Audit, Dept. of

Banking Division

Chapter 19: Enhanced Digital Asset Custody Framework

Effective Date: 05/13/2021 to Current

Rule Type: Current Rules & Regulations

Reference Number: 021.0002.19.05132021

Chapter 19
Enhanced Digital Asset Custody Framework

Section 1. Authority and Scope.

(a) These rules are promulgated pursuant to Wyoming Statute ("W.S.") 13-1-603(c)(v) and W.S. 34-29-104(o).

(b) This chapter governs banks, as defined in W.S. 13-1-101(a)(i), that elect to opt into enhanced regulatory requirements for digital asset custodial services under W.S. 34-29-104.

(c) If an examination conforming to the requirements of section 8 is not feasible because of the inability of any reasonably available auditor to comply with all provisions of subsection (s), the bank may voluntarily opt into all of the remaining provisions of this chapter.

Section 2. Definitions.

(a) As used in this chapter:

(i) "Bailment" means a legal circumstance when a customer has entrusted possession or control of a digital asset to a bank for a specific purpose, pursuant to an express agreement that the purpose shall be faithfully executed and that possession or control of the digital asset will be returned when the specific purpose is accomplished or when the customer requests return of the asset, consistent with W.S. 34-29-104. This term means a change in possession or control but not a change of title, and may be carried into effect through the exercise of fiduciary and trust powers or on a purely contractual basis;

(ii) "Control" means as defined in W.S. 34-29-103(e);

(iii) "Custody" or "custodial services" means as defined in W.S. 34-29-104(p)(iii) and other applicable federal laws, including those federal laws governing commodities as necessary, and means the possession or control and safekeeping of customer currency and digital assets. This term includes fund administration, the execution of customer instructions and custodial services customary in the banking industry, provided that the Commissioner may rely on guidance from foreign, federal or state agencies to determine customary custodial services. Custody consisting of non-discretionary asset safekeeping activities is generally non-fiduciary and an activity incidental to the business of banking. This term may include the exercise of fiduciary and trust powers to the extent the bank is exercising discretion in managing customer assets as well as providing safekeeping;

(iv) "Fungible" means a characteristic of a digital asset which makes the asset commercially interchangeable with digital assets of the same kind;

(v) "Independent public accountant" means a public accountant that meets the standards described in 17 C.F.R. 210.2-01, as incorporated herein by reference on July 1, 2019;

(vi) “Multi-signature arrangement” means as specified in W.S. 34-29-103(e)(ii);

(vii) “Nonfungible” means a characteristic of a digital asset which makes the asset unique and not commercially interchangeable with digital assets of the same kind for monetary, commercial or other intrinsic reasons;

(viii) “Omnibus account” means a commingled account in which a bank that provides custodial services does not strictly segregate digital assets for each customer or beneficial owner, consistent with W.S. 34-29-104(d)(ii);

(ix) “Private key” means as defined in W.S. 34-29-103(e)(iii);

(x) “Reasonable efforts” means providing written notice to a customer, but shall not require customer acknowledgement or consent;

(xi) “Rehypothecation” means the simultaneous reuse or repledging of a digital asset that is already in use or has already been pledged as collateral to another person;

(xii) “Source code version” means the version of the software that enforces block validation rules that enable consensus and define a digital asset.;

(xiii) "Possession" means as defined in W.S. 34-29-103(e);

(xiv) "Fiduciary and trust powers" means the discretionary authority customarily exercised by state and national banks in either a fiduciary or trust relationship.

(b) The term "blockchain" shall encompass any other form of distributed ledger appropriate for the context in which the term is used. Any reference in these rules to a technological process, system or other form of technology shall also include any other process or technology which is a substantially similar analogue, as determined by the Commissioner. For example, a "blockchain" is a form of "distributed ledger." The Commissioner shall adhere to the purposes and standards of this Chapter in analyzing any substantially similar analogue.

(c) The term "person" shall include a digital asset wallet possessed or controlled by a person for the purposes of any applicable commercial law, if agreed to by a bank and a customer.

(d) In classifying a digital asset within the categories of W.S. 34-29-101 for the purposes of this Chapter, the Commissioner shall use a predominant characteristics test and examine the substance of the asset over its form, consistent with federal law.

Section 3. Opt-In Procedure; Form of Notice.

(a) Consistent with W.S. 34-29-104(a), a bank may provide custodial services upon providing sixty (60) days written notice to the Commissioner.

(b) Written notice under subsection (a) shall contain the following information:

(i) A complete, detailed outline of the proposed custodial services, including measures which will be taken to comply with W.S. 34-29-104 and risk mitigation activities;

(ii) Verification that the bank is currently in compliance with all applicable state and federal statutes and rules, and will, unless a change in law occurs, be in compliance with all applicable state and federal statutes and rules while providing custodial services;

(iii) Reasons why the proposed custodial services will likely not impair the solvency or the safety and soundness of the bank, consistent with W.S. 34-29-104(m); and

(iv) The signatures of the Chief Executive Officer and Chief Financial Officer of the bank or the equivalent officers, verifying the true and complete nature of the written notice.

Section 4. Digital Asset Custodial Services; Permissible Transactions; Customer Funds.

(a) A bank providing custodial services under W.S. 34-29-104 may serve as a "qualified custodian," as specified by 17 C.F.R. § 275.206(4)-2, as incorporated by reference on July 1, 2019 or as a custodian authorized by the United States commodity futures trading commission or other law. A "qualified custodian" shall maintain customer digital assets, funds and other securities which are not digital assets:

(i) In a separate account for each customer under that customer's name; or

(ii) In accounts that contain only customer digital assets, funds and other securities which are not digital assets, under the bank's name as agent or trustee for customers.

(b) A bank shall maintain possession or control over each digital asset while in custody. If a customer makes an election under W.S. 34-29-104(d)(ii), a bank maintains possession or control under this subsection by entering into an agreement with the counterparty to a transaction which contains a time for return of the asset.

(c) Consistent with W.S. 34-29-104(d) and subsection (d) of this section, before providing custodial services to a customer, a bank shall require the customer to elect, via a written agreement with the bank, one (1) of the following relationships for each digital asset account, or class of digital assets, for which custodial services will be provided:

(i) Custody under a bailment as a nonfungible or fungible asset, dependent on the nature and quality of the asset. Assets held under this paragraph shall be strictly segregated from other assets; or

(ii) Custody pursuant to subsection (d) of this section for the purpose of conducting fiduciary and trust activities, which may include a securities intermediary relationship under title 34.1, article 8, Wyoming statutes (Uniform Commercial Code).

(d) If a customer makes an election under W.S. 34-29-104(d)(ii) and paragraph (c)(ii) of this section, the bank may, based solely on customer instructions, undertake transactions with a digital asset authorized under subsection (e) of this section on behalf of the customer. The bank shall not act, and may not use its discretion, unless explicitly granted such authority by the customer. As used in this chapter, "customer instructions":

(i) Except as otherwise provided in paragraph (e)(ii) of this section, mean a distinct, written authorization from a customer to undertake transactions specified under subsection (e) of this section, and need not include all or a majority of the aspects of the transaction, or all requirements customary to be provided to a directed custodian, as long as the intent of the customer regarding the type of transaction and understanding of potential risks is clearly apparent in the written authorization;

(ii) May include all information customarily provided to a directed custodian with respect to a transaction, and may provide for the bank to serve only as a directed custodian for that transaction;

(iii) May include a form the bank provides to a customer, whether solicited or unsolicited, listing a range of options from which a customer may choose, provided that the role of the bank shall be limited to setting forth the potential benefits and risks of a transaction in a straightforward manner.

(e) In accordance with customer instructions as specified under subsection (d) of this section and subject to applicable federal law, a bank may undertake the following transactions with digital assets in any market in which the transaction is not prohibited by law:

(i) Buying and selling digital assets;

(ii) Participating in staking pools for proof-of-stake-type digital assets, in masternodes, voting for delegates in delegated proof-of-stake protocols, leased proof-of-stake arrangements, locked stability fee arrangements, or similar revenue-generating arrangements characterized by higher gains accruing to larger pools of assets for the purpose of providing economic incentives for customers to pool assets. Banks may share in gains accruing to such pools but only if the terms through which the custodian may share in the gains, as well as the benefits and risks from participation in the pools, are fully disclosed to customers and customers expressly agree;

(iii) Regulated commodities activities, including derivatives, consistent with safe and sound banking practices;

(iv) Exchange services from digital assets to any official currency of a jurisdiction or other type of digital asset and vice versa. To the extent practicable, services under this paragraph shall be based on existing standards and best practices for foreign exchange transactions;

(v) Lending of digital assets, excluding rehypothecation, consistent with W.S. 34-29-104(k) and section 12 of this chapter;

(vi) Securities activities, including those specified by 17 C.F.R. 218.100, consistent with safe and sound banking practices;

(vii) Other classes of transactions approved by the Commissioner in writing in advance including exchange-traded derivative contracts defined by an exchange and over-the-counter derivative contracts. The role of the Commissioner under this paragraph shall not include consideration of the merits of a proposed class of transactions brought under this paragraph, but rather is limited to ensuring that the proposed class of transactions is clearly defined so that the boundaries of the approval are clear and that the solvency, safety and soundness of the bank is not likely to be impaired by participating in the proposed class of transactions.

(f) Consistent with section 2 of this chapter, custodial services includes providing services to mutual funds and investment managers, retirement plans, bank fiduciary and agency accounts, bank marketable securities accounts, insurance companies, corporations, endowments and foundations and private banking customers based on the following:

(i) Core custodial services: Control of customer assets, settlement of trades, investment or allocation of cash balances as directed, collection of income (including ancillary and subsidiary benefits), processing of corporate actions, pricing assets, providing recordkeeping, reporting services, fund administration, performance measurement, risk measurement, compliance monitoring and transactions based on customer instructions, consistent with subsections (d) and (e) of this section;

(ii) Global custodial services: Custodial services for cross-border transactions, executing foreign exchange transactions and processing tax reclaims and other tax-based transactions;

(g) A bank shall not provide custodial services under this chapter in a manner that would likely impair the solvency or the safety and soundness of the bank, as determined by the Commissioner after considering the nature of custodial services customary in the banking industry.

(h) A bank may act as a fiduciary or trustee while providing custodial services or may provide custodial services on a purely contractual basis.

(j) A special purpose depository institution, as chartered under W.S. 13-12-101 through 13-12-126, may, based on customer instructions consistent with this section, undertake all transactions specified under subsection (e) of this section while providing custodial services. Consistent with W.S. 13-12-103(b) and (c) and section 3, 2019 Wyoming Session Laws, chapter 91, the lending prohibition in W.S. 13-12-103(c) shall not apply to custodial services provided by a special purpose depository institution as a result of the customer assuming all risk of loss for custodial service transactions. This prohibition is intended to ensure the solvency of the special purpose depository institution's banking business, as defined in W.S. 13-1-101(a)(ii).

(k) A bank may execute all components of a transaction within the bank or as otherwise agreed by the bank and the customer if that execution is in the best interests of the affected customer. Unless a bank and a customer have entered into an agreement for transactions to be executed with a specific person or by the bank, the bank shall provide best execution and seek the most favorable terms for the contemplated transaction reasonably available under the circumstances. A bank may tailor execution based on the nature of the legal relationship with the customer. Public availability of pricing shall adhere to existing securities or commodities market practices for banks. Best execution shall not require that the lowest possible commission be obtained or be executed within a set period of time different from customer instructions. Banks shall establish procedures to evaluate and demonstrate that transactions are executed in accordance with these rules and customer instructions using the following standards:

(i) The selection of a person to complete a transaction, as well as all aspects of the transaction, shall comply with federal and state standards and, as reasonably possible, industry best practices. For purposes of this subsection, "person" may include broker-dealers, digital asset exchanges or digital asset lenders; and

(ii) Banks shall conduct reasonable research, under the circumstances, regarding best price, speed of execution, certainty of execution, counterparty risk, security practices, conflicts of interest, recordkeeping capabilities and the commission rate or spread.

(l) Banks shall provide custodial services for customer funds consistent with safe and sound banking practices, and as otherwise required by applicable securities or commodities laws.

(m) As an incidental activity, a bank may provide non-custodial key management services, including key services for multi-signature arrangements and smart contracts, transaction verification, signature services, oracle functions, dispute or emergency resolution and other services incidental to multi-signature arrangements or smart contracts which may be performed by a trusted third-party. A bank which provides such non-custodial key management services under this paragraph shall not be considered to have custody of an asset.

(n) A bank may provide safekeeping services for a device containing digital asset private keys. Unless otherwise agreed to by the bank, the bank shall not have a duty to provide power and monitoring services relating to the device.

(o) A bank may issue, use or participate in innovative payment instruments and networks, including independent node verification networks and stablecoins, consistent with applicable law and safe and sound banking practices.

Section 5. Customer Protections; Requirements for Customer Agreements.

(a) A bank and a customer shall agree in writing regarding the source code version the bank will use for each digital asset, and the treatment of each asset under the Uniform Commercial Code, title 34.1, Wyoming statutes, if necessary. Any ambiguity under this subsection shall be resolved in favor of the customer.

(b) A bank may periodically determine whether to implement a source code version that uses block validation rules different than those of the source code version specified in the customer agreement under subsection (a) of this section, including in circumstances where is not possible to predict in advance whether utilization of the different source code version will be in the best interests of the customer. Additionally, the nature of proposed changes to source code versions from time to time may require the bank to consider the potential effects resulting from third-party actors (a person not a party to the agreement between the bank and its customer), who may create different source code versions resulting in new networks that could create economic value for the customers of the bank. Banks shall not be required to support digital assets and source code versions which the bank has not entered into an agreement with customers to support. Banks shall not capriciously redefine the digital assets under their custody, and the Commissioner shall have discretion to determine whether a redefinition is capricious. In communicating with customers regarding the situations set forth in this subsection, banks shall have a duty to provide higher standards of customer notice and acknowledgement if there is likely to be a material impact on the economic value of the customer's digital asset. Customer agreements and notifications shall clearly describe the consequences of hard forks without replay protection, as required by the Commissioner, and how that may cause the transfer of assets that were previously in bank custody without explicit instructions to the bank, accounting for the fact that some forks allow valid transactions from another distributed ledger to also be valid on the fork. In the event of a replay protection attack by a new hard fork, the bank may pause withdrawals and investigate appropriately. As used in this paragraph, "replay protection" means, in the case of a digital asset fork, the ability to duplicate a transaction made on one fork of a distributed ledger to another fork. When changes to source code versions occur that use different block validation rules than those of the source code version specified in the customer agreement, the following customer notice and acknowledgement rules shall apply:

(i) If the bank chooses not to continue to support the original source code version agreed upon with the customer pursuant to subsection (a) of this section, it shall receive written affirmative consent from the customer as provided in this paragraph. Notice and affirmative consent are only required under this paragraph when the conditions in subparagraphs (A) through (C) occur:

(A) The bank seeks to implement a source code version that uses a consensus rule that differs from the original, as defined by the source code version specified in the customer agreement pursuant to subsection (a) of this section;

(B) The bank will not continue support for the original source code version; and

(C) The original source code version continues to exist, or is reasonably expected to continue to exist.

(D) The following examples apply to this paragraph:

(I) A hard fork of virtual currency "B" created a new source code version, "New B." Consequently, if a bank stopped supporting B but did choose to support

New B, then the notice and affirmative consent requirements of this subsection would apply. For illustrative purposes, "New B" and "B" could be considered as similar to the virtual currencies "Bitcoin Cash" and "Bitcoin," respectively.

(II) A hard fork of virtual currency "E" created a new source code version, "New E," and followed the block validation rule change contained in the newly created source code version. The original source code version of E did not change but was renamed "E-Classic" and continued to follow the original block validation rules. Consequently, if a bank supported New E but no longer supported E-Classic, then the notice and affirmative consent requirements of this subsection would apply. For illustrative purposes, "New E" and "E-Classic" could be considered as similar to the virtual currencies "Ethereum" and "Ethereum Classic," respectively.

(ii) If the bank continues to support the original source code version agreed upon with the customer pursuant to subsection (a) of this section, and the bank seeks to implement a source code version that uses a consensus rule that differs from the original, the bank shall make reasonable efforts to inform the customer, as provided in this paragraph. Notice under this paragraph is only required when all of the following occur:

(A) The bank seeks to implement a source code version that uses a consensus rule that differs from the original, as defined by the source code version specified in the customer agreement pursuant to subsection (a) of this section;

(B) The bank will continue to support the original source code version specified in the customer agreement pursuant to subsection (a) of this section; and

(C) The original source code version continues to exist, or is reasonably expected to continue to exist.

(iii) If the original source code version no longer exists, or is not reasonably expected to continue to exist, the bank shall make reasonable efforts to inform the customer regarding source code changes from the original source code version agreed upon with the customer pursuant to subsection (a) of this section, as provided in this paragraph. Notice under this paragraph is only required when all of the following occur:

(A) The bank seeks to implement a source code version that uses a consensus rule that differs from the original, as defined by the source code version specified in the customer agreement pursuant to subsection (a) of this section;

(B) The bank will not continue to accommodate the source code version specified in the customer agreement pursuant to subsection (a) of this section; and

(C) The original source code version no longer exists, or is not reasonably expected to continue to exist.

(iv) In all other circumstances, the bank shall make reasonable efforts to notify the customer regarding source code version changes and act in a manner that the bank reasonably believes will be of economic benefit to the customer.

(v) Notice requirements under this subsection shall not apply to security vulnerabilities or other emergencies, as reasonably determined by the bank. After a source code version change relating to a security vulnerability or other emergency which would affect block validation rules, the bank shall provide written notice of the change to each customer as soon as practicable to minimize the security risk to customer assets.

(vi) In the case of customers who have not maintained current contact information with the bank, a bank shall be deemed to meet the notice requirement if it provides notice through its website and other media routinely used by the bank.

(c) As applicable, the bank shall provide customers with clear notices of the following:

(i) The heightened risk of loss from transactions under subsections (d) and (e) of section 4. For asset pooling arrangements, including proof-of stake digital assets, masternodes or similar arrangements, a bank shall additionally describe the security measures the bank will undertake to manage risk of loss;

(ii) That some risk of loss as a pro rata creditor exists as the result of custody as a fungible asset or custody under paragraph (c)(ii) of section 4;

(iii) That custody under paragraph (c)(ii) of section 4 may not result in the digital assets of the customer being strictly segregated from other customer assets; and

(iv) That the bank is not liable for losses suffered as the result of transactions under subsection (e) of section 4, except for liability consistent with the bank's fiduciary and trust powers.

(d) A bank and a customer shall agree in writing to a time period within which the bank must return a digital asset held in custody. If a customer makes an election under paragraph (c)(ii) of section 4, the bank and the customer may also agree in writing to the form in which the digital asset shall be returned.

(e) All ancillary or subsidiary proceeds relating to digital assets held in custody, commonly known as forks, airdrops, staking gains or similar proceeds from offshoots, including interest, shall accrue to the benefit of the customer, except as specified by a written agreement with the customer. The bank may elect not to collect certain ancillary or subsidiary proceeds, as long as the election is disclosed in writing. A customer who makes an election under paragraph (c)(i) of section 4 may withdraw the digital asset in a form that permits the collection of the ancillary or subsidiary proceeds.

(f) A bank shall enter into a written agreement with a customer, if desired by the customer, regarding the manner in which to invest ancillary or subsidiary proceeds or other gains attributable to digital assets held in custody.

(g) A bank shall not authorize or permit rehypothecation of digital assets under its custody. The bank shall not engage in any activity to use or exercise discretionary authority relating to a digital asset except based on customer instructions.

(h) To promote legal certainty and greater predictability of digital asset transactions, a bank and a customer shall define in writing the terms of settlement finality for all transactions, as specified by subsection (j) of this section. The following components apply to all such agreements unless the parties contract otherwise:

(i) Wyoming law applies to all transactions and the venue for disputes is in the courts of Wyoming;

(ii) Transactions are deemed to have occurred in Wyoming, consistent with W.S. 34-29-103(g); and

(iii) Digital assets are deemed to be located in Wyoming, consistent with W.S. 34-29-103(g).

(j) Agreements entered into between a bank and a customer relating to settlement finality under subsection (h) shall also address the following issues:

(i) The conditions under which a digital asset may be deemed fully transferred, provided that these legal conditions may diverge from operational conditions under which digital assets are considered transferred, owing to the distributed and probabilistic nature of digital assets;

(ii) The exact moment of transfer of a digital asset; and

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

Section 6. Standard of Custodial Services.

(a) If a bank is subject to the requirements of the United States Securities and Exchange Commission's "Customer Protection Rule" for digital securities as specified by 17 C.F.R. 240.15c3-3, as incorporated by reference on July 1, 2019, the bank may be considered to have satisfied the requirement for a satisfactory control location if the bank has control of the digital security, consistent with supervisory manuals adopted by the Commissioner.

Section 7. Risk Management and Operations.

(a) In conducting supervision activities, the Commissioner shall determine whether a bank providing custodial services under this chapter has adequate systems in place to identify,

measure, monitor and manage risks. Such systems include policies, procedures, internal controls and management information systems governing custodial services.

(b) A bank shall have a clearly documented and audited operational risk management program. The program shall include the following:

(i) Developing strategies to identify, assess, monitor and manage operational risk;

(ii) Defining procedures concerning operational risk management;

(iii) Defining an operational risk assessment methodology; and

(iv) Managing a risk reporting system for operational risk.

(c) If an incident occurs relating to a breach of the operational risk management program, a report shall be prepared by an officer of the bank documenting the following:

(i) Known causes, if any, of the incident;

(ii) Impact of the incident;

(iii) A timeline of the incident, including duration of time to resolve the incident; and

(iv) Corrective action, if necessary.

(d) The report under subsection (c) of this section shall be disclosed to all officers of the bank, senior employees and the Board of Directors, and referenced for future revisions to the operational risk management procedure. In the event an incident results in revisions or additions to these procedures, the officer in charge of operational risk management shall establish a timeline for complying with the necessary changes and shall document compliance in a timely manner.

(e) Operational risk management procedures shall be revisited on a recurring basis by the bank to ensure all reasonably foreseeable scenarios have been considered. A bank shall demonstrate that its scope of scenario planning has taken into consideration current industry risks and practices and reflects possible high-severity and plausible risks. Scenario planning should also be undertaken with consideration of the bank's contingency planning and business continuity plans.

(f) At all times, a bank shall have in place a business continuity plan based on the following:

(i) Personnel redundancy;

(ii) Standards for triggering the business continuity plan;

(iii) Procedures to mitigate operational impacts or transfer operational functions;

(iv) An alternate site location sufficient to recover and continue operations for a reasonable period of time. A bank should be able to demonstrate that the alternate site has appropriate distance between it and the primary custody location to mitigate environmental and technical interruptions at both sites and which adheres to all criteria of these rules; and

(v) A recovery plan for the restoration of normal operations after interruption.

(g) A bank shall adopt procedures for providing customers with perpetual access to all digital assets in custody in the event the bank ceases to operate or cannot fulfill its custodial services agreement. This may include a formal disbursement or custody transfer process. This requirement may be satisfied by the adoption of a recovery or resolution plan by a special purpose depository institution.

Section 8. Business Requirements.

(a) A bank providing custodial services under this chapter shall have verified mechanisms in place to assess its liquidity needs, including sums required for the execution of transactions. These mechanisms shall inform the bank's customer private key storage policy for custodial services. Unless otherwise demonstrated to be no longer best practices:

(i) The customer private key storage policy should require that the method of digital asset storage (e.g., hot versus cold storage) be conducted on a risk-focused basis; and

(ii) The mechanism and thresholds for transfer between hot, cold and other forms of storage must be well documented and subject to rigorous internal controls and auditing. To ensure sufficient liquidity and the protection of customer assets, a bank shall be able to timely execute a withdrawal of all digital assets.

(b) As a component of the bank's private key storage policy under subsection (a) of this section, a bank shall take into account its ability to obtain insurance or other forms of risk mitigation.

(c) A bank may generate a new data address, as defined in W.S. 17-16-140(a)(xlvii), for each transaction to ensure a customer's privacy, security and confidentiality. Before adopting such a policy, a bank shall consider potential business cases where traceability of address activity is desirable, especially to ensure compliance with federal customer identification, anti-money laundering, sanctions and beneficial ownership requirements. A bank shall exercise appropriate judgment in determining a data address strategy based on the use case of its customers.

(d) Each digital asset type may have a different protocol for its wallet functionality. Regardless of protocol differences, a bank shall demonstrate its ability to manage a similar level of compliance related to safekeeping, recording and transaction handling. A bank shall demonstrate compliance with the standards outlined in these rules for every asset type in its custody.

(e) A bank shall develop a protocol for fraud detection and adherence to federal customer identification, anti-money laundering, sanctions and beneficial ownership requirements. This should include a detection system for identifying suspicious transactions as well as a procedure for reviewing and reporting identified transactions.

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

(g) A bank shall have established roles and responsibilities for custodial service operations and custody operational risk management. Responsibility for manually executed (non-automated) core functions of custodial services should be performed by employees who have been subject to appropriate background screenings.

(h) A bank shall provide industry-leading information technology security training on a regular basis to all employees and monitor its employees compliance with established procedures. This training shall include potential attacks that are specifically applicable to digital assets. Two training programs may be produced, one for information technology staff and one for non-information technology staff.

(j) A bank shall have appropriate numbers of staff who are trained and competent to discharge their duties effectively. The bank shall ensure that the responsibilities and authority of each staff member are clear and appropriate given the staff member's qualifications and experience, and that staff members receive the necessary training appropriate for their respective roles.

(k) A bank shall review and document the adequacy of its training programs at least annually, along with any relevant elements after the occurrence, or near occurrence, of material risk incidents. Policies and procedures must also provide for appropriate disciplinary measures for employees who violate policies and procedures.

(l) For any outsourced services or integrated partnerships, a bank shall demonstrate that proper due diligence was done in vetting the partner, whether an affiliate, vendor or supplier, regarding information security, operational risk and financial solvency. Although a bank may outsource such services, responsibility for compliance with applicable laws and rules shall remain with the bank. A bank shall also have sufficient governance mechanisms in place to monitor the outsourced party's continued compliance. To the extent possible under this chapter, bank policies on outsourcing or partnerships shall be consistent with the bank's existing processes for outsourcing or partnerships.

(m) A bank shall regularly assess the risk of information technology systems or software integrations with external parties, particularly as they relate to the risk of malicious intrusion, unauthorized access or theft of customer assets in custody, and ensure that appropriate safeguards are implemented to mitigate the risk. A bank shall engage a qualified, independent third party to conduct penetration testing annually. Results of such penetration tests shall be documented and retained for at least five years in a manner that allows the reports to be provided to the Commissioner upon request.

(n) For any third-party supplier of equipment that enables core functions of custodial services (e.g. steel storage, cold storage wallets, etc.), a demonstrated redundancy strategy shall exist that allows the bank to maintain service level agreements in the event of primary equipment or supplier failure.

(o) A bank shall provide to the Commissioner written verification that assets under custody carry appropriate insurance or other financial protections, as determined by the Commissioner, to cover or mitigate potential loss exposure.

(p) A bank shall maintain documented policies and procedures related to customer identification, anti-money laundering, sanctions and beneficial ownership requirements, which shall be as reasonably consistent as possible with existing processes, for both jurisdiction and asset types. A bank shall comply with all applicable federal laws relating to anti-money laundering, customer identification, sanctions and beneficial ownership, which may include enhanced compliance measures or procedures necessary to comply with these laws. A bank shall, upon request by the Commissioner, demonstrate its protocols for compliance with these laws, including its practice of new customer identity verification process as well as any required ongoing screenings and transaction-specific screenings.

(q) A bank shall comply with the following requirements:

(i) If applicable, a bank shall provide customer account statements as required by 17 C.F.R. § 275.206(4)-2(a)(3), as incorporated by reference on July 1, 2019, including a timeframe of statement activity, all digital asset transactions specific to each account with dates and transaction amounts of corresponding transactions, balances for each type of digital asset and valuation of assets for each digital asset type, including the method used to create the valuation, consistent with subsection (f) of section 8.

(ii) Disclose all service level agreements for custodial services to customers; and

(iii) Disclose its responsibilities with respect to processing of corporate actions, pricing assets, providing recordkeeping, reporting services, fund administration, performance measurement, risk measurement and compliance monitoring.

(r) Consistent with W.S. 34-29-104(c), regular examinations of both customer currency and digital assets shall be completed by an independent public accountant if required.

Any examination shall include, if feasible, independent and cryptographically verifiable control of all digital assets under custody or a random sample selected by the auditor. A proof of reserve scheme may be used, if feasible, but only if customer privacy is protected by disclosing the total balance, data addresses or keys to the independent public accountant on a confidential basis. The examination conducted by the independent public accountant under this subsection shall proceed as follows, unless otherwise directed by the Commissioner for good cause:

(i) A bank shall provide the independent public accountant with all public data addresses used and shall sign messages demonstrating possession or control of private keys for those addresses. A hash of the most recent block of an agreed-upon distributed ledger at the time of signature shall be included in the signed message in order for messages to serve as a timestamp for when the signature was made. The signatures of those shall be verified by the accountant. The accountant shall use the distributed ledger to extract the total amount available at those addresses at a certain point in time;

(ii) The accountant shall determine to his satisfaction that a bank has control of the public data addresses provided in the signed message by requiring a signed message of the accountant's choosing using the private key to any of the public addresses provided by a bank. A bank shall not provide the accountant with a private key to any digital asset under custody;

(iii) A bank shall provide the digital asset balances, per asset, of each customer to the accountant and generate a Merkle tree, or in the determination of the Commissioner, any substantially similar analogue. The accountant shall publicly publish the root node hash, and affirm if true, that the total holdings represented by the root hash closely approximates the value that the accountant has verified in the wallet of the bank relating to the distributed ledger. The accountant shall ensure that the bank is not attempting to obfuscate or conceal material issues in the nodes that lead to the root node; and

(iv) A bank shall provide customers with the digital asset balances reported to the accountant, as well as the nodes and adjacent nodes from their account to the root which matches the root node hash published by the accountant. A bank shall disclose the hashing method used to generate the hash for the bank's node to customers, so that customers can verify that the node accurately represents the balance that is claimed, enabling customers to independently prove that their account was included in the data verified by the independent public accountant.

(s) The Commissioner may conduct an examination of custodial services provided by a bank at any time, with or without notice to the bank.

(t) A bank shall designate a method for the public to responsibly disclose critical vulnerabilities or other potential exploits and security risks by protocol developers. A bank shall designate at least one employee to be responsible for handling inbound communication regarding critical security vulnerabilities or other security sensitive matters.

Section 9. Technology Controls and Custody Safekeeping.

(a) Consistent with this section, procedures shall be in place to ensure digital assets are securely created, stored and maintained to ensure uninterrupted availability appropriate for the circumstances.

(b) If applicable, a seed relating to a digital asset shall be created using a National Institute of Standards and Technology (NIST) compliant deterministic random bit generator, secure non-deterministic key generation mechanism, or other method approved by the Commissioner. A bank shall create safeguards in the seed and subsequent key generation process that demonstrates resistance to supposition and potential collusion. The seed or private key shall have, as a minimum, random sequence 256-bit entropy. The result shall be at least a 256-bit entropy input that is encoded into a mnemonic phrase. A bank shall then utilize a hashing function to generate a 512-bit value. Unless determined by the Commissioner not to be feasible in a particular instance, a bank shall use a passphrase as part of a seed which can be used as an additional measure of security and leveraged as a defense in brute force attacks, if the bank chooses to use mnemonic seed word phrases. The phrase referenced in this subsection shall be considered the backup seed because it can be utilized to regenerate a seed.

(c) A bank shall utilize at least three officers or employees to perform the process of creating entropy in the creation and production of the seed, with no single person ever possessing the entirety of the seed, private key or backup mnemonic word phrase. When a private key or single seed is produced for a signatory, the signatory shall not be involved in the production of the public and private keys. None of the seed, private key or entropy creators shall be permitted to participate in the act of cryptographically signing or have access to the systems that enable malicious activity.

(d) A bank shall comply with an industry-standard method of generating asymmetric private and public key combinations. Permissible industry-standard methods include those established by NIST.

(e) A bank shall have in place secure deletion and destruction mechanisms to ensure unwanted artefacts from seed, key and wallet generation, consistent with industry best practices.

(f) A bank shall adopt industry best practices utilizing strong encryption and secure device storage for customer private keys that are not in use. A bank shall ensure the keys stored online or in any one physical location are insufficient to conduct a digital asset transaction, unless appropriate controls are in place to render physical access insufficient to conduct a transaction. Key/seed backups shall be stored in a separate location from the primary key/seed.

(g) Key/seed backups shall be stored with strong encryption equal or superior to that used to protect the primary key. The key/seed backup shall be protected by access controls to prevent unauthorized access. For the storage of critical seeds, keys and key parts relating to the internal core cryptographic systems, hardware security modules that are at least Federal Information Processing Standard 140-2 Level 3 certified shall be used, or any other means which provides equal or superior protection, as determined by the Commissioner.

(h) If applicable, a bank shall ensure that once a mnemonic backup seed phrase has been generated, it is broken into at least two or more parts. A bank shall ensure that a sufficient number of backup seed phrases that could be used to facilitate a transaction are not stored within any single point of access.

(j) A bank shall use physical storage facilities which are appropriate for the risk profile of the bank. A bank shall ensure that all physical storage areas in use are monitored on an uninterrupted basis and shall include reinforced vaults equipped with alarms, locks, and other appropriate security devices and be resistant to fire, flood, heat, earthquakes, tornadoes and other natural disasters. Access to the physical storage facility shall be limited to authorized persons through multifactor identity verification, which shall be annually verified by the independent public accountant, consistent with industry best practices.

(k) A bank shall ensure that a regular and recurring internal audit of backup seeds is performed on storage devices to ensure that no backups were modified, copied or removed. The audit shall occur no less than quarterly. All audits of seeds and subsequent results shall be well documented, with any risk incidents noted and necessary corrective action taken. All audit records shall be retained for at least five years in a manner that can be made available to the Commissioner upon request.

(l) A bank shall develop a documented protocol in the event there is reasonable belief that a wallet, private key or seed is compromised or subject to a security risk. The protocol shall be protected against adverse events including, but not limited to, the compromise of the whole seed, partial seed or a key derived from a seed, or any other potential security risk. In this event, if the underlying seed is believed to be compromised or at risk, the bank shall create a new wallet and migrate the digital assets. If a key is compromised or is at risk, a risk event shall be documented and investigated.

(m) Strict access management safeguards shall be in place to manage access to keys. Upon departure of a signatory from employment that had access to a wallet key or multi-signature arrangement key, a formal assessment shall be conducted to determine whether a new key ceremony and accompanying migration of digital assets is required. An audit trail shall record every change of access including who performed the change.

(n) A bank shall adopt procedures for the immediate revocation of a signatory's access. Key generation shall be performed in a manner in which a revoked signatory does not have access to the backup seed or knowledge of the phrase used in the creation. All keys shall be encrypted in a manner preventing a compromised signatory from recovering the seed. Procedures shall follow the standard protocol around removing user access without the need to create a new wallet. Quarterly internal audits shall be performed by the bank on the removal of user access by reviewing user access logs and verifying access as appropriate. A bank shall have a written checklist/procedure document that is followed for on- and off-boarding of employees. The checklist shall outline every permission to grant/revoke for every role in the bank's key management systems. All grant and revoke requests must be made via an authenticated communication channel which was transmitted using an encrypted protocol.

(o) A bank may place digital assets in an omnibus account if the customer elects a custodial relationship under W.S. 34-29-104(d)(ii) and paragraph (c)(ii) of section 4, consistent with federal law and industry best practices. Proper accounting shall be in place to accurately allocate each digital asset to a customer. The bank shall document and implement measures to demonstrate that the level of security achieved is commensurate with custody under W.S. 34-29-104(d)(i) and paragraph (c)(i) of section 4.

(p) For cold storage of digital assets, a bank shall have physical security that requires at least two authorized key holders with security badges and at least two of the following multi-factor authentication methods:

(i) Personal knowledge, which shall include login credentials;

(ii) A tangible device or computer program, which shall include a hardware or software token or access card; or

(iii) Biometric data, which shall include fingerprints or eye scans.

(q) Physical security under subsection (r) of this section shall also include:

(i) Segmented access safeguards from primary workspaces;

(ii) A facility access logging system which maintains access records and security camera video for a minimum of one year on-site and for three years at an off-site location;

(iii) Security cameras which are hardened against attack and clearly show the entire body of a person upon access in and out of the vault; and

(iv) Documentation and use of principles of least privilege when assigning access controls. This documentation shall be made available to the Commissioner upon his request.

(r) A bank shall have procedures for required actions, customer notifications and notifications to the Commissioner in any situation whereby the bank has a reasonable belief that a digital asset under custody has been compromised or is subject to a security risk. These procedures shall be reviewed and audited annually and may include a velocity limit, freeze or circuit breaker actions designed to protect digital assets in an emergency.

(s) Within twenty-four (24) hours of forming a reasonable belief that any act has occurred that resulted in, or is likely to result in, unauthorized access to, disruption or misuse of the bank's electronic systems or information stored on such systems, a senior officer of the bank shall provide the following information to the Commissioner:

(i) The nature of the incident, including the categories and approximate number of digital assets involved;

(ii) The time of the incident;

(iii) An identification of the means by which the incident is likely to have occurred;

(iv) A description of the likely consequences of the incident, including any communications to customers which have been sent or are planned by the bank; and

(v) A summary of all mitigation actions the bank has taken in response to the incident.

(t) Within fourteen (14) days of a notification to the Commissioner under subsection (s) of this section, the senior executive shall furnish the Commissioner with a written report establishing all of the available details of the incident, as required by the Commissioner. The incident report shall also contain a root-cause analysis and impact analysis.

Section 10. Transaction Handling.

(a) To ensure that all transactions are subject to appropriate safeguards, a bank shall put in place secure and trusted measures to prevent fraud. Transactions shall be recorded in system audit records.

(b) A bank shall consider the use of multi-signature arrangements, as defined in W.S. 34-29-103(e)(ii), in all appropriate transactions. The Commissioner may require a bank to use multi-signature arrangements in specific situations.

(c) All individuals with authorized access to any secured location or system shall utilize individually named accounts to allow for auditing of access. Where a bank has various multi-signature arrangement procedures that vary depending on the risks of the transaction, including the value of a transaction, type of wallet risk, type of customer, the procedures of the bank shall be well-documented and audited.

(d) A bank shall adopt a method for managing a signing process that prevents a quorum of individuals from acting in bad faith to collude or manipulate automated systems. This may be achieved by separation of duties of different quorums over different subsystems, but does not require that quorums must not be used to protect individual subsystems. The bank shall use a system in which customer instructions for transactions may be authenticated or verified as genuine, and subsequently audited, to reduce the risk of theft and collusion. The risk of collusion and other malicious acts shall be addressed as part of recurring operational risk assessments. Collusion mitigation may be accomplished in the following ways:

(i) Safeguards including oversight and/or separation of duties that prevent a linear ability to create, approve, sign transactions and broadcast to distributed ledger networks;

(ii) Use of automated systems to create, approve, sign transactions and broadcast to distributed ledger networks;

(iii) Distribution of signatories with differing incentives, including customers, custodians, trustees, other financial institutions, counterparties, and other third parties;

(iv) Concealment of the identities of signatories among each other; and

(v) Rotation of signatories, signing times or signing locations.

(e) For a transaction, each signatory shall record their reasoning or evidence for the decision to authorize or reject the transaction. Reasoning or evidence to approve or reject a transaction shall be based on a set procedure and determined with the same diligence and with the same required information for each occurrence, without regard to customer identity or transaction value unless otherwise approved by the Commissioner. Transaction reasoning or evidence under this subsection shall be retained and available for review upon request by a customer, with a chain of custody evidencing every access attempt, but which may not disclose actual employee identities. The following shall also apply:

(i) The reasoning or evidence required for each signatory to prove true in order to authorize a transaction shall be contractually agreed upon by all signatories in the customer agreement. In the event approval signing and transaction signing are abstracted, transaction approvers shall have access and appropriate expertise to evaluate required reasoning or evidence prior to an authorized signing ceremony;

(ii) Each approver or signatory shall be required to provide proof of the evidence referenced for an authorization;

(iii) Each transaction and signature action associated with a transaction shall have a specific time duration tracked against each option for any transaction where the conditions of the evidence are time-based;

(iv) A bank shall store all reasoning or evidence internally and the evidence shall be reviewed at multiple levels within a transaction. A minimum of four separate individuals shall perform reviews around a specific request. Evidence shall be collected based on a set checklist of necessary documentation based on the role the signatory is representing. A bank shall establish safeguards around the processes that shall be evaluated on a periodic basis and adjusted as necessary;

(v) A bank shall maintain a full audit trail of all transaction activities. A bank shall conduct timely reconciliation of all transactions in its records. This includes specific information about each transaction, including the:

(A) Date and time of transaction;

(B) Transaction event type;

(C) Jurisdiction in which the customer is located;

(D) Relevant signatories; and

(E) Account balances and the value of the transaction.

(f) Each quarter, a bank shall extract a sample of transactions for internal audit in order to ensure that internal processes are functioning in conformity with established procedures. Banks shall take corrective action as needed in the event faults are discovered. Safeguards shall be in place to ensure that records and audit trails cannot be changed.

(g) A bank shall maintain a detailed policy covering data sanitization requirements, procedures and validation steps for every media type used by the bank. The bank shall inform officers and employees of how data may remain on digital media after deletion, how to securely wipe data and when secure wiping should be used.

Section 11. Custody Operations.

(a) A bank shall ensure that information technology operational safeguards are subject to industry best practices to ensure a secure and stable custody operating environment is in place. These safeguards shall include the following:

(i) A bank shall ensure that technology measures consistent with industry best practices are in place to protect all systems, which may include "defense in depth." A bank may adopt the ISO 27001 information technology standard, but if the bank chooses not to adopt this standard, it shall implement as many components of this standard as appropriate. The Commissioner may require the adoption of additional technology safeguards or standards. Particular rigor shall be applied to ensure that all internet-facing systems are hardened and secure; and

(ii) Access to systems and data shall only be granted to individuals with a demonstrated business need that cannot be achieved through other means. Safeguards shall be in place to ensure identification, authorization and authentication of the individual. A current list of access rights shall be maintained along with documented procedures for assigning and revoking access privileges. A log of all access changes shall be maintained to demonstrate proof of proper access rights management.

(b) A bank shall perform the following:

(i) Internal information technology security testing of both infrastructure and applications on a regular basis;

(ii) At least annually, penetration tests by an independent and qualified testing company. Any new internet facing services or significant changes to existing services shall be subject to internal penetration testing and hardened before being presented online as live services;

(iii) At least quarterly, internal system vulnerability audits; and

(iv) At least monthly, external system vulnerability audits.

(c) Decentralized applications shall be subject to a software development life cycle based on industry best practices.

(d) Proof of tests and audits conducted under subsection (b) of this section and corresponding results shall be documented and made available in an examination conducted by an independent public accountant or the Commissioner. Testing and audits shall include participation by both employees and external parties. Banks shall ensure external parties have a key role in testing and audits. Testing standards shall adhere to best industry practices. Recurring testing and audits under subsection (b) shall include:

(i) Wallet integrity audits;

(ii) Key and seed generation procedures;

(iii) Completed transactions, to ensure compliance of proof of evidence protocols;

(iv) Suspicious transaction handling;

(v) Migration of storage devices, including cold to hot storage; and

(vi) Random verification of digital asset balances and control of digital assets.

(e) A bank may, in its discretion, employ risk mitigation tools designed to automate a core function, including transaction signatures that have received and passed a demonstrated risk assessment performed by a qualified third party. Corresponding operational risk procedures shall be documented. The bank shall implement risk monitoring mechanisms to identify failures in automation if they occur.

Section 12. Digital Asset Lending Based on Customer Instructions.

(a) Based only on customer instructions and authority, consistent with W.S. 34-29-104 and section 4 of this chapter, a bank may undertake digital asset lending. Digital asset lending shall exclude rehypothecation of digital assets, consistent with W.S. 34-29-104(k) and subsection (g) of section 5 of this chapter.

(b) Digital asset lending shall be restricted solely to the department of the bank providing custodial services and shall not extend to any other functions of the bank which are not required for custodial services.

(c) Bank-owned assets or customer depository accounts shall not be involved in digital asset lending, except that the bank may accept deposits of customer funds related to digital asset lending.