Vaults as Qualified Custodians

A Joint White Paper · June 2026

Vaults as Qualified Custodians

Chris Brummer* **and TuongVy Le†**

Abstract

The SEC custody rule should be understood functionally: its central object is not to privilege a particular institutional form, but to protect client assets against misappropriation, commingling, insolvency exposure, fabricated reporting, and unchecked adviser control. The qualified-custodian requirement is the rule's principal mechanism for achieving those ends in traditional markets. It should not be treated as the only possible mechanism in digital-asset markets.

Properly designed on-chain vault architecture, paired with continuous verification infrastructure, can perform the core functions the custody rule assigns to qualified custodians. A vault that eliminates unchecked withdrawal authority, enforces asset segregation, makes governance transparent, undergoes independent security review, supports continuous verification, and maintains examiner-accessible records can provide a live, cryptographically verifiable account of asset existence, ownership, backing, authority, and control. In that respect, it can do more than replicate the periodic assurances of legacy custody; it can make the protective facts of custody continuously observable.

Table of Contents

* Chris Brummer is the Chief Executive Officer of Bluprynt and Agnes Williams Sesquicentennial Professor of Financial Technology at Georgetown University Law Center.
† TuongVy Le is General Counsel of Veda. Ms. Le served in the SEC's enforcement unit for over a half a decade before joining private practice. We would like to thank Robert Greenfield, Juan Carlos León Villarreal, and Professor Yesha Yadav for their expert comments and substantive input.

Executive Summary

Custody is one of the core concepts of securities markets. It addresses the risks that arise when an investor relies on another person or arrangement to safeguard assets, maintain authoritative records, or administer access to them. Whether assets are represented by paper certificates, book entries, or digital records, the regulatory problem is fundamentally the same: how to protect the investor's interest when the integrity and availability of the assets depend, at least in part, on systems or actors other than the investor. Custody regulation has therefore long operated as a substitute for trust—using segregation, recordkeeping, account statements, independent verification, and regulatory examination to ensure that client assets are present, properly accounted for, protected from misuse, and available to the investor.

The SEC custody rule should be understood against that background. Its central object is not to privilege a particular institutional form, but to protect client assets against misappropriation, commingling, insolvency exposure, fabricated reporting, and unchecked adviser control. The qualified-custodian requirement is the rule's principal mechanism for achieving those ends in traditional markets. It should not be treated as the only possible mechanism in digital-asset markets.

Properly designed on-chain vault architecture, paired with continuous verification infrastructure, can perform the core functions the custody rule assigns to qualified custodians. A vault that eliminates unilateral withdrawal authority, enforces asset segregation, makes governance transparent, undergoes independent security review, supports continuous verification, and maintains examiner-accessible records can provide a live, cryptographically verifiable account of asset existence, ownership, backing, authority, and control. In that respect, it can do more than replicate the periodic assurances of legacy custody; it can make the protective facts of custody continuously observable.

The regulatory question is therefore one of functional equivalence. Where a vault arrangement demonstrably protects against the harms the custody rule was designed to prevent, regulators should have a pathway to recognize that arrangement as a technology-native safeguarding mechanism. That pathway could take the form of staff guidance, conditioned no-action relief, a supervisory pilot, or rule modernization recognizing functionally equivalent safeguarding arrangements. Such recognition should be provider-neutral and standards-based. It should apply to any architecture that satisfies the required safeguards, not to any particular firm, protocol, or product. The aim is not to weaken custody regulation for digital assets, but to modernize it: preserving the custody rule's investor-protection objectives while recognizing that, for on-chain assets, those objectives may be achieved more directly through verifiable architecture than through traditional intermediation alone.

I. The Custody Rule: Origins, Objectives, and Evolution

The custody rule has evolved considerably from its roots, driven consistently by both crisis and technological development.

Rule 206(4)-2 under the Investment Advisers Act of 1940, commonly referred to as the Custody Rule, was promulgated pursuant to the Commission's authority, conferred by Section 206(4) of the Act, to define and prescribe means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, and courses of business by registered investment advisers.[1] Since its initial adoption on February 27, 1962, the rule has served a single, consistent protective objective: safeguarding client assets from misuse or

[1]Investment Advisers Act of 1940 § 206(4), 15 U.S.C. § 80b-6(4); Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-2176, 68 Fed. Reg. 56,692, 56,692 (Oct. 1, 2003) [hereinafter 2003 Adopting Release].

misappropriation by the adviser in whose custody they reside.[2] As the Commission stated directly in its 2002 proposing release, the rule "seeks to protect clients' assets in the custody of advisers from misuse or misappropriation."[3] Three specific hazards animate that objective—misappropriation of client funds, commingling of client and adviser assets, and exposure of client property to the adviser's insolvency—and every substantive amendment to the rule has returned to those three concerns as its touchstone.[4]

A. Origins and early development

The rule's original 1962 incarnation was, by contemporary standards, sparse: its adopting release ran to just three pages.[5] For more than four decades the Commission made no substantive amendments; instead, it issued a body of no-action and interpretive letters—approximately ninety in number—that clarified the rule's operation but, in doing so, created a layered interpretive overlay that the Commission itself would later describe as having "diminished the transparency of the rule's requirements."[6] During this extended period the rule's custodial standard was not one of prescribed intermediation but of reasonable safekeeping: it required, in essence, that client assets be maintained in a manner reasonably designed to prevent loss, destruction, or misappropriation, without mandating that they be entrusted to any particular category of financial institution.

B. The 2003 Amendments

That changed in 2003. In Release No. IA-2176, the Commission adopted comprehensive amendments designed, in its own words, to "modernize the rule by conforming the rule to modern custodial practices" and to require advisers with custody of client assets to maintain those assets with broker-dealers, banks, or other qualified custodians.[7] The Commission explained that the 1962 rule "was designed to operate in the securities markets of that time" and that, over the intervening decades, "custodial practices ha[d] changed" and "portions of the rule ha[d] become outdated."[8] Among the specific concerns prompting the change was the practice of advisers maintaining clients' stock certificates in their office files—precisely the kind of inadequate safekeeping the new qualified-custodian requirement was designed to foreclose.[9] Two points of lasting significance follow. First, the qualified-custodian requirement of 2003 was not a restatement of the rule's original purpose but a modernization of its operative mechanism—a translation of a decades-old reasonableness standard into the vocabulary of then-prevailing custodial infrastructure. Second, the Commission's stated rationale centered on conformity with contemporary practice, not on any independent

[2]Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-123 (Feb. 27, 1962); see also J. Robert Plaze, Regulation of Custodial Practices Under the Investment Advisers Act of 1940, at 1 (Proskauer Rose LLP 2020) (noting the rule was adopted "under newly-acquired authority to adopt rules to prevent fraud by investment advisers").

[3]Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-2044, 67 Fed. Reg. 48,579, 48,580 (Jul. 25, 2002) [hereinafter 2002 Proposing Release].

[4]See 2003 Adopting Release, supra note 1, at 56,692–93; Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-2968, 75 Fed. Reg. 1,456, 1,457 (Jan. 11, 2010) [hereinafter 2009 Adopting Release] (amendments designed to "prevent those assets from being lost, misused, misappropriated or subject to advisers' financial reverses").

[5]Plaze, supra note 2, at 1 ("The adopting release was three pages long.").

[6]2003 Adopting Release, supra note 1, at 56,692–93 (noting that "accumulated guidance in these no-action and interpretive letters . . . has diminished the transparency of the rule's requirements").

[7]2003 Adopting Release, supra note 1, at 56,692 (summary) ("modernize the rule by conforming the rule to modern custodial practices").

[8]2002 Proposing Release, supra note 5, at 48,580 ("We adopted rule 206(4)-2 in 1962 and the rule was designed to operate in the securities markets of that time"); accord 2003 Adopting Release, supra note 1, at 56,692–93.

[9]Securities and Exchange Commission, Press Release No. 2002-107, "SEC Proposes Changes in Investment Adviser Custody Rules" (Jul. 17, 2002) ("the proposed change is designed to prevent advisers from, for example, keeping clients' stock certificates in their office files").

determination that institutional intermediation was the sole legitimate means of achieving the rule's protective ends.

C. The 2009 Amendments

The rule's most recent substantive amendments came in 2009, in the immediate aftermath of the frauds perpetrated by Bernard Madoff and Allen Stanford—both of which resulted in criminal convictions—and a series of related Commission enforcement actions alleging misappropriation and misuse of client assets.[10] Those events prompted a significant strengthening of the independent-verification apparatus. Release No. IA-2968 required, among other things, that advisers with custody undergo annual surprise examinations by independent public accountants—which the Commission described as providing "another set of eyes" on client assets and "an additional set of protections against their misappropriation"[11]—and that the amendments were designed to "provide for a more robust set of controls over client assets designed to prevent those assets from being lost, misused, misappropriated or subject to advisers' financial reverses."[12] The 2009 amendments did not revisit the foundational qualified-custodian requirement itself; they reinforced the verification and notification architecture erected around it.

D. The present moment

More recently, the Commission has signaled, both implicitly and explicitly, that the custody rules warrant application to modern infrastructure. Explicitly, the Division of Investment Management's regulatory agenda states that it is considering amendments to modernize the custody framework for advisory client and fund assets, including crypto assets; and a custody-modernization discussion circulated in late 2025 has reportedly suggested that the rule's core tenets can be satisfied — and in some respects advanced — by technology-native safeguarding, on the view that blockchain systems already support transparent accounting, continuous auditability, and real-time reconciliation.[13] Implicitly, the Commission withdrew the 2023 Safeguarding Proposal in June 2025,[14] the staff has been reported to permit advisers to treat qualifying state trust companies as custodian banks for crypto, and, in March 2026, the Commission joined the CFTC in a Memorandum of Understanding and a related harmonization initiative that, among other things, commits the agencies to facilitating the exploration of alternative compliance frameworks.[15, 16] These

[10]2009 Adopting Release, supra note 6, at 1,456; Safeguarding Advisory Client Assets, Investment Advisers Act Release No. IA-6240, 88 Fed. Reg. 14,672, 14,673 (Mar. 9, 2023) ("The Commission most recently amended the rule in 2009 after several enforcement actions . . . including actions stemming from the frauds perpetrated by Bernard Madoff and Allen Stanford . . . alleging fraudulent conduct that included, among other things, misappropriation or other misuse of client assets.").

[11]2009 Adopting Release, supra note 6, at 1,461 ("to provide 'another set of eyes' on client assets, and thus an additional set of protections against their misappropriation").

[12]Id. at 1,458 ("provide for a more robust set of controls over client assets designed to prevent those assets from being lost, misused, misappropriated or subject to advisers' financial reverses").

[13]SEC regulatory agenda (Agency Rule List), announced Sept. 4, 2025 (listing the modernization of how registered investment advisers and funds custody and safeguard client assets, including crypto assets, among contemplated rulemakings). The further view that the rule's core tenets can be satisfied — and in some respects advanced — by technology-native safeguarding is advanced in a third-party submission to the Commission's Crypto Task Force, not by the Commission or its staff. *See* Written Submission to the SEC Crypto Task Force, *Custody Rule Modernization: A Model Framework for Crypto Asset Safeguarding* (Dec. 19, 2025), https://www.sec.gov/about/crypto-task-force/written-submission/custody-rule-modernization-model-framework-121925. It is cited to identify that position, not to attribute it to the Commission.

[14]Withdrawal of Proposed Regulatory Actions, 90 Fed. Reg. 25,531 (June 17, 2025) (Release No. IA-6885) (omnibus notice withdrawing fourteen proposed rules, including the Safeguarding Advisory Client Assets proposal, Safeguarding Advisory Client Assets, 88 Fed. Reg. 14,672 (Mar. 9, 2023) (Release No. IA-6240)).

[15] *Simpson Thacher & Bartlett LLP*, SEC No-Action Letter, Div. of Inv. Mgmt., Office of Chief Counsel (Sept. 30, 2025) (Evenson, Sr. Counsel).

[16]SEC-CFTC Memorandum of Understanding Regarding Harmonization in Areas of Common Regulatory Interest (Mar. 11, 2026); Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets, Release No. 33-11412 (March 17, 2026) (joint interpretation).

developments do not resolve the questions this brief addresses, but they establish that the Commission regards the custodial framework as open to modernization.[17]

Read as a whole, the Custody Rule's history supports a proposition with direct bearing on that modernization: the qualified-custodian requirement is an instrument of investor protection, calibrated in 2003 to the custodial infrastructure of that era, and not an end in itself. The rule has never been static—it has been amended when prevailing technology and market practice rendered its mechanisms inadequate or obsolete—and it has always rested, at its foundation, on a reasonableness standard directed at the protection of client assets rather than on categorical fidelity to any particular custodial form.[18] That history matters because it reframes the operative question. The issue is not whether a vault fits the 2003 description of a qualified custodian, but whether it can serve the protective ends that description was adopted to advance. It is to that question — and to the conditions a vault would have to satisfy — that we now turn.

II. Applying the Qualified-Custodian Criteria to Vault Architecture

Applying the custody rule's protective functions to vault architecture requires assessing the operations of the infrastructure, and system, in question. The question is not whether every vault qualifies as a custodian, but what conditions a vault would have to satisfy to serve the rule's protective objectives. We proceed in three steps: first, the rule's core tenets and the harms each is meant to prevent; second, how those tenets translate into conditions on vault architecture; and third, the broader conditions and risk controls on which any recognition should depend.

A. The Core Tenets of the Custody Rule

The Custody Rule's single protective purpose — shielding client assets from misuse and misappropriation — resolves, on closer inspection, into five distinct conceptual commitments, reflected in the rule's operative provisions and recently organized in custody-modernization discussion as five core tenets: safeguarding, segregation, client notifications, account statements, and independent verification.[19] Each warrants examination on its own terms — what it requires, why the rule demands it, and which species of harm it is meant to forestall — before we turn to the machinery through which the rule has historically given the tenets effect, and ultimately to whether an on-chain vault can honor the same commitments.

*Safeguarding***.** Safeguarding is the rule's foundational and most general command: an adviser that has custody of client funds or securities must keep them secure, intact, and recoverable, and the rule makes it a fraudulent, deceptive, or manipulative act to hold custody at all except in compliance with the protections that follow.[20] The requirement exists because custody confers practical dominion—an adviser able to reach client property is an adviser able to lose, divert, or dissipate it, whether through outright theft, careless controls, or its own financial distress. The harms it targets are correspondingly broad: embezzlement, loss through inadequate operational controls, and, at the extreme, the Ponzi-style fraud in which the assets a

[17] Amendments to the Custody Rules, 90 Fed. Reg. 45,652, 45,656 (Sept. 22, 2025) (SEC Spring 2025 Regulatory Flexibility Agenda, Seq. No. 322, RIN 3235-AN46) (Division of Investment Management) ("The Division is considering recommending that the Commission propose amendments to existing rules and/or propose new rules under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 to improve and modernize the regulations around the custody of advisory client and fund assets, including to address in each case crypto assets").

[18] See 2003 Adopting Release, supra note 1, at 56,692 ("The amendments modernize the rule by conforming the rule to modern custodial practices"); 2009 Adopting Release, supra note 6, at 1,456 (amendments designed to "provide additional safeguards under the Advisers Act").

[19] The five-tenet articulation tracks the rule's operative provisions and the structure used in recent custody-modernization discussion. See supra note 15.

[20] Rule 206(4)-2(a) (rendering it a "fraudulent, deceptive, or manipulative act, practice or course of business" for an adviser to have custody of client assets except in compliance with the rule); see 2009 Adopting Release, supra note 6, at 1,458.

client believes are safely held have in fact ceased to exist. Safeguarding is thus less a discrete mechanic than the protective end that the four remaining tenets operationalize.

Segregation. Segregation requires that client assets be held apart from the adviser's own—maintained either in a separate account in the client's name or in accounts containing only client assets held by the adviser as agent or trustee.[21] Its rationale is that commingling dissolves the legal and practical distinctness of client property: once client and proprietary assets are pooled, client funds can be drawn upon to meet the adviser's obligations, become difficult to trace and return, and—critically—are exposed to the claims of the adviser's creditors. The harms it prevents are therefore twofold: misappropriation accomplished through blending, and the loss of client property to the adviser's estate in insolvency. It is no accident that segregation is the tenet most heavily litigated when an intermediary collapses; whether pooled customer assets are property of the customer or property of the bankruptcy estate was the decisive question in the failures of Celsius, Voyager, and BlockFi, and in the Prime Trust receivership.

Client notifications. The notification tenet requires that the adviser promptly inform a client when it opens a custodial account on the client's behalf, and when the information in that notice materially changes.[22] Its purpose is to enlist the client as a monitor of her own assets: a client who knows where her property is held, and by whom, is positioned to detect arrangements she did not authorize and to compare what she is told against what she independently receives. The harm it addresses is the information asymmetry on which custodial fraud depends—the diversion of assets into accounts the client never learns of, and the client's resulting inability to notice that anything is amiss.

Account statements. The account-statement tenet entitles the client to receive, at least quarterly, a statement of holdings and transactions sent directly by the qualified custodian.[23] The emphasis on direct delivery is deliberate and load-bearing: a statement furnished by the custodian, independent of the adviser, gives the client a second source of truth against which to check the adviser's own reporting, including the propriety of fee deductions and transactions. The harm it forecloses is the one most vividly illustrated by Madoff—fabricated account statements produced by an adviser who is the client's sole source of information about her own holdings.

Independent verification. Finally, independent verification requires that a third party with no stake in the adviser's representations confirm that client assets actually exist and are where they are said to be—historically through an annual surprise examination by an independent public accountant, supplemented, where the adviser or a related person itself serves as custodian, by an internal-control report from an accountant registered with the Public Company Accounting Oversight Board (PCAOB).[24] The rationale is that every other control can be defeated by a sufficiently determined insider, so the rule supplies an external backstop: a verifier who answers to no one within the firm. The surprise character of the examination is itself purposive—its unannounced, year-to-year-irregular timing deprives a fraud of the opportunity to stage

[21]Rule 206(4)-2(a)(1) (requiring that a qualified custodian maintain client assets "in a separate account for each client under that client's name" or in accounts containing only clients' assets held "under your name as agent or trustee for the clients").
[22]Rule 206(4)-2(a)(2) (prompt notice upon opening a custodial account on the client's behalf and upon any change to the required information); see 2009 Adopting Release, supra note 6 (requiring, where the adviser sends its own statements, a legend urging clients to compare them with the custodian's).
[23]Rule 206(4)-2(a)(3) (reasonable belief, after due inquiry, that the qualified custodian sends account statements directly to clients at least quarterly); 2009 Adopting Release, supra note 6 (direct delivery by the custodian "will provide greater assurance of the integrity of account statements received by clients").
[24]Rule 206(4)-2(a)(4) (examination "at a time that is chosen by the accountant without prior notice or announcement" and "irregular from year to year"); id. (a)(6) (internal-control report, by a PCAOB-registered accountant, where the adviser or a related person serves as qualified custodian); 2009 Adopting Release, supra note 6.

assets for a scheduled review.[25] The harm it targets is the self-certification problem at the heart of the gravest custodial frauds: the absence of anyone, other than the wrongdoer, who has confirmed that the assets are real.

These five commitments are the rule's protective ends. The question for any custody regime is how those ends are institutionalized. In the traditional securities markets for which the modern rule was written, the Commission answered that question principally through the qualified-custodian requirement. Rather than prescribe safekeeping practices directly, the 2003 rule required custody to be effected through a defined class of regulated intermediaries — banks and savings associations, registered broker-dealers, registered futures commission merchants, and qualifying foreign financial institutions.

That design borrows the safeguards that already attach to those institutions. Each is subject to its own regime of capitalization, segregation, supervision, and recordkeeping, so routing client assets through a qualified custodian imports a body of prudential protection the adviser could not be trusted to supply itself. Equally important, the qualified custodian stands between the adviser and the assets, preventing the adviser from unilaterally disposing of client property. The single requirement thus operationalizes safeguarding and segregation at once.

The rule then supplements that institutional separation with information rights. The notification and account-statement provisions ensure that the client, and not merely the adviser, possesses independent information about the account. The rule requires written arrangements and reasonable assurances surrounding the custodial relationship, prompt notice when an account is opened or altered, and — most consequentially — delivery of account statements directly by the qualified custodian. The 2009 amendments sharpened this protection where it was weakest: they eliminated the prior alternative under which the adviser itself could send the statements, on the theory that the integrity of the document used to police the adviser should not depend on the adviser's own hand.

Finally, the rule supplies an external backstop. Independent verification is provided through the annual surprise examination, the audit exception available to pooled vehicles that distribute audited financial statements, and the internal-control report required where the adviser or a related person serves as its own custodian — each performed by an independent public accountant. The architecture is deliberately graduated by risk. The configuration the rule treats with greatest suspicion is the one in which the adviser is also the custodian — the very configuration that enabled the Madoff fraud — and it is there that the rule layers verification most heavily.

Taken together, these mechanisms share a revealing characteristic: each is a proxy for direct observation. The qualified custodian, the custodian-delivered statement, and the surprise examination all exist because, for traditional securities and funds, clients and regulators could not continuously observe whether assets remained in existence, segregated, and unencumbered. The rule therefore built an apparatus of intermediation, periodic reporting, and after-the-fact inspection to approximate that vantage. That observation is the hinge of the analysis that follows. If a new custody technology can make the relevant facts continuously and verifiably observable, the operative question is not whether it uses the inherited proxies, but whether it serves the protective ends those proxies were designed to approximate.

B. Translating the Criteria into Vault Architecture

The same functional framework can be applied to vault architecture. The question is not whether a vault uses the traditional machinery of qualified custody, but whether it provides at least equivalent protections

[25] See 2009 Adopting Release, supra note 6 (the examination is conducted "at a time that is chosen by the accountant without prior notice or announcement" and is "irregular from year to year"); supra note 25.

against the same risks. The discussion that follows therefore asks, function by function, what a vault must do to protect client assets in the way the custody rule requires.

Safeguarding. For a traditional custodian, safeguarding is achieved through institutional key management, internal controls, and supervisory oversight. In a vault, the smart contract is itself a safeguarding stack, and it operates as an independent custodial counterparty rather than as self-custody. A depositor receives a non-transferable receipt token representing a proportionate claim, and the only action that token authorizes is redemption to the authorized wallet; the contract performs a single, unspoofable cryptographic check rather than authenticating a human who could be deceived. To satisfy this criterion—and thereby foreclose the diversion that safeguarding targets—a qualifying vault must vest no unilateral withdrawal authority in any provider, adviser, or curator, with its core withdrawal and redemption logic either immutable or governed by transparent, time-locked mechanisms. All the while, asset-level safeguarding extensions can be deployed to enable compliance with OFAC requirements and facilitate anti-counterfeiting protections.

Segregation. The harm segregation guards against—the commingling that exposes client property to the adviser's creditors—is answered structurally rather than contractually. Although depositors are typically pooled within a single contract, each depositor's entitlement is precisely defined by the contract and represented by the receipt token, and no participant holds a balance-sheet claim against the pool. To qualify, a vault must segregate withdrawal rights at the contract or address level and ensure that no provider, adviser, or curator holds a proprietary interest in client assets. Because crypto-native assets held non-custodially sit on no participant's balance sheet, there is no estate into which they can be drawn in an insolvency. For assets that are only tokenized representations of off-chain property, insolvency-remoteness instead depends on the off-chain legal wrapper—a true sale to a bankruptcy-remote vehicle, trust or custodial segregation, and a perfected, enforceable claim for token holders— subject to the legal-structuring conditions discussed in Part II.C.

Client notifications. Where the rule combats information asymmetry by requiring notice of custodial arrangements and material changes, a vault can satisfy that objective through multiple layers. First, any material change to the vault's terms, governance, or withdrawal conditions can be queued behind a mandatory time-lock and rendered publicly visible, creating a tamper-evident record with a fixed, knowable execution time. The adviser or vault sponsor can additionally deliver plain-language notice to clients—by email, platform alert, or even onchain communications to customer wallets—within that same time-lock window, keyed to the on-chain event and citing its reference (transaction hash, block, and scheduled execution time) so that the client can independently verify the notice against the chain.

Account statements. The stated tenet's purpose—to give the client an independent source of truth against which to detect fabricated reporting—is satisfied natively. In a vault, balances and transaction history are continuously and publicly verifiable on-chain; where confidentiality is required, that visibility can be scoped through selective-disclosure mechanisms to the account holder, auditors, and examiners without public exposure. The statement is no longer a periodic snapshot delivered in arrears and capable of fabrication; it is the chain itself, available at any moment, particularly where the on-chain record can be linked to the client's legal account through an identity or credentialing process, and where an examiner can identify the complete set of relevant client positions.

Independent verification. Finally, the verification tenet's external backstop—historically the annual surprise examination—is supplied in a vault by on-chain auditability together with independent third-party security review. To qualify, a vault's balances and transaction history must be independently verifiable on-chain, its contracts must undergo third-party security audits before deployment and after any material upgrade, and any adviser relying on the arrangement remains subject to its applicable examination and audit obligations.

Translated this way, the five tenets yield a concrete set of structural conditions: no unilateral withdrawal authority; programmatic preservation of redemption and transfer rights; cryptographic segregation; transparent, time-locked governance, with any curator's deployment authority bounded to an on-chain-verifiable allowlist; documented security operational controls; independent verification and on-chain auditability; and no affiliated protocol routing that would let a participant profit by steering client assets. This is the framing Veda placed on the record in its March 2026 written input to the harmonization initiative.[26] A vault that satisfied all of these conditions would not, under the rule as currently written, automatically become a qualified custodian. It would, however, perform the investor-protection functions the qualified-custodian requirement was designed to serve — and would therefore provide a strong basis for staff guidance, no-action relief, pilot relief, or rule modernization recognizing functionally equivalent safeguarding arrangements. The conditions on which any such recognition should depend, and the risks it must contain, are the subject of the next Part.

C. Conditions for Recognition and Risk Containment

The case for recognizing vault-based safeguarding does not depend on treating code as riskless. It depends on the opposite proposition: that the material risks of custody should be made explicit, bounded by architecture, tested by independent review, and visible to clients, auditors, and supervisors. Legacy custody also relies on systems, people, legal arrangements, and operational controls that can fail. The relevant question is therefore comparative and regulatory: which arrangement provides equivalent or greater protection against misappropriation, commingling, insolvency exposure, false reporting, and undetected control failure?

Three premises frame the analysis. First, recognition of vault-based safeguarding should be conditional, not categorical: not every vault would satisfy the rule's protective objectives, and a vault should be eligible only if it satisfies specific structural, operational, verification, governance, and disclosure conditions. Second, the relevant comparison is not between a risky vault and a risk-free legacy custodian. Legacy qualified custodians present material risks of their own — internal-control failures, employee misconduct, rehypothecation, affiliated routing, insolvency, account-statement fabrication, operational outages, opaque books and records, limited asset coverage, conflicts in staking and other asset-use arrangements, and delayed detection through periodic examination. Vault risks should therefore be assessed comparatively, not in isolation. Third, vault-specific risks can in many cases be contained, monitored, and made visible through architecture and verification more readily than their legacy analogues. The point is not to deny these risks but to show that a properly designed framework can make them explicit, bounded, testable, and supervisor-accessible.

Smart-contract and code risk. Any instrument connected to the internet, and running on software, is vulnerable to code risk and a vault is no exception. A vault's logic can contain bugs, be exploited, or behave in unintended ways. Recognition could as a result be conditioned on formal verification of the smart contracts that hold and move assets, third-party security audits before deployment, bug-bounty programs, constrained upgrade authority, post-upgrade re-verification, and public disclosure of material code changes. Such an approach would be an upgrade from current approaches, where the custody rule imposes no minimum standard on how a custodian typically holds assets. Legacy custodian internal systems and controls, even amongst the largest financial institutions, are instead typically opaque to clients and examined only periodically.

Upgradeability and governance risk. A legacy custodian can amend its terms of service, enter affiliated arrangements, or alter operational practices, and a client may learn of such changes only after they take effect. A vault's rules can likewise be modified after assets are deposited. The relevant question is therefore

[26] Veda Tech Labs Inc., written input to the Joint SEC-CFTC Harmonization Initiative (Mar. 23, 2026).

not whether change is possible, but what disciplines it. In a vault, that discipline is structural and should operate in layers: transparent, on-chain governance makes any proposed change publicly visible in advance; mandatory time locks and advance notice give clients a window in which to act before a change takes effect; client exit rights to ensure they can withdraw rather than be bound by terms they did not accept; and a defined set of core withdrawal rights rendered immutable, so that no upgrade — however it is governed — can impair a client's ability to redeem.

Oracle, bridge, and dependency-stack risk. A vault's safety may depend on external contracts, bridges, and oracles several legs removed from the token. Proper risk containment requires such dependency-stack disclosure as a condition. Legacy custody offers more limited account-level visibility and is generally not positioned to expose the full risk stack of a tokenized asset at all.

Key, wallet, and authorization risk. Private-key compromise, wallet compromise, and user error are genuine hazards. They can be mitigated through multi-signature controls, hardware security modules where appropriate, role separation, transaction policies, allowlists, withdrawal delays, recovery mechanisms, and cryptographic entitlement checks, any of which could be required as a condition of recognition. Legacy custody is not free of the analogous risk; it relies on human instruction pathways, operational personnel, and internal authorization systems that can themselves fail or be socially engineered — a vector the cryptographic entitlement check is designed to remove.

Insolvency and property-rights risk. Whether a client's interest in vault assets is enforceable and insulated from the insolvency estate of any adviser, provider, curator, or infrastructure provider is not answered by on-chain accounting. Instead, the answer lies in whether the full set of instruments governing the arrangement—the smart contract, any off-chain service agreement, and the receipt-token documentation—left the client a retained property interest or merely a contractual claim against the provider.[27] The most robust protections do not turn on a general assurance of insolvency-remoteness but on terms retaining beneficial ownership and disclaiming any provider proprietary claim, segregation with a prohibition on commingling and rehypothecation, a bankruptcy-remote holding vehicle and commercial-law perfection where appropriate, and the disclosure of any loss-allocation backstop, including provider capital, insurance, or another solvent obligor sized to the assets safeguarded.

Conflicts of interest and affiliated routing. A vault provider, adviser, curator, or affiliated protocol could profit by directing assets into related venues. Regulatory recognition could require the absence of undisclosed affiliated routing, disclosure of compensation, on-chain allowlists, conflict-of-interest policies, and verification of deployment pathways. The same risk pervades legacy custody and staking arrangements, where clients may be routed through affiliated or revenue-generating services with limited visibility; the difference a vault can offer is that the permitted deployment pathways are enumerated on-chain and checkable.

Privacy and supervisory access. Public auditability is in tension with client confidentiality. That tension can be managed through selective disclosure, zero-knowledge proofs, permissioned examiner access, auditor

[27] On-chain arrangements have produced a catalogue of losses, and an honest case for vault-based safeguarding must begin there rather than around it. The largest have come from three sources. First, contract logic: Euler Finance lost approximately $197 million in March 2023 to a flaw in a single function that permitted an account to render itself insolvent and self-liquidate — in a protocol that had undergone roughly ten audits by six independent security firms before the exploit. Second, dependencies external to the contract that holds the assets: the Ronin and Wormhole bridge failures, totaling nearly a billion dollars, turned on compromised validator keys and a forged signature check, not on any defect in the underlying token. Third, economic manipulation that is valid at the level of the code: the Mango Markets exploit extracted roughly $117 million by manipulating the price oracle the protocol relied upon, so that every transaction executed exactly as written

credentials, and account-holder-specific views, so that confidentiality is preserved while verification remains available to those entitled to it. In legacy custody, by contrast, privacy is typically achieved through opacity rather than cryptographic access control — which protects confidentiality at the cost of the very visibility supervision depends on.

Compliance controls. Sanctions screening, anti-money-laundering obligations, transfer restrictions, and investor-eligibility limits must be honored. Some of these constraints can be embedded directly into transfer logic, enforced through pre-execution checks and allowlists, and monitored continuously — so that a prohibited transfer fails before it executes rather than being detected afterward.[28] Legacy systems more often rely on after-the-fact surveillance and manual controls, which detect violations rather than prevent them.

Across all of these categories the regulatory posture is the same: every custody system has risks, and the question is whether those risks are identified, controlled, disclosed, and supervised. Framed that way, the conditions enumerated here are not concessions but the substance of a disciplined recognition framework. The next Part makes that framework concrete by describing one safeguarding model that implements these conditions; the comparative assessment that follows then evaluates how such a model fares against legacy custody, an evaluation that holds only where these conditions are satisfied.

III. A Vault-Based Safeguarding Model

Having translated the custody rule's protective functions into architectural conditions, this Part describes one way those conditions could be implemented in practice. The model is illustrative, not exclusive. It uses Veda Vaults and Bluprynt to show how a vault-based safeguarding arrangement could separate custody, verification, assurance, adviser responsibility, and regulatory supervision into distinct roles.

That separation is central to the model. The arrangement does not depend on a single actor operating the vault, verifying the assets, auditing the controls, advising the client, and supervising the result. Instead, each function is assigned to a different participant, making the arrangement more legible, testable, and examinable. Figure 1 illustrates this division of responsibility.

Veda Vaults—vault provider. Veda supplies and operates the smart-contract vault architecture. The vault receives client assets, issues receipt tokens or other entitlement records, enforces withdrawal and redemption logic, constrains deployment authority, and maintains on-chain records of balances and transactions. It is not the adviser, the verifier of record, the auditor, or the regulator.

Bluprynt—verification and disclosure infrastructure. Bluprynt supplies the verification and disclosure layer that makes the vault arrangement legible to clients, auditors, and regulators. Its Know Your Issuer infrastructure binds verified issuer identity and mint authority to the token. Its Proof of Collateral infrastructure verifies asset backing, maps the dependency stack, distinguishes verified from attested data, integrates smart contract verifications, and seals results in tamper-evident evidence records. Bluprynt does not operate the vault, serve as custodian, act as legal issuer, audit the arrangement, advise the client, or regulate the result.

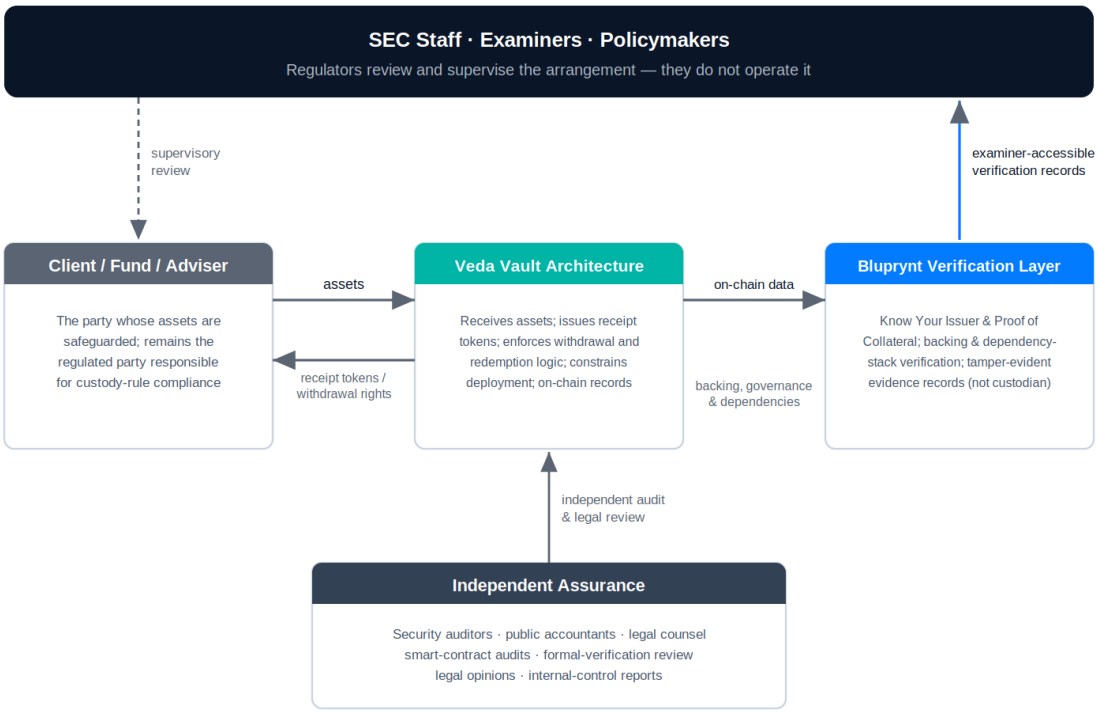
The investment adviser or fund manager. The adviser or fund manager remains the regulated party responsible for compliance with the custody rule or any successor safeguarding framework. Recognition of vault-based safeguarding would not transfer that responsibility to the vault provider or the verification

[28] Architecture & Flow of Funds, Veda Docs, https://docs.veda.tech/architecture-and-flow-of-funds (last visited June 16, 2026) (describing the optional Hook module, which can enforce custom logic before share transfers and enable compliance features such as address whitelisting and transfer restrictions).

provider. It would instead identify a different mechanism through which the adviser may satisfy the rule's protective requirements.

Independent assurance providers. Security auditors, public accountants, and legal counsel supply the independent review on which the model depends. They may provide smart-contract audits, formal-verification review, legal opinions, internal-control reports, or other assurance outputs required by law, regulation, or supervisory conditions. Their independence from both the vault provider and the verification provider is part of what makes the arrangement supervisable.

SEC staff, examiners, and policymakers. Regulators evaluate whether the arrangement satisfies the rule's protective purposes under defined conditions. They do so through access to examiner-readable or permissioned verification records, account-level evidence, disclosures, audit outputs, and other supervisory materials. They review and supervise the arrangement; they do not operate it.



Verification and disclosure outputs are available to the adviser, client, auditors, and examiners.
Vault operation, verification, independent assurance, adviser responsibility, and supervision are distinct, separable roles.

Figure 1. Technology-Native Safeguarding Architecture: Vault, Verification, Assurance, and Supervisory Access.

Taken together, these roles create a layered safeguarding system. The vault provides the asset-control mechanism; the verification layer makes the asset, issuer, backing, and authority structure observable; independent assurance providers test the legal and technical controls; the adviser remains the regulated party responsible for compliance; and regulators receive records that allow the arrangement to be examined rather than taken on trust. The point is not merely that the functions are separated, but that each function produces evidence another participant can test.

The figure should be read as a functional map of a vault-based safeguarding arrangement. It shows how vault operation, verification, independent assurance, adviser responsibility, and supervisory access can be separated rather than collapsed into a single actor. In doing so, it illustrates how any recognition framework

should turn on whether an architecture satisfies the required safeguards, not on the identity of the firms or protocols supplying them.

IV. A Comparative Assessment: Vault-Based and Legacy Safeguarding

With that model in view, this Part compares conditioned vault-based safeguarding with legacy qualified custody. The comparison makes the further point that a vault meeting the conditions identified above can serve several of the rule's protective objectives more directly, continuously, and transparently than legacy intermediated custody. It is not a claim of categorical superiority, and it holds only where the conditions described in Part II.C are satisfied; it is offered to inform a judgment about equivalent-or-greater investor-protection value, not to disparage institutions that have safeguarded client assets for decades.

A. Continuous observability and verification

The central difference is that what a vault holds and how a vault transacts its holdings can be observed and proven continuously. Public chain state makes balances, segregation, and asset movement directly observable; Bluprynt's Proof of Collateral turns that raw state into verified, sealed, plain-language evidence by traversing the asset's full dependency graph to terminal backing, reading every value at a pinned block, confirming each read against several independent sources, submitting each contract to formal verification, running a deterministic suite of backing-state checks, and sealing the result in a hash-chained, version-addressable record that any client, auditor, or examiner can independently check.[29] It verifies crypto-native existence and encumbrance directly on-chain, and for off-chain backing it binds and discloses structured attestation — its source and freshness — rather than asserting verification it cannot perform; Know Your Issuer adds contemporaneous evidence of issuer identity, mint authority, and controller privileges. Where traditional custody confirms holdings through a statement issued periodically and an examination conducted once a year, this evidence is contemporaneous: the annual surprise examination becomes re-proof on every traversal, and the quarterly statement becomes a live one. The practical consequence is that collateral integrity is tested on every snapshot rather than reconstructed after a loss.[30]

B. Reduced intermediary risk

The custody rule was built around the risk that the adviser misappropriates assets, but several of the defining custodial failures involved the custodian itself misusing the assets it held. A qualifying vault reduces the custodian as a point of failure. Because withdrawal is gated by cryptographic entitlement rather than by human instruction, there is no instruction pathway to socially engineer or coerce; because a qualifying vault prohibits affiliated protocol routing and any proprietary claim against the pool, the provider cannot lend, rehypothecate, or self-deal with client assets; and because client assets sit on no participant's balance sheet, an operator's insolvency does not draw them into an estate — subject, again, to the legal-structuring conditions of Part II.C. The protection runs not only against the adviser but against the custodian, a risk the legacy framework addresses only indirectly.

[29] Bluprynt, Proof of Collateral (June 2025), available at: https://bluprynt.com/research/proof-of-collateral-brief

[30] In this way, continuous verification strengthens rather than replaces, the evidentiary framework for safeguarding. It can establish that the on-chain state is what it purports to be and that the dependency stack resolves as recorded. Where relevant facts sit off-chain — such as the existence or sufficiency of backing assets held outside the blockchain environment — the evidence record can bind and timestamp the relevant attestation, including its source and freshness. In that setting, the system does not eliminate reliance on a qualified attestor, but it can make that reliance more precise, visible, and auditable than in many legacy arrangements.

C. Operational and fiduciary advantages

Vault-based safeguarding also offers operational characteristics that bear on an adviser's fiduciary obligations. Settlement and redemption occur on-chain at any hour, without wire cutoffs, settlement-cycle delays, correspondent-bank dependency, or operating-hour gaps, which matters when a client must act on short notice. Within the universe of on-chain assets, a vault can in principle hold a broader range of tokens than a given qualified custodian currently supports; where such an arrangement is recognized as compliant safeguarding and paired with per-asset verification of legitimacy and backing, that breadth could ease the access bottleneck that can otherwise leave an adviser unable to custody, in a compliant manner, a digital asset its client wishes to hold And within bounded, on-chain-verifiable permissions, a vault can permit productive use of assets — staking or governance participation, for example — without surrendering custody, where a legacy arrangement might force a choice between safekeeping and use. These advantages are genuine but conditional, and should not be overstated; some depend on scale and on the maturity of the surrounding market.

More generally, onchain infrastructure enables the programmability of compliance. A vault need not function merely as a passive receptacle for assets; it can incorporate rules, credentials, permissions, attestations, and transaction-level controls that determine how assets may be held, transferred, staked, voted, or redeemed. This matters not only because compliance conditions can be automated, but because they can be applied at the point of transaction, helping ensure that permitted operations remain aligned with changing legal or regulatory requirements as those requirements are translated into updated rules or credentials. In traditional custody, that alignment often depends on human review, institutional consensus, and consistent operational execution across intermediaries. By contrast, programmable vault architecture — including hook-based designs used in DeFi infrastructure — can embed compliance logic directly into asset operations. In this particular case, a credentialing system such as Bluprynt's can supply the machine-readable status, attestations, and permissions that allow those controls to operate, making compliance more continuous, auditable, and embedded in the safeguarding infrastructure itself.

D. Supervisory and audit advantages

The infrastructure, by residing and operationalized onchain, also offers advantages to those who oversee it. An examiner can query the chain and verify the credential directly, without subpoenaing records or depending on a custodian's cooperation, and can do so on any cadence rather than once a year — a form of embedded, ongoing supervision. Auditors gain continuous, view-only access and can prove onchain controls through test transactions. Confidentiality need not be sacrificed: selective disclosure and zero-knowledge techniques can keep balances private from the public while remaining verifiable to the account holder, auditors, and examiners. And because the controls are expressed in code and disclosed, diligence across arrangements can proceed on a more standardized, comparable basis than is possible across opaque, firm-specific custodial systems.

E. Residual risks and why conditions matter

None of these advantages is automatic. Each presupposes that the vault satisfies the structural, operational, verification, governance, and disclosure conditions set out in Part II.C — formal verification and audit of the code, transparent and time-locked governance, mapped and disclosed dependencies, sound key management, appropriate legal structuring for insolvency remoteness, the absence of undisclosed affiliated routing, supervisor-accessible records, and embedded compliance controls. A vault that lacks these properties is not a better custodian; it may be a worse one. The comparative case is therefore inseparable from the conditions, and the table that follows should be read with that qualification in mind.

At a glance

A summary comparison. Each row reflects a protective function of the custody rule and how the two models deliver it; the vault column assumes the conditions in Part II.C are satisfied.

Protective function	Traditional qualified custody	Conditioned vault + verification
Verification cadence	Annual surprise examination; quarterly statements delivered in arrears.	Continuous — backing re-proven on every traversal, describing one pinned moment; contemporaneous, not retrospective.
Scope of verification	Top-level account balances held at one custodian.	The full dependency closure: the asset, its vault, bridges, oracles, and every contract down to terminal backing.
Segregation	Contractual and periodically reconciled; subject to pooling disputes in bankruptcy.	Cryptographic and continuously observable; no participant balance-sheet claim, with legal structuring per Part II.C.
Custodian misuse	Custodian can lend, rehypothecate, or be instructed to misappropriate; staking terms may override custody terms.	No affiliated routing and no proprietary claim; no instruction pathway to abuse where conditions are met.
Evidence integrity	A custodian-issued statement taken largely on trust; books can be falsified.	A hash-chained, tamper-evident record on an immutable ledger: the integrity of what was recorded is checkable rather than asserted, while any off-chain value incorporated into the record remains tied to the source, method, and evidentiary basis through which it was introduced.
Detection latency	Problems typically surface months later, at exam or audit.	Real-time: the moment a verified on-chain property stops holding, that change is recorded in the evidence chain. For matters that depend on off-chain facts — such as asset backing, oracle inputs, or legal characterization — the same framework ties verification to the relevant attestation or input, so the evidentiary record updates when that source is refreshed.
Code & contract soundness	Not addressed by the rule; custodian controls are effectively a black box.	Formal verification and third-party audit of every contract, re-run on upgrade — a condition of recognition.
Issuer & authority identity	Not addressed; a statement says nothing about issuer provenance and authority.	Know Your Issuer binds issuer identity and mint authority to the token and enumerates controller privileges.
Asset coverage	Thin, slow-to-grow list; onboarding gated by the custodian’s priorities.	Broader coverage, including assets no qualified custodian supports, subject to the same conditions.
Settlement & access	Wire cutoffs, settlement cycles, operating hours; protracted illiquidity in a custodian insolvency.	On-chain redemption at any hour; direct access, subject to insolvency-remoteness structuring.

Protective function	Traditional qualified custody	Conditioned vault + verification
Supervision & audit	Periodic exam reliant on custodian cooperation; opaque, firm-specific controls.	Examiner- and auditor-accessible records on any cadence; privacy preserved via selective disclosure.
Residual risk	Internal-control, insolvency, and reporting risks, often detected late.	Code, governance, key, oracle, and legal-characterization risks — made explicit, bounded, and supervised.

V. Regulatory Pathways

Functional equivalence does not, by itself, change the law. A demonstration that a conditioned vault arrangement serves the custody rule's protective purposes supports defined forms of staff or Commission action; it does not effect them. This Part sets out a graduated set of pathways through which the Commission and its staff could responsibly explore recognition — without relaxing the rule's protective objectives — ranging from interpretive guidance to rule modernization. They are presented as options, not demands, and each could be conditioned on the safeguards described in Part II.C.

Staff guidance recognizing technology-native safeguarding. Staff could articulate, through interpretive guidance or a statement of position, the conditions under which a technology-native safeguarding arrangement would be viewed as consistent with the custody rule's protective purposes. Guidance of this kind would not amend the rule, but it would give advisers and providers a defined compliance target and would let the staff observe arrangements in operation before considering more formal steps.

*No-action relief for arrangements that meet enumerated controls***.** For arrangements satisfying a defined set of structural, verification, governance, and disclosure conditions, the staff could provide no-action relief specifying those conditions and the records that must remain available for examination. Conditioned no-action relief is a familiar and well-suited instrument for extending an existing framework to a new technology incrementally, and recent staff practice in adjacent digital-asset contexts supplies a template.[31]

A pilot or time-limited supervisory program. The Commission or its staff could establish a pilot or time-limited supervisory program under which a defined number of arrangements operate with enhanced reporting to staff, examiner-accessible verification records, and a sunset and review date. A pilot would allow the protective claims advanced here to be tested against operational experience, with the option to expand, condition further, or discontinue based on evidence.

Rule modernization recognizing a broader safeguarding category. The Commission could, through notice-and-comment rulemaking, separate the concept of a "qualified custodian" from a broader category — a "qualified safeguarding arrangement" or "functionally equivalent safeguarding arrangement" — defined by the protective functions an arrangement performs rather than by the institutional form it takes. The Commission's own withdrawn 2023 proposal, which would have redesignated the custody rule as a broader "safeguarding rule," demonstrates that the agency has already contemplated reframing the rule around safeguarding functions rather than custodial form.[32]

[31]Conditioned no-action relief has been used in adjacent digital-asset contexts. See, e.g., CFTC Market Participants Division no-action relief regarding recognition of digital-asset collateral (Staff Letter 25-40, Dec. 8, 2025; reissued Feb. 6, 2026).
[32]Safeguarding Advisory Client Assets, Release No. IA-6240 (Mar. 9, 2023) (proposing to redesignate the custody rule as a broader "safeguarding rule" under new Advisers Act Rule 223-1), withdrawn June 12, 2025, see supra note 16.

A principles-based equivalent-protection standard. Within any of these pathways, the operative test could be a principles-based standard of equivalent protection: an arrangement qualifies if it provides protection against misappropriation, commingling, insolvency exposure, false reporting, and undetected control failure that is at least equivalent to that provided by a traditional qualified custodian. Such a standard would be technology-neutral by design, applying to any architecture — not only vaults, and not only those enabled by the authors — that meets it.

Examiner-accessible records and disclosure as conditions of relief. Common to every pathway, and central to all of them, should be a requirement that the arrangement maintain examiner-accessible verification records and satisfy defined disclosure obligations to clients, auditors, and the staff. Supervisory access is what allows recognition to proceed without relaxing protection: it substitutes continuous, verifiable visibility for the periodic inspection on which the legacy framework relies, and it ensures that recognition can be monitored and, if necessary, withdrawn.

None of these pathways requires the Commission to conclude that vaults are categorically superior to banks or broker-dealers, and none requires it to lower the bar the custody rule sets. Each asks only that the bar be defined functionally — by the protections an arrangement delivers and the supervision it permits — so that arrangements demonstrably meeting it can be recognized under conditions the staff sets and oversees.

Conclusion

The custody rule's investor-protection objectives — preventing misappropriation, commingling, insolvency exposure, fabricated reporting, and unchecked control over client assets — are as important as ever and have not changed. What has changed is the set of mechanisms available to achieve them. For sixty years the rule has pursued those ends through intermediation, periodic reporting, and after-the-fact examination, because the underlying assets could not be observed directly. On-chain assets can be, and a vault that meets defined conditions, paired with continuous verification, can serve the same ends through architecture and evidence rather than through institutional form.

That possibility should be approached conditionally, not categorically. Not every vault qualifies; recognition should depend on enumerated structural, operational, verification, governance, and disclosure conditions, and on supervisory access to the records that make the arrangement legible. A vault that lacks those properties is not entitled to recognition, and the comparative advantages described here arise only where the conditions are met. Any recognition framework should also be neutral, applying to any architecture that satisfies the required safeguards rather than to any particular provider, including the authors.

We therefore invite the staff and the Commission to consider a defined regulatory pathway— guidance, conditioned no-action relief, a supervisory pilot, or rule modernization recognizing functionally equivalent safeguarding arrangements—for technology-native custody that demonstrably meets the rule's protective purposes. The Commission can preserve the rule's protective purpose while recognizing new mechanisms that may achieve that purpose more directly, continuously, and transparently. That, and not any claim of categorical superiority, is the proposition this brief is offered to support.

The proposal is cited only to show that the Commission has previously contemplated reframing the rule around safeguarding functions; the authors do not endorse the withdrawn proposal's substance.