be intentionally designed to mitigate threats and minimize risks. If the reserve is not comprised of fiat currency, Department examiners should particularly assess whether all of the underlying investments are appropriately liquid short-term (up to three months' remaining maturity)

[48] See "OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves" Interpretive Letter 1172 (October 2020)

[49] For Digital Asset Depository Department established under the existing FDIC-insured Financial Institution, the Financial Institution is eligible to hold the fiat-based reserves on deposit.

with very low credit risk (e.g., A+ rating from S&P and A1 from Moody's, or higher) and that those securities trade in highly liquid secondary markets. Per *PFMI* Principle 7, even if a DD does not have access to routine central bank credit, it should still take account of what collateral typically accepted by the relevant central bank, as such assets may be more likely to be liquid in stressed circumstances. A DD should not assume the availability of emergency central bank credit as a part of its liquidity plan.[50] Department examiners should evaluate and review the investment policies of the underlying reserve and confirm that all opportunities and risks from the management of the underlying assets, be they in the form of profits or losses, from interest, fluctuations in the value of financial instruments, counterparty or operational risks, must be borne by the issuer of the token, the DD.[51]

- **Reserve Oversight.** DDs should have a process in place to monitor how stablecoins reserves are managed by the third-party (i.e., FDIC-insured financial institution) to ensure the reserve is managed properly. In particular, DDs should understand the following from the selected financial institutions:

    - Whether the participating financial institution has effective operational and analytical tools to identify, measure and monitor the settlement and funding flows on an ongoing and timely basis.[52]

    - Whether the participating financial institution segregates the reserves from the other operating funds of the financial institution and adopts strict procedures to monitor and report the daily status of the reserve.

    - Whether the participating financial institution conducts proper due diligence on the customers before accepting the stablecoin reserves, including proper name screening and customer due diligence.

    - Whether the participating financial institution and DD have the operational capabilities to daily monitor the level of liquid assets that it holds.

    - Whether the financial institution and or DD can determine the value of its available liquid assets, taking into account the appropriate haircuts on these assets.

---

[50] *PFMI*, Principle 7, "An FMI may supplement its qualifying liquid resources with other forms of liquid resources. If the FMI does so, then these liquid resources should be in the form of assets that are likely to be saleable or acceptable as collateral for lines of credit, swaps, or repos on an ad hoc basis following a default, even if this cannot be reliably prearranged or guaranteed in extreme market conditions. Even if an FMI does not have access to routine central bank credit, it should still take account of what collateral is typically accepted by the relevant central bank, as such assets may be more likely to be liquid in stressed circumstances. An FMI should not assume the availability of emergency central bank credit as a part of its liquidity plan."

[51] See Swiss Financial Market Supervisory Authority. "Supplement to the Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs)" (11 September 2019).

[52] *PFMI*, Principle 7

- Whether the financial institution and DD can conduct constant monitoring of the on-balance sheet liquidity position, reconciliation, monitoring and reporting of the account books.

- Whether the financial institution and DD has engaged third party firms to conduct auditing of its books and records on a periodic basis to ensure the reserve held by the financial institution is always equal to or greater than the number of outstanding stablecoins issued.

- Whether DD publishes a report on the reserves held by the stablecoin issuer audited by a third-party every 30 days.

Department examiners should have access to the current composition of the reserve and the current market value of the assets on a daily basis and on an as-needed basis. This can be in the form of a periodic report shared with Department examiners.

Capital, Liquidity, and Contingency Planning. Despite the highly liquid nature of the underlying assets, DDs could still incur losses due to significant changes to interest rates or extreme economic conditions. Department examiners should evaluate the DD's capital position to ensure it maintains an appropriately sized and loss-absorbing capital buffer to protect against potential losses from the credit market, and operational risks of the stablecoin payment network. The Department has the power to increase or decrease the amount of required capital on the basis of an evaluation of the risk assessment mechanism of the DD, the quality and volatility of the assets in the reserve backing the stablecoins or the aggregated value and number of total stablecoins.

Department examiners should also evaluate a DD's policies and procedures regarding the frequency and requirements for conducting stress testing of liquidity resources,[53] and whether the DDs has in place rules and procedures to enable it to effect same-day, intraday, and multiday settlement of payment obligations on time following any individual or combined default among its participants.[54] These rules and procedures should address unforeseen and potentially uncovered liquidity shortfalls and should aim to avoid unwinding, revoking, or delaying the same-day settlement of payment obligations. These rules and procedures should also indicate the DD's process to replenish liquidity resources it may employ during a stress scenario, so that it can continue to operate in a safe and sound manner.

In preparations for stress scenarios that could result in a run or otherwise threaten the safety of the payment system, Department examiners should also review the DD's recovery and resolution plan regarding redemption rules (e.g., redemption stays or early redemption haircuts) to evaluate

[53] See more details on liquidity stress testing on Pg. 68 of the *PFMI*, Principle 7. Also see Board of the Governors of the Federal Reserve System. "SR 20-16: Supervision of De Novo State Member Banks" (24 June 2020).

[54] *PFMI*, Principle 7

whether the controls in place are able to slow the speed of a run on the reserve assets were such an extreme case to occur.

4.6. Legal (Compliance) Risk

Legal risk arises from failure to comply with statutory or regulatory obligations. It can result from a DD's failure to comply with the bylaws and contractual agreements established with the bankcard networks, clearing houses, and other counterparties with which it participates in processing, clearing, and settling retail payment transactions. Legal risk also arises if the rights and obligations of parties involved in a payment are subject to considerable uncertainty; for example, if the rights of the parties are not clear when a payment participant declares bankruptcy or if a court interprets an applicable law in an unexpected way. In addition, legal risk can occur when customer agreements or contracts do not clearly establish the roles, responsibilities, governing regulations or guidelines, and dispute resolution processes.

Legal disputes that delay or prevent the resolution of payment settlement can cause credit, liquidity, or reputation risks at individual institutions. Though unlikely, these disputes also can cause potential systemic risk to the payments system. Contractual terms may further define responsibilities within the legal framework; and contracts between financial institutions, customers, and third-party service providers may further integrate risk-sharing responsibilities applicable to payments made through a specific clearing or settlement arrangement.

Digital assets, particularly stablecoins, as a new and emerging payment rail, face legal uncertainties across various jurisdictions. Ambiguous rights and obligations could make the stablecoin payment network vulnerable to loss of confidence by its holders. Therefore, having a well-founded, clear and transparent legal basis is a core element of payment, clearing and settlement arrangements. There is currently no federal guidance regarding the legal qualification of stablecoins, nor do most jurisdictions have regulatory regimes specific to digital assets in general or for stablecoins in particular.[55]

The application of digital assets to the UCC provides greater legal certainty on topics such as settlement finality, rules for adverse claims, discharge of underlying obligations and the concept of a security entitlement.

Settlement Finality

Settlement finality generally refers to the moment after which the parties engaged in transactions cannot unilaterally revoke the transaction. This provides assurance to parties who receive payment

[55] Financial Stability Board. "Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements" (14 April 2020)

that they do not need to worry about the insolvency of their counterparty or parties earlier in the transfer chain.[56]

Digital assets are particularly susceptible to settlement finality challenges because of their probabilistic nature.[57] This situation occurs when there is misalignment between legal finality and technical settlement may occur. [58] Nebraska requires the parties, when not inconsistent with applicable law, to agree to settlement finality conditions under specified principles. Examples may include[59]:

- Clearly define the point at which a transfer on the ledger becomes irrevocable and technical settlement happens, and make it transparent whether and to what extent there could be a misalignment between technical settlement and legal finality; and

- Ensure proper transparency regarding mechanisms for reconciling the misalignment between technical settlement and legal finality and have measures in place to address the potential losses that could be created in case of reversal stemming from the misalignment between technical settlement and legal finality.

Adverse Claims and Negotiability

Under UCC negotiable instrument laws, if the transferee is a holder in due course (i.e., a good faith purchaser that among, other things, does not have notice of the facts that are the basis of the original owner's claim), then the original owner cannot recover the item from the transferee.[60] Similarly, where the item is an investment security or a security entitlement, if the transferer delivers the securities without notice of the adverse claim, then the transferee has the right to take the item free from any adverse claim and the original owner cannot revoke the transfer because the intermediate party acted wrongfully. [61] However, it is worth noting that while negotiability of assets under the UCC provides a good deal of commercial law protection, it does not authorize DDs to reduce the monitoring of the potential illicit activities of network participants and does not reduce the DDs' liabilities for activities proscribed under relevant BSA/AML/KYC and sanctions laws.

Due to the nature of stablecoins and depending on the access criteria of the stablecoin payment network (e.g., permissioned vs permissionless, public network vs private network), the stablecoin could be used for cross-border transfers involving multiple jurisdictions. In such case, DDs may

---

[56] Jess Cheng, Berkeley Business Law Journal. "How to Build a Stablecoin: Certainty, Finality, and Stability Through Commercial Law Principles" (2020)

[57] Nancy Liao, Yale Journal on Regulation. "On Settlement Finality and Distributed Ledger Technology" (2017)

[58] The misalignment can occur when legal finality is thought to have been achieved, but a "fork" causes technical settlement to be reversed.

[59] Bank of International Settlements. "Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements." (October 2021)

[60] UCC § 3-202

[61] UCC § 8-105

face heightened and uncertain legal risks absent of international standards for certain activities. If DDs wish to engage in activities across multiple jurisdictions, DDs must obtain the Director's approval. This may require analysis of customer agreements and consultation with foreign regulatory bodies.

Given the rapidly changing landscape for stablecoin payment network regulation, it is critical that a DD to pay close attention to changing legal and regulatory requirements, as well as to new network rules that might create unexpected liability for the institution.

DDs should also understand the laws and rules that apply to payments they handle and understand the associated legal risks and liabilities they take on with respect to those payments. In particular, a DD must ensure it is in compliance with all applicable Federal laws and regulations governing payment activity, including the Bank Secrecy Act, the USA Patriot Act, and laws regarding economic sanctions. *Appendix C: Legal Framework for Interbank Payment Systems* provides details on the general legal framework for payments and securities settlement systems.

Bank Secrecy Act (BSA)

The BSA requires financial institutions to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor, identify unusual activity, and report suspicious activity. As such, all retail payment systems and wholesale payment systems should be reviewed in terms of BSA/AML compliance requirements. The DD Payment System Manual does not seek to replicate the guidance and expectations, however, and only a brief summary of this compliance risk is offered. Financial institutions should develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the record keeping and reporting requirements set forth in subchapter II of the Bank Secrecy Act. The BSA requires a written compliance program that is approved by the board of directors. The board must note the approval in the board minutes. The compliance program must include, at a minimum:

- Provision for a system of internal controls to ensure ongoing compliance;
- Provision for independent testing for compliance to be conducted by institution personnel or by an outside party;
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and
- Provision for training for appropriate personnel.

Refer to *4.4. Stablecoin Network* of the DD BSA/AML and OFAC Examination Manual for more details on requirements to mitigate compliance risk.

Office of Foreign Assets Control (OFAC)

OFAC administers and enforces economic sanction programs directed against countries and groups of individuals such as terrorists and narcotics traffickers. All U.S. persons and incorporated

entities involved in a payment transaction (i.e., all U.S. citizens and permanent resident aliens, wherever located; all persons and entities within the U.S.; and all U.S. incorporated entities and their foreign branches) are subject to OFAC regulations.

Refer to *4.4. Stablecoin Network* of the DD BSA/AML and OFAC Examination Manual for more details on requirement to mitigate compliance risk.

USA PATRIOT Act

On October 26, 2001, the President signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The USA PATRIOT Act contains strong measures to prevent, detect, and prosecute terrorism and international money laundering. The provisions of the USA PATRIOT Act that most affect financial institutions are those contained in Title III. Among other things, Title III amends the Bank Secrecy Act and provides the Treasury Department and federal agencies with enhanced authority to combat international money laundering and block terrorist access to the U.S. financial system.

The Act is far-reaching in scope, covering a broad range of financial activities and institutions. One such provision is section 312 - Due Diligence for Correspondent and Private Banking Accounts. Section 312 requires a U.S. financial institution that maintains a correspondent account or private banking account for a non-U.S. person to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering. Section 312 also describes specific enhanced due diligence standards for U.S. financial institutions that enter into correspondent banking relationships with foreign banks operating under offshore banking licenses or under banking licenses issued by countries that have been:

- Designated as non-cooperative with international anti-money laundering principles by an international body (such as the Financial Action Task Force) with the concurrence of the U.S. representative to that body, or

- The subject of special measures imposed by the Secretary of the Treasury under section 311 of the USA PATRIOT Act.

Refer to the DD BSA/AML and OFAC Examination Manual for more details on requirement to mitigate compliance risk.

4.7. Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or external events. Operational risk can arise from a technology failure, human or technical errors in financial models and reporting, or other internal control system deficiencies. In the case of emerging new payments (e.g., stablecoin payment networks), weakness in the underlying stablecoin arrangement infrastructure would give rise to operational risk (including cyber risk) and potential risk of loss of both on-chain and off-chain data. DDs may face additional challenges if the DD leverages existing blockchain on the market instead of developing its own

underlying technology infrastructure. As a result, a DD could experience delays or disruptions in processing, clearing, and settling payment transactions that could lead to credit and liquidity problems within the DD or potentially at other financial institutions.

Operational risk can also arise from fraud perpetrated by employees or by external sources. A DD is exposed to operational risk from fraud when a wrongful or criminal deception can lead to a financial loss for one of the parties involved.

Emerging payment mechanisms, such as stablecoin payment networks, equally face fraud risk exposures when the claimed underlying reserve of the stablecoin is deployed for other illicit uses without the awareness and acknowledgement of the clients, leading to potential credit risk and liquidity risk issues. In other cases, depending on the nature of the stablecoin payment network (permissioned vs permissionless; public vs private), certain stablecoin may be leveraged by network participants (e.g., wallet holders or trading platform) to conduct fraudulent activities such as Ponzi schemes[62] without the proper monitoring of the network arrangement governance or timely response from DDs.

Lastly, while distributed ledgers may have features that make them more resilient to certain operational and cyber risks than centrally managed ledger systems, unlike other more traditional payment instruments that have relatively mature and standard underlying infrastructures, the underlying infrastructures of stablecoin payment networks are still evolving and may create operational risk if any of the key components of the infrastructure were disrupted or compromised. Some key considerations include:

- Reliability and resilience of the stablecoin arrangement's ledger and validation mechanism, including validator nodes;
- Capacity of network to validate and process large volumes of transactions; and
- Reliability of custodians/trustees.

Mitigation of Operational Risk

DDs should establish a robust operational risk management framework with appropriate systems, policies, procedures and controls to identify, monitor, and manage operational risks. In particular, a DD's operational risk framework shall include the following:

- Strategies to identify, assess, monitor and manage operational risk;
- Procedures concerning operational risk management;

[62] MMM BSC, the third largest holder of the U.S. dollar stablecoins issued by Paxos Trust Company, used the Paxos stablecoin to engage in a Ponzi scheme, involving around $4 million. See https://www.coindesk.com/10b-stablecoin-industry-has-fraud-problem-its-not-addressing for more details.

- An operational risk assessment methodology; and
- A risk reporting system for operational risk.

For stablecoin payment networks, due to the evolving nature of the use cases, DDs need to frequently conduct risk assessments to identity the potential sources of fraudulent activities and develop a protocol for fraud detection to monitor the transactions or activities using the underlying stablecoins. Clear roles and responsibilities should be outlined by DDs to govern the access criteria and monitor the activities conducted by the network participants. DDs also need to have the ability todevelop criteria for freezing and blocking certain transactions to prevent unlawful activities.

Identifying, evaluating, and addressing potential legal and compliance risks associated with new payment systems providers can also help mitigate operational risk. For example, a thorough legal review process can ensure that there are clearly defined roles and responsibilities for the financial institution, its service providers, and its customers. Financial institutions should also comply with the regulations and consumer compliance mandates that apply to retail payment services (e.g., Regulation E).

Department examiners should evaluate whether DDs have conducted rigorous risk assessments, contingency preparedness, and business continuity planning. In particular, DDs need to have a robust assessment of its technology model and rules for transferring stablecoins that provide assurance of settlement finality consistent with commercial law best practices.

In addition, DDs should have in place robust systems for safeguarding, collecting, storing and managing data. Aside from conforming to all applicable data privacy requirements, DDs should implement and operate data management systems that record and safeguard data or information collected in the course of operations in a discoverable format. Adequate controls need to be in place to safeguard the integrity and security of both on-chain and off-chain data. Department examiners need to be provided timely and complete access to relevant data and information to enable them to conduct supervisory activities.

DDs also should have appropriate risk control functions such as audit, information security, vendor management, and business continuity, as discussed in the following sections.

4.7.1. Audit

An effective audit function should include internal and external audit coverage, tailored to the complexity of the DD, and based upon an accurate, enterprise-wide assessment of the DD's risk profile. Due to the potentially large transaction volumes and associated dollar value when initiating payments, internal audit coverage is critical for an effective oversight of the DD's retail and wholesale payment systems.

For retail payment systems, auditors should perform an evaluation of the DD's business lines on the basis of overall risk to the DD. Based on this evaluation, they should develop an appropriate schedule of audits. The audit coverage should be sufficient to validate the internal control

environment surrounding the processing, clearance, and settlement of retail payment transactions. Auditors should review accounting controls and assess the effectiveness of transaction processing, clearance, and settlement processing procedures.

The board of directors should ensure the operational and IT audit program tests retail payment system internal controls, management policies, and procedures. IT audit coverage should include the design and implementation of retail payment products, and the supporting IT environment encompassing internal data centers, contingency sites, and network infrastructure. IT audit coverage should verify the adequacy of internal controls in applicable business lines responsible for managing day-to-day retail payment system services. Internal audit should assess the comprehensiveness of the institution's vendor management program to ensure the institution is appropriately managing vendor risk.[63] Internal audit should also evaluate payment systems when conducting BSA audits.

For wholesale payment systems, a DD's internal auditors should conduct periodic independent reviews of the funds transfer operation, including all pertinent internal policies and procedures. An external audit can supplement or replace internal audit procedures. DD audits should verify the effectiveness of the funds transfer control environment and identify funds transfer deficiencies for correction.

Department examiners should perform an evaluation of the DD's audit function to determine whether audit activities related to funds transfer operations are comprehensive and effective. Department examiners also should review the auditor's opinion of the adequacy of accounting records and internal controls for funds transfer operations. The review of audit procedures should focus on:

- The scope and frequency of the internal funds transfer audit program;
- The effectiveness of audit procedures in determining any control/operating problems disclosed since the previous examination and what corrective measures management has taken;
- Audit work papers to ensure they document adherence to prescribed audit procedures;
- IT audit coverage of new system enhancements and development projects; and
- External audit findings and recommendations

4.7.2. Information Security

For stablecoin payment networks, DDs need to consider the security of storing customer private keys. As detailed in the DD Information Security Examination Manual, management should only maintain private keys in hot storage when used to conduct customer transactions, and “the mechanism and thresholds for transfer between hot, cold and other forms of storage must be well

[63] See the IT Handbook Audit Booklet.

documented and subject to rigorous internal controls and auditing." Refer to the DD Information Security Examination Manual and DD Custody and Fiduciary Manual for more details on specific considerations related to digital assets.

DDs should have in place a written Response Program detailing DDs' prescribed method of handling an unauthorized access to customer information. [64] The Response Program will be reviewed by Department Examiners as a part of a DD's regular examination. In addition, according to the Statement of Policy #18 released by the Department:

- If a DD becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information, the institution should immediately notify the Department of the apparent security breach and the DD should review Neb. Rev. Stat. §§ 87-801 – 87-807 (the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006);

- If an incident requires customer notification, the Department should be provided one sample copy of the customer(s) notice or other documentation, prior to, or simultaneously with, the customer (s) receiving the notice; and

- If an incident requires a filing of a Suspicious Activity Report ("SAR"), a copy of the SAR must be timely delivered to the Department.

Refer to the DD Information Security Manual for more detailed requirements.

4.7.3. Business Continuity Planning

Effective business continuity planning is an important component in managing operational risk. DDs and their TSPs should develop, implement, and test appropriate disaster recovery and business continuity plans capable of maintaining acceptable retail payment-related customer service levels. Business continuity plans should be based on business impact analyses and the relative importance of payment system products and services to the DDs.[65]

For stablecoin payment networks, the degree of vulnerability would also depend on the operational resilience arrangements for the stablecoin payment network's other participants such as wallet providers or exchanges, including stand in and fallback arrangements that ensure continuity of service to users, and of the continued liquidity of the secondary market for stablecoins.[66] DDs should consider stablecoin arrangements as part of business continuity planning and subject the plan to periodic review and testing, which should address various scenarios and changes that

[64] Nebraska Statement of Policy#18. Response Program/Notification Unauthorized Access to Customer Information

[65] See the IT Handbook Business Continuity Planning Booklet.

[66] Financial Stability Board. "Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements" (14 April 2020)

simulate wide-scale disasters and intersite switchovers.[67] See the DD Supervision Handbook for more information regarding business continuity planning.

4.7.4. Vendor and Third-Party Management

Some DDs may rely on third-party service providers and other financial institutions to provide retail payment system products and services to their customers. Many retail payment services are directly related to core processing financial institution operations (e.g., accessing demand deposit accounts through the use of financial institution-issued bankcards) and may be run in-house through the use of purchased turnkey systems. DDs may also outsource many retail payment-related services to third parties, including foreign-based, either to enhance the services performed in-house or to offer new retail payment services that are otherwise not cost effective.

To ensure payment operations are conducted appropriately, DDs should have comprehensive contract provisions and adequate due diligence processes. They should also monitor service providers for compliance with contracts and service level agreements. Effective monitoring should include the review of select retail payment transaction items to ensure they are accurate and processed timely. The integrity and accuracy of retail payment transactions posted to customer accounts depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Regardless of whether the DD's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to processing checks, including through RDC, as well as electronically created payment orders, electronic bankcard, debit card, and ACH transactions. Financial institutions must also maintain effective control over service provider access to customer and financial institution information consistent with GLBA section 501(b). Contractual provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors.[68]

As issuers of stablecoins, DDs are required to establish and maintain appropriate contractual agreements with third-party entities that ensure the stabilization mechanism and the investment of the reserve assets backing the value of the tokens, and where applicable, the distribution of the stablecoins to the broader audience. The contractual arrangements should precisely set out the roles, responsibilities, change management, rights and obligations of the issuer of stablecoins and each of these third-party entities.

If the underlying infrastructure is outsourced to a third-party technology provider, Department examiners should obtain the technology assessment performed by the DDs to evaluate whether the DD has conducted proper technology due diligence on the risks relying on the third-parties, and whether roles, responsibilities, change management and risk mitigation are clearly outlined.

---

[67] *PFMI*, Principle 17

[68] See the IT Handbook Outsourcing Technology Services Booklet.

4.8. Payment Instrument-Specific Risk Management Controls

Payment instruments introduce risks that require effective internal controls and adherence to the relevant clearing house, association, interchange, and regulatory requirements. DDs should address these risks in their information security, business continuity planning and risk management programs.

4.8.1. Stablecoin Payment Arrangement

A stablecoin payment network poses specific risks that need to be evaluated and reviewed by Department examiners. The following sections discuss additional risks and controls DDs need to account for when designing the stablecoin payment network other than the general risk categories discussed in Section 4.2 through Section 4.7.

The NFIA requires that all stablecoins issued by a DD be backed by a fully-funded reserve of highly liquid assets. [69]

In general, where stablecoins are used in payment networks as money-like instruments, Nebraska requires that they must meet standards equivalent to commercial bank money in terms of stability of value, robustness of legal claim, and the ability to redeem at par in fiat.[70]

4.8.1.1. Governance

DDs must employ a comprehensive governance framework that is clear, transparent and promotes safety and efficiency to ensure ongoing risk management effectiveness of the stablecoin payment network. For example, the access criteria as well as the roles and responsibilities of the network participants may be dependent on the underlying distributed ledger technology ("DLT") infrastructure. Sound governance may be particularly challenging under a permissionless network where the validation process is decentralized or in a public network where the general public can participate in the network, with challenging due diligence performed in the background. For a stablecoin consortium, through which a group of financial institutions participate in the stablecoin issuance and settlement following a standardized operating agreement set by the centralized organization, it is important for Department Examiners to understand the detailed roles and responsibilities played by the DD and the consortium to avoid the possibility of unlimited liability.

In summary, Department examiners need to clearly understand the overall governance framework of the DD's stablecoin payment network. In particular, examiners should seek to understand the following areas when assessing the soundness of the governance framework:

[69] Neb. Rev. Stat § 8-3009(2)(b) (LB707, 2022)

[70] Bank of England Financial Policy Committee. "Financial Stability Report" (December 2019)

- DDs need to have a clear ownership structure and organizational form of the stablecoin payment network;

- DDs need to clearly lay out roles and responsibilities of network participants. This includes the types of entities that could be involved in the arrangement, the protocols for validating transactions, as well as the rules for modifying or updating the protocol and source codes. If the DD is part of the consortium, the DD should be expected to provide the operating rules and relevant documents set forth by the consortium for the examiner's assessment;

- DDs need to provide evidence that the management team of the network has sufficient skills and expertise, and that the operational team has appropriate segregation of duties for their roles and responsibilities;

- DDs must have in place policies and procedures to enable them to effect same-day, intraday, and multiday settlement of payment obligations on time following any individual or combined default among their participants;[71]

- DDs must identify the access criteria of network participants and due diligence requirement for approving the network participants to prevent them from engaging in illicit activities;

- DDs must maintain a documented risk management framework that includes the payment network's risk-tolerance policy, assigns responsibilities and accountabilities for risk decisions, and addresses decision making in crises and emergencies;[72] and

- DDs should maintain coordination plans with other jurisdictions if the stablecoin arrangement is cross-border in nature.

Access and Participation Requirement

Depending on the underlying structure of the stablecoin payment network (e.g., public network vs private network), a stablecoin payment network may have different access criteria for determining who can access the network, who is the asset issuer, or who will serve the role as the validator[73] and proposer. [74] Nebraska does not restrict DDs from selecting a particular stablecoin arrangement, other than the requirements that the stablecoin must be fully backed by reserve assets.

---

[71] *PFMI*, Principle 7

[72] *PFMI*, Principle 2

[73] The Committee on Payments and Market Infrastructures defines "validator nodes" as node permissioned to confirm the validity of proposed changes. See "Distributed Ledger Technology in Payment Clearing and Settlement" (February 2017)

[74] The Committee on Payments and Market Infrastructures defines "proposer nodes" as node permissioned to propose updates to the ledger. See "Distributed Ledger Technology in Payment Clearing and Settlement" (February 2017)

That said, DDs are required to satisfy the following principles when designing the access and participation criteria:

- The access criteria for participation should be risk-based and justified in terms of the safety and efficiency of the stablecoin arrangement; and

- DDs must be able to monitor compliance with its participation requirement on an ongoing basis and have clearly defined procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participant requirement. [75] Particularly, Department examiners need to ensure DDs can conduct screening and transaction monitoring of the network participant to meet BSA/AML/KYC and sanctions requirements.[76]

Tiered Participants Arrangement

A tiered participation arrangement occurs "when some firms (indirect participants) rely on the services provided by other firms (direct participants) to use the financial market infrastructure's central payment, clearing, settlement, or recording facilities,"[77] and the PFMI require that an "FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements." As there may be downstream implications (e.g., liquidity risk, credit risk, operational risk) caused by the indirect participation, DDs should regularly review risks arising from tiered participation arrangements, if any, and should take mitigating actions when appropriate. Department examiners should evaluate:

- Whether DDs have processes to identify material dependencies between direct and indirect participants that may affect the network;

- Whether DDs have processes to identify indirect participants responsible for "a significant proportion of transactions" processed by the DDs and "indirect participants whose transaction volumes or values are large relative to the capacity of the direct participants" through which they access the DDs in order to manage the risks. Particularly, DDs should clearly and appropriately define what would constitute as "a significant proportion of transactions"; and

- Whether such controls and processes noted above are well documented in the relevant policies, procedures, or arrangements, and have been timely updated.

FMI Links

According to the PFMI Principle 20, an FMI link is "a set of contractual and operational arrangements between two or more FMIs that connect the FMIs directly or through an

[75] *PFMI*, Principle 18

[76] Refer to the DD BSA/AML and OFAC Examination Manual for more details.

[77] *PFMI*, Principle 19

intermediary."[78] An FMI may establish links with other FMIs to expand the similar services to additional financial instruments, markets, or institutions, or may establish a link with a different type of FMIs. For stablecoin payment networks, this principle applies when the network establishes agreement with other stablecoin payment networks (or in certain cases with an international payment network) to facilitate cross-border transactions. The Department requires DDs to follow the PFMI Principle 20 for FMI link-related requirements. Particularly, DDs that establish a link with one or more payment networks should identify, monitor, and manage link-related risks.

4.8.1.2. Stabilization Mechanism

In order to stabilize the value of the stablecoins, DDs, as the issuers of such tokens should constitute and maintain the reserve assets of stablecoins at all times based on the following core principles:

- Creation and destruction of stablecoins should always be matched by a corresponding increase or decrease in the reserve assets, and such increase or decreases are adequately managed to avoid adverse impacts on the market of the reserve assets;
- The redemption should be at predictable and transparent rates of exchange, including at par into fiat money consistent with similar instruments used widely for payment purposes;[79]
- DDs should establish and maintain detailed policies that describe, among others, the following elements:
    - The composition of the reserve assets and the allocation of assets;
    - A comprehensive assessment of the risks raised by the reserve assets;
    - The procedure for the creation and destruction of the stablecoins;
    - The documented process for monitoring and overseeing the reserve management practices in the participating financial institution(s); and
    - The procedure to purchase and redeem the stablecoins against the reserve assets; and
- Where the reserve assets are invested, a procedure describing the investment policy should be developed and disclosed to the public. Note that DDs are allowed to invest only in high-quality liquid assets as discussed in this Manual.

---

[78] *PFMI*, Principle 20

[79] Financial Stability Board. "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" (23 October 2020).

4.8.1.3. Custody and Investment Risk

DDs should safeguard their own and their participants' assets and minimize the risk of loss or delay in accessing to these assets, for both fiat currency and digital assets. For stablecoin custody, a DD should generally custody the assets itself, but if appropriate may enter into a sub-custody arrangement with another provider as an external provider of domestic or global custody services. Refer to the DD Custody and Fiduciary Manual for more information.

For stablecoin reserve custody, DDs must have clear and well-documented custody/safekeeping policies and procedures to describe how the reserve assets should be maintained and monitored. In particular:

- The cash reserve assets must be held on deposit with an FDIC-insured, Nebraska-based financial institution.[80]
- The reserve assets should not be pledged as collateral at any time;
- DDs need to have prompt access to the reserve assets; and
- DDs should set up monitoring process to ensure the reserve assets are constantly monitored and daily reconciliations are conducted to provide assurance of the proper management of the account.

DDs may also enter a custody relationship if the DD decides to hold treasury and/or agency bonds as part of their stablecoin liquid reserves. The selected custodian will manage the safekeeping, coupons, and redemptions, among others, in accordance with the custody agreement set forth between the DD and the custodian.

DDs must ensure the underlying reserve assets are highly liquid and are fully (100%) backed, corresponding to the total value of stablecoins issued. Where the reserve assets are invested, procedures describing the investment policy should be developed and disclosed to the public. See *4.5 Liquidity Risk* for more guidance.

For other requirements related to custody of digital assets, refer to the DD Custody and Fiduciary Examination Manual for more details.

4.8.1.4. Consumer Protection and Transparency

DDs should have clear and comprehensive policies and procedures and should provide sufficient information to enable the network participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in such network. All relevant rules and key

[80] Neb. Rev. Stat § 8-3009(2)(b) (LB707, 2022)

procedures should be clearly and publicly disclosed, including in a customer agreement.[81] This includes:

- General information on the DD, including its rights and responsibilities with respect to a stablecoin;
- General information on the customer, including their rights and responsibilities with respect to a stablecoin;
- Stabilization mechanism of the stablecoins;
- Structure and composition of the underlying reserve assets;
- Investment and valuation policy of the underlying reserve assets;
- Redemption and claim rights, including the means by which a person can make a claim while the DD is in operation and in the event of a receivership;
- A statement that Nebraska law requires the stablecoin to be 100% backed by high quality, liquid assets and that the DD is required to monitor compliance on a daily basis;
- A statement that Nebraska law guarantees the segregation of stablecoins and reserve assets in the event of a receivership;
- The name and information of the participating financial institutions responsible for maintaining the stablecoin reserves on behalf of the DD;
- A summary explanation of the assets backing the stablecoins not more than 10 business days after the end of each month. The detailed explanation should include the value of the assets, total liabilities, and the percentage of total assets for each kind of asset held in reserve;
- Custody policy, and if used, identification of any subcustodian;
- The commercial laws applicable to the token and the legal rights of the customer with regards to security interests, negotiability and disputes;
- Information on the underlying technology used (e.g., source code version and changes) [82] and the related risks relating to the technology; and
- A statement that any complaints regarding the DD or the stablecoins can be filed with the Nebraska Department of Banking.

---

[81] *PFMI*, Principle 23

[82] Refer to the DD Custody and Fiduciary Examination Manual for more details.

DDs should clearly document the rights of customers relating to the redemption of reserve assets, including precisely defining the conditions for exercising such rights and communicating such information to customers. DDs should provide all necessary and appropriate documentation and training to facilitate network participants' understanding of the rules and procedures, as well as the risks they may face from participating in the network.

In addition to the disclosure of information described above, DDs are also required to disclose material information on a continuous basis. In particular, they should disclose the number of stablecoins and the value and the composition of the reserve assets, at least on a monthly basis to customers. DDs should also disclose any event that is likely to have a significant impact on the value of the stablecoins or on the reserve assets. Such change management processes must be documented and disclosed so that participants have sufficient knowledge of the general practice.

DDs should also put in place a policy to identify, manage and disclose potential conflicts of interest that would arise from their relationships with their managers, shareholders, clients or third- party service providers.

Lastly, stablecoins and other digital assets could result in reveal sensitive data on users' identities and transactions being centrally visible to a DD. [83] Therefore, the data DDs maintain may become valuable to companies that are interested in such information and represent an attack vector for hackers. DDs need to have in place a clear data privacy policy approved by the Director, as well as procedures to ensure the relevant data is properly stored, maintained and utilized.

[83] Bank of England. "Reinventing the Wheel (with more automation)" (3 September 2020).

5. EXAMINATION PROCEDURES

Examination Objective. *Examiners should use the following examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control environment including information security, business continuity, and management of financial institutions and technology service providers (involved in stablecoin payment networks).*

Examiners should incorporate the Examination Procedures as part of a DD examination. The Examination Procedures can be used in their entirety, or can be used in modular fashion. Depending on the size and complexity of the DD or service provider, examiners may tailor the use of the examination procedures. In many cases, examiners can eliminate certain procedures and still arrive at a conclusion regarding the quality of risk management practices.

Objective 1: Assess the level of risk.

1. Determine the types of payment products and services offered. Consider the following:
    - The types of customers using the products and services.
    - The geographic service footprint (e.g., international usage)
2. Determine whether new payment products and emerging technologies pose increased risk due to the lack of maturity of the respective control environments. Consider:
    - New payment products and services that have been introduced within the past year, such as stablecoin arrangements.
    - Whether the institution introduced any existing products into new markets within the past year.
3. Determine if the quality of management and staff, and the staffing levels are adequate for the specific payment products and processes the institution provides.
    - Obtain and review the following:
    - Reports showing staffing levels, turnovers, and trends.
    - Biographies of managers and key staff
    - Consider:
    - The levels of skill and experience of key managers and staff, particularly in terms of the sophistication and complexity of the products, processes, and systems.
    - Whether the institution has appropriate depth of management and staff.

- The adequacy of staffing levels for peak operating periods.
- Management and staff turnover.

4. Determine if the quality of process design and control points are adequate for existing products, and if these factors are considered for new products. Consider whether:
   - There is adequate capacity for current and planned transaction volumes.
   - Processes are clearly designed.
   - Processes are automated.
   - There is a reasonable degree of manual intervention.
   - Any processes have been re-engineered during the past year.
   - Processes are outsourced or performed at the customer location.
5. Evaluate the use of in-house and outsourced data processing systems. Consider:
   - How new are existing systems.
   - How stable are existing systems.
   - How current are existing systems.
   - Whether there is adequate capacity for current and planned transaction volumes.
   - Whether the institution uses leading edge technologies or only mature technologies.
   - To what extent are systems outsourced.
   - Whether outsourcing arrangements are governed by contracts and service level agreements.
   - Whether vendors are considered to be industry-recognized leaders.

Objective 2: Establish the scope and objectives of the examination.

1. Review previous reports of examination for comments. Review:
   - Regulatory reports of examination, including consumer and compliance information.
   - Prior examination work papers, including any documentation obtained through on-going supervision.
   - Internal control self-assessments completed by business lines.

- Internal and external audit reports, including annual attestation letters.
- Regulatory, audit, and information security reports from service providers.
- Supervisory strategy documents, including risk assessments.

2. Review past examination reports for comments relating to the institution's internal control environment and technical infrastructure. Review:
   - The institution's processing architecture, including processing outsourcing arrangements.
   - Internal controls, including physical and logical access controls in the data entry area, data center, and item processing operations.
   - Stablecoin payment network governance and controls.
3. Review the financial institution's risk and control assessments for comments. Review the following risk assessments:
   - External and internal audit;
   - Management controls;
   - Information security;
   - Business continuity;
   - Regulatory compliance; and
   - AML/CFT.

Objective 3: Assess the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's payment systems management function. Consider:
   - The alignment of the institution's business plans with its technology and operational plans for payment systems.
   - Departmental management and the quality of internal controls.
   - Departmental management and the quality of information security and GLBA 501(b) compliance policies relating to retail payment system-generated customer data.
2. Determine the quality and effectiveness of the financial institution's wholesale payment systems management function. Consider:

- Data center and network controls over backbone networks and connectivity to counter parties.
- Departmental controls, including separation of duties and dual control procedures, for funds transfer, clearance, and settlement activities.
- Compliance with the Federal Reserve's Payment System Risk policies and procedures, if applicable.
- Physical and logical security controls designed to ensure the authenticity, integrity, and confidentiality of wholesale payments transactions.

3. Assess management's ability to manage outsourced relationships with third-party service providers. Consider:
   - Process utilized to encrypt transactions while in route between third-party service providers and the institution.
   - Adequacy of third-party controls related to the roles and usage of third parties in payment systems and stable coin functions such as management of reserves.
   - Adequacy of contract provisions including service level, performance agreements, responsibilities, liabilities, and management monitoring.
   - Management's determination of the service provider's compliance with applicable financial institution and consumer regulations and with third-party requirements (e.g.,AML/CFT, NACHA, GLBA, bankcard company, and interchange).
   - Adequacy of contract provisions for personnel, equipment, and related services.
   - Quality of management information systems (MIS) and reports needed to monitor the third-party service provider's performance appropriately.
4. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business continuity planning. Consider:
   - Ability to recover transaction data and supporting books and records based on retail and wholesale payment system business line requirements and timelines.
   - Level of testing conducted to ensure adequate preparation.
   - Fraud detection protocol to monitor fraudulent activities.
   - Ability to return to normal operations once the contingency condition is over.
   - For wholesale payment system, also consider confidentiality and integrity of interbank and counter party data in transit and storage.

- Whether the institution conducts risk assessments prior to deployment of new and emerging technologies.
- Whether the processes involve the institution's compliance functions, including consumer compliance, AML/CFT, GLBA 501(b), and third party requirements.
- Whether risk assessment and compliance status are communicated to senior management and the board of directors.

Objective 4: Assess the quality of policies, procedures, and limits supporting payment services.

1. Review policies, procedures, and limits for supporting all r payment services.
   - Determine if there are written policies.
   - Determine if the policies reflect the current business and processes.
   - Determine if the policies establish reasonable limits.
   - Determine if the policies correctly reflect the assessment of risks for emerging new technologies.
2. Review staff training programs and determine if they are appropriate for supporting policies.
3. Determine whether the institution monitors compliance with policies, procedures, and limits.
   - Determine if exception monitoring reports are elevated to appropriate levels of management.
4. Determine if the relevant policies and procedures are properly communicated and disclosed to customers.

Objective 5: Assess the quality of management information systems and reports used to manage payment services.

1. Review management reports for all payment services including reports from service providers, liquidity reports, and reserve reports of stablecoin arrangements.
   - Determine if the reports are appropriate to the businesses and processes in terms of scope and frequency.
   - Determine if the reports are reviewed at the appropriate levels of management.

Objective 6: Determine the quality of risk management and support for internal audit and the effectiveness of the internal audit program for wholesale payment systems.

1. Review the audit program to ensure all functions of the FTS are covered. Consider:
    - Payment order origination (funds transfer requests).
    - Message testing.
    - Customer agreements.
    - Payment processing and accounting.
    - Personnel policies.
    - Physical and data security.
    - Contingency plans.
    - Credit evaluation and approval.
    - Incoming funds transfers.
    - Federal Reserve's Payment Systems Risk Policy.
2. Review a sufficient sample of supporting audit work papers necessary to confirm that they support the execution of procedures established in step 1 above.
3. Review all audit reports related to the FTS and determine the current status of any exceptions noted in the audit report.

Objective 7: Assess the quality of risk management of the stablecoin payment network

1. Determine whether the DD has in place rules and processes to ensure the proper governance of the stablecoin payment network.

1.1. Determine whether the stabilization mechanism of the stablecoin payment network is clear and well documented.

- Interview management and review documents to understand the underlying stabilization mechanism of the stablecoin payment network.
- Review documents explaining the operation of intended value stabilization mechanism and determine if technical and legal details are sufficient.
- Evaluate if the stablecoin is linked to a single asset or a basket of assets and how the individual token holder’s share of the value is calculated.

1.2. Evaluate whether the stablecoin redemption right is clearly disclosed and communicated.

- Review contractual terms or relevant documents that explain the token holder's redemption rights on the underlying assets, including conditions required for redemption and how claims may be treated in insolvency or resolution. Redemption in U.S. dollars is deemed to have occurred when the Issuer has fully processed and initiated the outgoing transfer of funds to the holder's financial or other institution, if and as requested by the holder, or has credited the funds to the holder's cash account with the Issuer, if requested by the holder.

- Review documents detailing the operation of the redemption or return mechanism, including under stress scenarios.

- If stablecoin holders are granted a direct claim against the issuer or the reserve, review mitigating controls in case for a reserve run under extreme circumstances to minimize the liquidity risk and credit risk.

1.3. Evaluate the liability terms and whether such terms have been disclosed and are compliant with existing Nebraska law and this Manual.

- Review contractual terms that explain the liability of the stablecoin and the underlying assets. For example, is the claim on the issuer and if so, is there a condition for meeting that claim?

1.4. Review marketing material and other relevant documents to assess whether DDs provide sufficient customer protection and transparency for the operation of the stablecoin arrangement network, based on the standards of this Manual.

- Review the marketing material and disclosed information to evaluate whether the stablecoin governance arrangements have been sufficiently and timely shared with the users and stablecoin holders. In particular, Department examiners should determine whether the following information has been shared:

    - Design of the stabilization mechanism, including how the stablecoin's value is maintained;

    - The amount of stablecoin in circulation;

    - Composition of the underlying reserve backing the stablecoins;

    - Name and relevant contractual agreements with the participating financial institution(s) that custody the reserves on behalf of the DD; and

    - Redemption rights and required conditions for redemption;

- Review the relevant documents to determine whether DDs have change management processes in place to define what types of information need to be disclosed after significant changes to the stablecoin protocol or network and what types of information is disclosed on a continuous basis.

- Review the relevant documents to determine whether DDs have in place policies or procedures to identify, manage and potentially disclose conflicts of interest arising either from their customers, shareholders or third-party service providers.

1.5. Assess the vendor management program covering the technology service providers that support the stablecoin arrangement, if applicable. Determine:

- The adequacy of due diligence performed on the technology service provider;
- Whether management regularly reviews the financial status of the technology service provider;
- Whether management receives independent audits, third-party review, or data information security reviews performed on the technology service provider;
- Whether the information exchanged with the technology service provider is documented and meets the DD's requirements;
- Whether the dispute resolution process between the technology service provider and customer is documented and meets the DD's requirements;
- Whether MIS received from the technology service provider is adequate; and

1.6. If the DD is part of a stablecoin consortium, Department Examiners should review the operating agreement and relevant procedures outlining the roles and responsibilities of the consortium membership, including the DD itself.

1.7. Evaluate other governance protocols of the stablecoin arrangement to assess if they can ensure the safety and soundness of the network.

- Determine whether the DD's stablecoin network governance includes an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided.
- Review the due diligence undertaken by the DD regarding network participants or any other third parties that are involved in the stablecoin payment network. Identify different roles of network participants. Assess whether existing onboarding and ongoing oversight programs are reasonably satisfactory to protect the DD.
- Review the DD's procedures regarding network participant access criteria to determine whether they are risk-based and justified in terms of the safety and efficiency of the stablecoin arrangement.
- Review documents or procedures that define the compliance monitoring and fraud monitoring of the network participants. Refer to the DD AML/CFT and OFAC Examination Manual for more detailed considerations.

- Review the DD's tiered participation arrangement documents, if any, to evaluate if the DD provide clear guidance on complying with tiered participation arrangements.

- Discuss with the DD whether it has established any FMI link with other financial market infrastructures and review the contract to evaluate the DD's risk exposure.

- Evaluate whether the DD has conducted proper due diligence into individuals involved in the management and control of the stablecoin arrangement, as well as those who exercise significant power or discharge significant responsibilities in relation to the stablecoin arrangement.

- Evaluate the internal controls of the DD stablecoin arrangement and whether there is a clear segregation of duties among its operational staff.

2. Determine whether the DDs' protocol on issuing, creating and destroying stablecoins is clearly documented and executed.

- Review procedures detailing DD's processes on issuing, creating and destroying stablecoins, particularly:

    - Is the process automatic or manual. If automatic, what is the system supporting the process and are these procedures to ensure the maintenance of the system.

    - If the process is manual, are there clearly documented procedures and sufficient staffing with appropriate skillsets? Is there clear segregation of duties among operational staff, reflected in both documentation and actual execution.

- Review third-party independent reports on whether creation and destruction of stablecoins are always matched by a corresponding increase or decrease in the reserve assets.

3. Determine whether the DD has appropriate reserve management processes and risk mitigation controls.

- Review the DD's procedures regarding collateral reserve requirement, including percentage of reserves, location of reserves, as well as the monitoring and reporting processes.

- Review the DD and participating financial institution's (or institutions') operating agreement on reserve management, including monitoring, reconciliation, and reporting processes.

- Review the DD's liquidity management documentation to evaluate whether liquidity risks have been sufficiently identified and can be mitigated properly.

- Obtain and review audit reports that attest the reserve held by DDs/participating financial institutions is always equal to or greater than the number of outstanding stablecoins issued.

- Review rules and procedures for participant default management and whether a sufficient capital buffer or contingency plan is in place for mitigating potential liquidity risk.

- Collect a sample of MIS reporting on the reserve assets and evaluate whether the report is consistent with the actual amount of reserves the DD holds.

- Obtain the DD's investment policy for the underlying reserve and evaluate whether the investments, including type of asset, duration, interest rate risk and credit risks, are appropriate based on market conditions and whether the investment policy has been fully disclosed to customers.

- If a DD holds treasury and/or agency bonds as part of stablecoin liquid reserves and the DD contracts with a custodian to manage the safekeeping, coupons, redemptions, etc., obtain the custody agreement to review the detailed terms on redemption and reconciliation.

4. Evaluate the safety and soundness of the custody arrangement for the underlying reserve of the stablecoins is safe, transparent and able to retain confidence in the stablecoins.

- Review the custody arrangement to understand the following:

    - Whether DDs have prompt access to the reserve assets;

    - The account segregation model for the underlying reserves (i.e., are the reserves maintained separately from the operating funds of the selected financial institution? If required, are reserves maintained separately from other customers funds?); and

    - Whether the participating financial institution(s) have reporting mechanism to provide daily reports, or more frequently, as warranted, on the amount and composition of the reserve to the DD.

5. Evaluate whether the processes for ensuring the appropriate operation of the underlying infrastructure of the stablecoin network.

- Review DDs' policies and procedures to evaluate whether DDs have:

    - Developed strategies to identify, assess, monitor and manage operational risk;

    - Documented the operational risk management framework;

    - Defined an operational risk assessment methodology; and

    - Maintained a risk reporting system for operational risk.

- Review documents to evaluate whether DDs have robust systems for safeguarding, collecting, storing and managing data, and whether DDs have data privacy requirements in place.

- Review audit policies or procedures to ensure the auditing processes are executed timely and properly.

- Review the DD's business continuity plan to evaluate whether the continuity plan considers unique risks related to stablecoin arrangements.

- If DDs outsource the underlying infrastructure of the stablecoin arrangement, obtain third-party vendor management policies and a list of all vendors the DD currently works with.

- Obtain the technology assessment documents to evaluate whether the DD has conducted proper technology due diligence on the risks of third-parties, and whether the roles, responsibilities, change management and risk mitigation are clearly outlined.

6. Evaluate the mechanism by which a transaction is authorized and validated by nodes.

- Sample a batch of transactions to understand how transactions are validated and how long the average validation takes.

- Review the technology assessment to understand whether DDs have a clear understanding of the capacity of the network they rely on to validate and process large volumes of transactions.

- Review the operational resilience document and contingency planning procedures to evaluate whether there are sufficient back-up plans if the stablecoin arrangement ledger was compromised due to failure of multiple validator nodes.

7. Evaluate whether DDs safely store the private keys which provide access to stablecoins.

- If the private keys are stored in-house, refer to the DD Custody and Fiduciary Manual for detailed examination questions.

- If the service is provided by a subcustodian, review the stablecoin arrangement and technology assessment to understand whether DDs have a clear understanding of the processes and underlying technology applied and a monitoring/control framework in place.

8. Evaluate whether DDs have appropriate rules to govern the exchange, trading, reselling and market-making of stablecoins.

- Evaluate whether DDs have maintained a list of available exchange platforms or brokers participating in the stablecoin arrangement and could make such information available at any time.

- Review DDs' liquidity management program and operational risk management to evaluate mitigating controls and continuity planning under a stress scenario (e.g., withdrawal of liquidity provision by authorized resellers or market makers, disruption of a trading platform or cyber incident).

- Review DDs' fraud and market manipulation programs to evaluate whether there is clear standard on identifying fraud activities and market manipulation activities. See the DD Custody and Fiduciary Manual for further information.

APPENDIX

Appendix A: List of Digital Asset Guidance and Supervision Documents from Other Jurisdictions

A number of supervisory bodies have developed regulations, guidance, and other descriptions of digital assets that address payment system risk and stablecoin arrangements. 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 23, 2022, and will be updated periodically.

Source	Reference Material
Applicable U.S. federal and state standards for reference	• FFIEC: FFIEC Retail Payment Systems IT Examination Handbook (June 2010) • FFIEC: FFIEC Wholesale Payment Systems IT Examination Handbook (September 2004) • Federal Reserve: Federal Reserve Policy on Payment System Risk (March 2021) • Federal Reserve: Federal Reserve Banks Operating Circular 1 (August 2021) • Federal Reserve Bank of New York: Account and Financial Service Handbook (February 2019) • Federal Reserve: Federal Reserve System Proposed Guidance for Evaluating Account and Services Requests (March 2022) • President's Working Group on Financial Markets, FDIC, and OCC: Report on Stablecoins (November 2021) • New York Department of Financial Services Part 200 (Virtual Currencies) including 200.15 (Anti-Money Laundering Program) and (Proposed Guidance Regarding Adoption or Listing of Virtual Currencies) • NYDFS: Guidance on the Issuance of U.S. Dollar-Backed Stablecoins (June 2022) • White House: United States Strategy on Countering Corruption (December 2021) • White House: Executive Order on Ensuring Responsible Development of Digital Assets (March 2022) • House Bill: Stablecoin Classification and Regulation Act of 2020 (November 2020) • Senate Bill: Stablecoin Transparency Act (March 2022)

	• Senate Bill: Stablecoin Transparency of Reserves and Uniform Safe Transactions Act of 2022 (April 2022) • Senate Bill: Lummis-Gillibrand Responsible Financial Innovation Act (June 2022)
Select Foreign-jurisdiction standards	• Monetary Authority of Singapore: Singapore Payment Service Act (January 2019) • Monetary Authority of Singapore: Consultation on the Payment Services Act 2019: Scope of E-money and Digital Payment Tokens (December 2019) • Monetary Authority of Singapore: FAQs on the Payment Service Act (March 2022) • Switzerland FINMA: Swiss Financial Market Infrastructure Act (June 2015) • Switzerland FINMA: Supplement to the Guidelines for Enquires Regarding the Regulatory Framework for Initial Coin Offerings (ICOs) (September 2019) • European Commission: Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (September 2019) • Abu Dhabi's Financial Services Regulatory: Authority Guidance – Regulation of Virtual Asset Activities in ADGM (February 2020) • UK Financial Conduct Authority: The Electronic Money Regulations 2011 (2011) • UK HM Treasury: UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence (January 2021) • UK HM Treasury: UK Regulatory Approach to Cryptoassets, Stablecoins, and Distributed Ledger Technology in Financial Markets: Response to the Consultation and Call for Evidence (April 2022)
Industry Guidance	• Committee on Payments and Market Infrastructures (CPMI): Investigating the impact of global stablecoins (October 2019) • Committee on Payment and Settlement Systems (CPSS): CPSS- IOSCO Principles for Financial Market Infrastructures ("PFMI") (August 2012) • CPMI: Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements (October 2021) • CPMI: Enhancing cross-border payments: building blocks of a global roadmap (July 2020)

- CPMI: Wholesale digital tokens (December 2019)
- IOSCO: Global Stablecoin Initiatives Public Report (March 2020)
- Financial Stability Board: Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements (October 2020)
- Global Digital Finance: Global Digital Finance - Stablecoin Taxonomy and Key Considerations (May 2020)

Appendix B: DD Request Letter Items

Audit / Independent Review Program

- Internal and external audit reports and reviews completed since the previous examination, including reviews of the Information Security Program, IT general control reviews, wire transfer, Identity Theft Program, and NACHA Rule Compliance audits. Include engagement letters for outsourced audits and reviews.

- Audit and regulatory findings/exceptions tracking reports and audit committee minutes, if not already provided as part of the risk assessment request package

- Most recent IT audit plan

Management

- A description of the payment system activities performed and scope of operations.

- Operational reports for retail payment system activities, including transaction volumes, dollar and stablecoin amounts, and trends. Where possible, compare levels and trends with peer financial institutions. Significant increases may indicate a change in risk to the financial institution and management awareness should be evaluated.

- Organization charts of retail lines of business to determine reporting relationships and how the collective retail lines of business are structured and managed.

- The retail payment system functions performed through outsourcing relationships and the financial institution's level of reliance on those services.

- Any significant changes in retail payment system policies, personnel, products, strategy and services since the last examination.

- A listing of all payment processing and clearing house settlement arrangements in which the financial institution participates. Include any bilateral retail payment clearing arrangements the institution may have with other institutions that are outside traditional clearing houses such as FedACH and EPN. Evaluate the methodology used by the financial institution in assessing its operational and settlement risk from these arrangements.

- Operational Risk Management Policy and related procedures. Documentation of any related operational or credit losses incurred, reasons for the losses, and actions taken by management to prevent future losses for each retail payment system.

- A network diagram of the transaction flow from the merchant end of the network, through any intermediary processors, to the financial institution, for all types of payment channels.

- Obtain a thorough description of the wholesale payment system activities performed, including transaction volumes, transaction dollar amounts, and scope of operations, including Fedwire Funds Service, CHIPS, SWIFT, and all wholesale payment messaging systems in use.

- Obtain the financial institution's payment system risk policy and evaluate its compliance with net debit caps and other internally generated self-assessment factors.

Stablecoin Arrangements:

- Sample of customer agreements and type and volume of transactions conducted;

- Governance arrangement policies and guidance including stabilization mechanism operations, redemption and liability guidance and network participants requirements;

- Sample of marketing material and customer disclosure policy;

- Procedures detailing the DD's processes on stablecoin issuance and reserves;

- Investment policy governing the reserve asset composition and management;

- Custody policy of the arrangement, including any sub-custodial agreements;

- Internal/external audit reports of the DD's stablecoin reserves and sample MIS reporting;

- Operational risk management documents and vendor contract samples; and

- Transaction sample based on the known operations of the DD.

Appendix C: Abbreviations and Key Terms

Abbreviation or Term	Full Name or Description
AML	Anti-Money Laundering
ANSI	American National Standards Institute
ARC	Accounts Receivable
ASC	Accredited Standards Committee
ATM	Automated Teller Machine
A2A	Account-To-Account
BSA	Bank Secrecy Act
BOC	Back Office Conversion
CHIPS	Clearing House Interbank Payment System
CHIP Co.	The Clearing House Interbank Payments Company L.L.C
CI	Computer interface
Circular 3	Federal Reserve Bank Operating Circular 3
CPSS	Committee on Payment and Settlement Systems
CVC	Convertible Virtual Currency
DAI	The MakerDao's Dai digital asset
DD	Digital Asset Depository Institution
DeFi	Decentralized Finance
Digital Asset (or "controllable electronic record" per NRS-8-3003 (5))	A digital asset that is used or bought primarily for consumptive, personal or household purposes and includes: (A) An open blockchain token constituting intangible personal property as otherwise provided by law; (B) Any other digital asset which does not fall within the definitions of digital security or virtual currency. Per Nebraska legislation, the term digital asset has the same meaning as 'controllable electronic record,' which is defined as an electronic record that can be subjected to control and does not include electronic chattel paper, electronic documents, investment property, and transferable records under the Uniform Electronic Transactions Act.

	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."
EBT	Electronic Benefits Transfer
EIC	Examiner in Charge
E-Money	Electronic Money
EPN	Electronic Payments Network
ET	Eastern Time
FATF	Financial Action Task Force on Money Laundering
FFIEC	Federal Financial Institutions Examination Council
GUSD	Gemini Dollar
IAT	The International ACH Transaction SEC code
IOSCO	International Organization of Securities Commissions
IP	Internet Protocol
IrFM	The Infrared Financial Messaging Group
ISOs	Independent Sales Organizations
MICR	Magnetic Ink Character Recognition
MIS	Management Information Systems
MSP	Merchant Service Provider
NACHA	National Automated Clearing House Association
NFIA	Nebraska Financial Innovation Act
NFC	Near Field Communication
NSS	Federal Reserve's National Settlement Service
ODFI	Originating Depository Financial Institution

OFAC	Office of Foreign Assets Control
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Digital Assistant
PIN	Personal Identification Number
POP	Point-Of-Purchase
POS	Point-Of-Sale
PSR Policy	Federal Reserve Policy on Payment System Risk
P2P	Person-To-Person
RDFI	Receiving Depository Financial Institution
RFID	Radio Frequency Identification
RTGS	Real-Time Gross Settlement System
SEC	Standard Entry Class Code
SSL	Secure Socket Layer
Stablecoin	Stablecoin means a cryptocurrency designed to have a stable value that is backed by a reserve asset.
UCC	Uniform Commercial Code
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
Virtual Currency	A digital asset that is: (A) Used as a medium of exchange, unit of account or store of value; and (B) Not recognized as legal tender by the United States government. Note: Virtual currency or a digital security, as defined in W.S. 34-29-101(a), shall not constitute an open blockchain token.
VPN	Virtual Private Network