Wave Digital Assets
11740 San Vicente Blvd, Suite 109-632
Los Angeles, CA 90049

April 7, 2026

Division of Investment Management
Securities and Exchange Commission

Crypto Task Force
Securities and Exchange Commission

Division of Market Participants
Commodity Futures Trading Commission

Joint SEC-CFTC Harmonization Initiative

Re: Letter of Support for Veda Tech Labs Inc., *Recommendations Regarding Recognition of Vaults as Satisfying SEC Qualified Custody and CFTC Segregation Requirements for Digital Assets* (March 23, 2026), and Additional Recommendations Regarding Individually Managed Accounts and Privacy-Preserving Verification

---

I. INTRODUCTION

Wave Digital Assets LLC ("Wave") respectfully submits this letter in support of the recommendations made by Veda Tech Labs Inc. ("Veda") in its letter to the Division of Investment Management, the Crypto Task Force, the Division of Market Participants, and the Joint SEC-CFTC Harmonization Initiative dated March 23, 2026 (the "Veda Letter").[1] Wave urges the Commission and the CFTC to adopt the guardrail-based compliance pathway for vault-based custody architectures proposed by Veda, and submits this letter to provide the regulators' perspective of an SEC-registered investment adviser that actively manages digital asset portfolios on behalf of clients.[2]

---

[1] *See* https://www.sec.gov/files/sec-cftc-harmonization-initiative-written-input-veda-tech-labs-inc-032326.pdf.

[2] Wave further submits this letter in response to (i) the SEC's Division of Investment Management's statement in the Commission's 2025-2026 Regulatory Agenda that it is considering recommending amendments to modernize the custody framework for advisory client assets, including crypto assets and (ii) the SEC-CFTC Memorandum of Understanding Regarding Harmonization in Areas of Common Regulatory Interest, signed March 11, 2026 (the "2026 MOU"), which commits both agencies to facilitating the exploration of alternative compliance frameworks capable of achieving regulatory objectives while preserving investor protection and market integrity.

Wave is registered with the Commission as an investment adviser (CRD#305726) under the Investment Advisers Act of 1940, as amended (the "Advisers Act"). Wave manages discretionary portfolios composed entirely of digital assets, including Cardano (ADA), Polkadot (DOT), Avalanche (AVAX), and Stellar (XLM), among others. Wave manages assets both through pooled investment vehicles and through individually managed accounts ("Separately Managed Accounts" or SMAs") on behalf of institutional and high-net-worth clients. Wave also has familiarity with decentralized finance ("DeFi") strategies including protocol staking, liquidity provision, and yield-generating activities conducted through automated smart contract protocols.

Wave writes in support of Veda's proposal for three distinct but related reasons. First, Wave has experienced firsthand the infrastructure constraints and fiduciary tension that Veda's letter describes. Wave has familiarity with long-tail and newly-issued digital asset positions for which no qualified custodian currently provides infrastructure support, creating a structural compliance gap that Veda's proposal would directly address. Second, Wave manages client assets through separately managed accounts, which is a custody structure that Veda's letter does not fully address. Wave respectfully submits that the SMA context presents a particularly compelling case for vault-based custody recognition, with investor protection characteristics that in some respects exceed those available under traditional qualified custodianship. Third, Wave's institutional clients have material confidentiality requirements that create tension with the on-chain transparency features of vault architectures, and Wave recommends that the Commission explicitly recognize privacy-preserving cryptographic verification mechanisms as a compliant alternative to full public on-chain transparency, so that the auditability benefits of vault custody can be achieved without compromising client confidentiality.

II. WAVE'S OPERATIONAL EXPERIENCE WITH INFRASTRUCTURE CONSTRAINTS

As Veda's letter correctly observes, qualified custodian support for digital assets is not universal. Custodian decisions about which assets to support reflect engineering integration timelines, node infrastructure requirements, operational monitoring capacity, and commercial prioritization rather than regulatory determinations about asset risk or appropriateness for client portfolios.

Wave manages portfolios that include digital assets across multiple blockchain architectures, including assets that represent the long tail of the digital asset universe. This includes governance tokens, protocol-layer assets, recently launched Layer 1 and Layer 2 native tokens, and DeFi receipt instruments including liquidity provider tokens, staking receipts, and vault share tokens. For a significant subset of these assets, Wave has encountered one or more of the following operational realities: (1) no qualified custodian currently supports the asset; (2) the relevant custodian supports the asset on mainnet but not on certain Layer 2 networks where Wave's strategy requires execution; (3) the custodian supports custody of the underlying asset but cannot hold or account for the receipt token issued upon DeFi deployment; or (4) custodian onboarding timelines create a gap period during which Wave cannot receive assets to which clients are contractually entitled under token purchase agreements or Simple Agreement for Future Tokens ("SAFT") structures.

Each of these scenarios creates a concrete fiduciary problem. Wave cannot decline to receive assets to which clients are entitled without potentially breaching its investment management agreement and its fiduciary duty. Delaying receipt pending custodian integration may impose adverse tax timing consequences on clients or cause Wave to miss time-sensitive investment opportunities. Further, accepting assets into a wallet structure that does not satisfy Rule 206(4)-2 under the Advisers Act creates direct regulatory exposure for Wave. The result is precisely the fiduciary tension Veda's letter describes. Rule 206(4)-2 risks functioning as a de facto innovation bottleneck

rather than a calibrated investor protection mechanism, when the constraint is custodian infrastructure readiness rather than asset-level risk.

Wave further observes, consistent with the experience of other institutional participants in digital asset markets, that these infrastructure gaps are compounded by structural features of the qualified custodian market that the Commission should expressly acknowledge. The concentration of custody services among a small number of providers that confers significant pricing power and contractual leverage over investment advisers; the misalignment between the continuous, 24/7 operation of crypto asset markets and the limited operating hours of most qualified custodians, which creates real-time liquidity and execution challenges particularly acute for digital asset managers; and the need for pre-funding assets on non-qualified custodian trading venues, which may impair best execution and increase systemic risk exposure for clients. Each of these structural features reinforces the case for a technology-native compliance pathway that reduces investment advisers' dependence on a constrained and concentrated custodian infrastructure.

A guardrail-based vault custody compliance pathway would directly resolve this tension. Vault architectures provide multi-asset and cross-chain coverage with minimal engineering integration requirements, making them particularly well-suited to long-tail and newly issued digital asset positions. Wave strongly supports Veda's recommendation that the Commission establish such a pathway as part of any proposed amendments to Rule 206(4)-2 under the Advisers Act.

III. WAVE'S ENDORSEMENT OF VEDA'S GUARDRAIL FRAMEWORK

Wave endorses the seven structural guardrails proposed by Veda as a framework for a compliant vault-based custody pathway. Wave's operational experience as an investment adviser confirms that each guardrail addresses a genuine investor protection concern and that, taken together, they produce a risk profile that is reasonably comparable, and in important respects superior, to the protections available under traditional qualified custodianship for digital assets.

Wave specifically endorses the following aspects of Veda's analysis from the perspective of an investment adviser:

- The elimination of unilateral withdrawal authority (Guardrail 1) maps directly onto the structural separation between trading authority and custody that is foundational to the Advisers Act framework. An investment adviser exercises discretionary investment authority over client assets but does not have the right to withdraw those assets to itself. In a qualifying vault, this constraint is enforced cryptographically rather than contractually, providing a stronger structural guarantee than the contractual arrangements that govern traditional SMA custody.
- The programmatic preservation of redemption rights (Guardrail 2) directly addresses Wave's experience with token lockup schedules and vesting arrangements. As Veda's letter notes, vault architecture can encode lockup and vesting logic directly in smart contract code, replacing manual compliance workflows with programmatic enforcement. This is a material improvement over current practice, in which lockup enforcement depends on internal administrative controls that are vulnerable to human error, social engineering, and operational failures, each of which can result in premature releases carrying significant regulatory consequences under Rule 144 and Section 4(a)(2) of the Securities Act of 1933, as well as the Advisers Act.
- The cryptographic segregation of withdrawal rights (Guardrail 3) addresses Wave's most fundamental concern about the current custody framework. Namely, the exposure of client assets to intermediary insolvency. The bankruptcies of Celsius Network, Voyager Digital,

and BlockFi demonstrated in stark terms that contractual segregation is insufficient when the legal character of custody arrangements is litigated in insolvency proceedings. Vault architectures in which no participant holds a balance-sheet claim against pooled assets provide structural insolvency protection that does not depend on the specific terms of any user agreement, the outcome of any judicial interpretation, or the regulatory framework governing any particular custodian.

- The no affiliated protocol routing requirement (Guardrail 7) directly addresses a conflict-of-interest concern that is acutely relevant to investment advisers. Wave's fiduciary duty requires it to act in the best interests of clients in all investment decisions, including decisions about which protocols to use for yield generation, staking, and liquidity provision. A vault custody framework that prohibits advisers and vault infrastructure providers from holding material economic interests in underlying protocols, or from receiving compensation based on asset routing decisions, aligns the structural constraints of vault custody with the fiduciary obligations of the investment adviser. Wave supports this guardrail and would welcome Commission guidance confirming that satisfaction of this structural constraint is relevant to, but distinct from, an adviser's ongoing fiduciary obligations under the Advisers Act.

Wave further notes that these structural guardrails reflect a broader principle that leading industry participants and regulators alike are increasingly recognizing. The regulatory standard for custody arrangements should be technology-neutral, evaluated by reference to functional investor protection outcomes rather than the specific technological mechanism through which those outcomes are achieved. The principle that equivalent activities presenting equivalent risks should produce equivalent regulatory outcomes across custody models is one Wave endorses, and that Veda's guardrail-based framework operationalizes for vault-based custody architectures. Wave observes in this connection that other technology-native safeguarding solutions, including multi-signature frameworks and multi-party computation arrangements, which similarly eliminate single points of failure and provide distributed control over private keys, may serve as complementary tools within a broader technology-neutral custody framework, and that the Commission's guidance in this area should accommodate the full range of cryptographic safeguarding models that provide equivalent investor protection outcomes, of which vault architectures satisfying Veda's guardrails represent one compelling category.

IV. VAULT CUSTODY FOR INDIVIDUALLY MANAGED CLIENT ACCOUNTS

A. The SMA Structure and Its Custodial Characteristics

Veda's letter addresses vault custody primarily in the context of pooled investment vehicles, which are funds in which a single vault contract holds the collective assets of multiple investors, with each investor's proportionate entitlement represented by a receipt token. Wave manages a significant portion of its client relationships through Separately Managed Accounts, which are individual client accounts in which each client's assets are managed pursuant to a tailored investment management agreement and held in an account in the client's own name (or in a nominee structure for the client's exclusive benefit), separate from the assets of any other client.

The SMA structure has a well-established custody architecture under Rule 206(4)-2 of the Adviser's Act. The client's assets are held at a qualified custodian in an account that is titled in the client's name or a clearly identified nominee structure. The investment adviser has a limited trading authority over the account, with the authority to direct transactions within the account, but does not have the authority to withdraw assets to itself or to any party other than the client. The qualified custodian enforces this constraint contractually and operationally.

B. Vault Architecture in the SMA Context

Wave respectfully submits that vault architecture in the SMA context is analytically distinct from, and presents an even more compelling case for regulatory recognition than, the pooled fund context that Veda's letter primarily addresses. The distinction turns on where the receipt token is issued and held.

In a pooled fund vault, the receipt token is typically issued to the fund entity, which holds it on behalf of the fund's investors. The client's entitlement to vault assets is mediated through the fund's governance structure and the terms of the fund's governing documents. In an SMA vault context, the architecture can be structured so that the receipt token is issued directly to the individual client, in a wallet controlled by the client or the client's independently designated custodian. In this structure, the client holds direct cryptographic proof of their entitlement to the underlying vault assets. No action by Wave, the vault infrastructure provider, or any affiliate can cause the vault to transfer assets to any wallet other than the client's authorized redemption wallet. The client's redemption rights are cryptographically invariant and independently enforceable.

This structure replicates the custody architecture of the traditional SMA model in every meaningful respect, using cryptographic enforcement rather than contractual enforcement as the mechanism. Wave has the authority to direct investment strategy within the vault, analogous to the limited trading authority in a traditional SMA, but has zero withdrawal authority. The vault smart contract enforces this constraint at the code level, independently of any agreement between Wave and the client. The client's assets cannot be misappropriated by Wave through any mechanism that the vault architecture permits.

C. Superior Investor Protection Characteristics of the SMA Vault Model

Wave submits that the SMA vault model offers investor protection characteristics that are superior to traditional SMA custody in several important respects, and requests that the Commission recognize these advantages explicitly in any guidance addressing vault-based custody.

First, in a traditional SMA, enforcement of the adviser's limited trading authority depends on contractual arrangements between the adviser and the qualified custodian, and on the custodian's operational implementation of those arrangements. If the custodian processes an unauthorized withdrawal instruction, whether due to internal error, fraud, or system failure, the client's only remedy is contractual and legal. In an SMA vault, unauthorized withdrawal is architecturally impossible because the smart contract will not process a redemption instruction from any wallet other than the client's authorized address. The protection is not dependent on any human process.

Second, in a traditional SMA, the client's independent verification of their holdings depends on account statements delivered by the qualified custodian on a periodic basis. In an SMA vault, the client's holdings are continuously verifiable on-chain in real time. The client can independently confirm at any moment, without relying on any intermediary, that their receipt token entitles them to a specified proportion of the vault's underlying assets. This is a materially superior verification mechanism.

Third, in a traditional SMA, the client's assets are exposed to the qualified custodian's operational and insolvency risk. Even with contractual segregation, a custodian insolvency can result in litigation over the status of customer assets, as the recent histories of digital asset custodians and traditional financial institutions alike have demonstrated. In an SMA vault, the client's assets are held in a smart contract in which no vault participant holds any balance-sheet claim. The client's entitlement is protected by the vault's architecture, not by the creditworthiness or regulatory compliance of any intermediary.

Wave therefore respectfully requests that the Commission, in any guidance or rulemaking addressing vault-based custody, explicitly confirm that the SMA vault model in which the receipt token is issued directly to the individual client and redeemable exclusively by the client's authorized wallet satisfies the custody requirements of Rule 206(4)-2 under the Advisers Act with respect to each individual client's account, independently of whether any pooled fund vault custody framework is adopted.

D. Active Investment Management and DeFi Strategy Execution Within the Vault

Veda's guardrail framework, and the vault custody discussion generally, has been framed primarily around the question of static asset holding, that is, whether a vault that securely holds a client's digital assets can satisfy the qualified custodian requirement of Rule 206(4)-2. Wave supports that framing, but respectfully submits that the Commission must also address the more complex question of how vault architecture accommodates active discretionary investment management, including the deployment of client assets into DeFi strategies, which is far more operationally significant for active managers like Wave.

Deploying client assets into DeFi protocols on a discretionary basis involves depositing assets into automated market makers to earn trading fees, providing assets to lending protocols to generate yield, staking assets with validator networks to earn staking rewards, and participating in governance protocols on behalf of clients. Each of these activities involves moving client assets out of passive custody and into a protocol that returns a receipt instrument, such as a liquidity provider token, a lending receipt, a staking receipt, or a vault share, representing the client's claim on the deployed assets and their accrued returns. The vault custody framework must address this execution layer, not merely the holding layer.

Wave submits that a well-designed vault architecture can accommodate active DeFi management through a two-layer model. In the first layer, the so-called custody layer, the vault holds the client's base assets under the structural guardrails Veda proposes, with cryptographic segregation, programmatic redemption rights, and no unilateral withdrawal authority for the adviser. In the second layer, the strategy layer, the adviser exercises limited trading authority to direct the vault to deploy assets into approved DeFi protocols, subject to protocol whitelisting constraints established in the vault's governance parameters. Receipt tokens returned by those protocols flow back into the vault and are attributed to the client's account. At all times, the client's composite position (undeployed base assets plus all outstanding DeFi receipt tokens) constitutes the assets held in custody for purposes of Rule 206(4)-2. The adviser's authority is limited to directing strategy within this structure; withdrawal to unauthorized addresses remains architecturally impossible at both the base asset and receipt token levels.

This two-layer model is the digital asset equivalent of the traditional SMA structure, in which the investment adviser directs trades within an account at a qualified custodian but cannot withdraw assets to itself. The key distinction from the traditional context is that in an active DeFi SMA vault, the "account" is dynamic because it holds a composite of base assets and DeFi receipt tokens whose composition changes as the adviser executes strategy. The vault custody framework must recognize this dynamic composition and confirm that the adviser's authority to execute DeFi transactions, including but not limited to, deposits into protocols, harvesting of accrued yield, rebalancing between positions, and redeployment of receipt tokens, falls within the scope of permissible limited trading authority rather than constituting custody or withdrawal authority. Without this confirmation, active DeFi management within a vault structure carries inadvertent custody risk under the current text of Rule 206(4)-2, notwithstanding the structural protections the vault architecture provides.

Wave further requests that the Commission confirm that a vault custody framework for active DeFi management must specify the treatment of DeFi receipt tokens for purposes of the qualified custody requirement. When an investment adviser deploys a client's digital assets into a staking protocol and receives a staking receipt in return, the question of which instrument, the deployed digital asset or the staking receipt, must be held in custody, and by what mechanism, is unresolved under current guidance. Wave's position is that a vault architecture in which both the base assets (while undeployed) and the receipt tokens (while deployed) are held within the vault and attributed to the client's account should satisfy the custody requirement with respect to both instruments, provided the vault's structural guardrails ensure that neither instrument can be transferred to any unauthorized address. The Commission should confirm this position expressly to eliminate the ambiguity that currently makes vault-based active DeFi management a compliance risk.

Wave notes that the Commission's interpretive release issued March 17, 2026[3] has provided meaningful regulatory clarity in this context, confirming that certain proof-of-stake staking, redeemable wrapped-token arrangements, and airdrops do not constitute securities transactions. Wave respectfully submits that this confirmation, which acknowledges the functional, non-securities character of these common DeFi activities, reinforces the case for a vault custody framework that affirmatively accommodates active DeFi management within its compliance architecture, enabling investment advisers to execute these strategies in compliance with the Custody Rule without inadvertent custody risk or regulatory uncertainty.

V. PRIVACY-PRESERVING TECHNOLOGY AND THE INDEPENDENT VERIFICATION REQUIREMENT

A. The Tension Between On-Chain Transparency and Client Confidentiality

Veda's letter correctly identifies on-chain transparency as a significant advantage of vault-based custody. Vault balances and transaction history are continuously verifiable by any authorized party, providing real-time proof of holdings that periodic account statements cannot replicate. Wave endorses this observation as a general matter and agrees that on-chain verifiability is a material improvement over examination-based oversight for purposes of detecting misappropriation and confirming segregation.

However, Wave's institutional clients present a distinct consideration that Veda's letter acknowledges in a footnote but does not fully develop. Namely, the tension between on-chain transparency and client confidentiality. Wave's clients are sophisticated institutional investors and high-net-worth individuals with material confidentiality expectations regarding the composition of their digital asset portfolios. These expectations arise from multiple sources, including competitive sensitivity (revealing a significant position in a long-tail asset before it is fully established can create adverse price impact); contractual confidentiality obligations owed to portfolio company issuers; regulatory obligations arising under applicable privacy laws; and prudential risk management considerations that counsel against public disclosure of specific holdings.

Public blockchain transparency is by design globally visible. A vault architecture that requires continuous on-chain publication of each client's full portfolio composition, such as balances, positions, and transaction history, would make Wave's institutional clients unwilling to use vault-based custody regardless of its structural merits, because the confidentiality cost would outweigh the custody benefit. This is the same confidentiality tension that has historically led

[3] *See Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets, CFTC and SEC Interpretive Release,* Release Nos. 33-11412; 34-105020, 91 FR 13714 (Mar. 23, 2026).

institutional investors to prefer off-chain or permissioned custody arrangements over fully transparent on-chain structures.

B. Zero-Knowledge Proofs and Selective Disclosure as a Solution

Advances in cryptographic technology have produced a practical solution to this tension. Zero-knowledge proofs ("ZKPs") and selective disclosure mechanisms allow a party to prove a statement about data without revealing the underlying data itself. In the vault custody context, ZKPs and selective disclosure mechanisms can be deployed to provide the following:

- A regulator or authorized examiner can cryptographically verify that a vault holds at least a specified quantity of a specified asset on behalf of a specified client, without that information being visible to any other party, including other clients, market participants, or the general public.
- A client can independently verify the real-time value of their vault holdings without revealing the specific composition of their portfolio to the vault infrastructure provider, the investment adviser, or any third party.
- An independent auditor can generate and publish a cryptographic attestation that a vault's aggregate holdings satisfy all client redemption entitlements (a proof of solvency) without revealing the underlying portfolio composition of any individual client account.
- Regulatory examiners can conduct examinations of vault-based custody arrangements using cryptographic audit trails that provide stronger evidentiary guarantees than traditional account statement review, while preserving the confidentiality of client portfolio information with respect to the general public.

Zero-knowledge proof systems, including zk-SNARKs, zk-STARKs, and commitment-based proof systems, are in production deployment across multiple blockchain networks and are used by institutional participants in digital asset markets today. The cryptographic guarantees they provide are mathematically rigorous and not subject to the manipulation or forgery risks that affect human-administered verification processes.

C. Confidentiality of Proprietary Trading Strategies and On-Chain Transparency

A registered investment adviser's investment strategies are among its most competitively sensitive assets. The timing of trades, the selection of protocols, the sizing of positions, the sequencing of rebalancing transactions, and the specific yield strategies employed by an RIA all reflect substantial research, analytical judgment, and proprietary methodology. In the traditional securities context, custody and settlement infrastructure is private. Brokerage records, custodial statements, and order flow are not publicly accessible, and an adviser's trading activity is not visible to competitors, market participants, or the general public in real time.

The public blockchain environment is structurally different. Every on-chain transaction is permanently and publicly recorded on a distributed ledger that is accessible to anyone with an internet connection. When Wave executes a strategy on behalf of clients that activity is visible on-chain in near real time. Competitors can monitor Wave's wallet addresses, reverse-engineer its strategy, front-run its transactions, or replicate its methodology at no cost. This on-chain transparency is not a feature Wave can opt out of; it is an inherent property of the blockchain infrastructure on which digital asset strategies operate. The custody and reporting frameworks that the Commission develops for digital asset registered investment advisers must account for this structural reality. Any requirement that mandates public on-chain disclosure of client positions or adviser transactions, whether as a condition of custody compliance, examination access, or regulatory reporting, would effectively compel the public disclosure of proprietary investment

strategies and could cause material harm to Wave's clients by dissipating the alpha embedded in those strategies.

Wave submits that the Commission should develop a privacy-preserving compliance architecture that permits regulators to obtain the supervisory information they require without requiring the public disclosure of adviser trading strategies or client portfolio composition. Emerging cryptographic tools, including zero-knowledge proofs and selective disclosure protocols, can enable regulators to verify compliance facts without requiring full on-chain transparency, and the Commission should engage with these tools as it develops its digital asset custody and examination framework.

D. Regulatory Recognition of Privacy-Preserving Verification

Wave respectfully requests that the Commission explicitly recognize privacy-preserving cryptographic verification mechanisms as a compliant alternative to full public on-chain transparency in any vault-based custody framework, subject to the following conditions:

- The privacy-preserving mechanism must provide cryptographic proof of holdings that is verifiable by the Commission and its authorized examiners upon request, with the same evidentiary reliability as direct on-chain observation.
- The mechanism must allow each client to independently verify their own holdings in real time, without reliance on the adviser or the vault infrastructure provider, using cryptographic proof rather than periodic account statements.
- The mechanism must support cryptographic proof of solvency, i.e., proof that aggregate vault holdings are sufficient to satisfy all outstanding client redemption entitlements and that can be verified by an independent auditor and published to the relevant regulatory authority without revealing individual client portfolio compositions.
- The privacy-preserving mechanism must not impair the anti-misappropriation, anti-commingling, or insolvency-protection characteristics of the vault architecture that qualify it for the compliance pathway under the guardrails proposed by Veda.

Wave submits that the adoption of a privacy-preserving verification standard would not compromise the investor protection objectives of Rule 206(4)-2. Rather, it would expand access to vault-based custody for the institutional investor segment, the segment for which confidentiality requirements are most acute, while preserving all of the structural safeguards that make vault custody a meaningful improvement over traditional custody for digital assets. A regulatory framework that requires full public transparency as the price of vault custody recognition would inadvertently exclude the most sophisticated and compliance-conscious segment of the market from accessing a custody model that would serve them well.

Wave further notes that privacy-preserving verification is consistent with the Commission's existing approach to the Custody Rule's independent verification requirement. The surprise examination requirement of Rule 206(4)-2 is designed to ensure that an independent party can verify that client assets exist and are properly segregated. A ZKP-based audit trail that provides cryptographic proof of holdings to an independent auditor satisfies this functional objective, and does so with stronger mathematical guarantees than periodic examination-based oversight, while preserving the confidentiality of portfolio information that institutional clients require.

VI. SUMMARY OF WAVE'S REQUESTS

Wave respectfully requests that the Commission and the CFTC, in any rulemaking or guidance addressing vault-based custody for digital assets:

- **Adopt Veda's guardrail-based compliance pathway.** Recognize qualifying vault architectures satisfying Veda's seven structural guardrails as an additional, technology-native compliance pathway for satisfying the qualified custody and segregation requirements of Rule 206(4)-2 and CFTC Regulations 1.20 and 4.20 respectively, without displacing existing qualified custodian frameworks.
- **Explicitly address the SMA vault model.** Confirm that a vault-based custody arrangement in which the receipt token is issued directly to the individual client and redeemable exclusively by the client's authorized wallet satisfies Rule 206(4)-2 with respect to each individual client account, independently of any pooled fund vault custody framework, and that this structure replicates the functional architecture of the traditional separately managed account custody model.
- **Confirm the two-layer active management model.** Confirm that a vault architecture permitting an investment adviser to exercise limited trading authority to direct deployment of client assets into whitelisted DeFi protocols, with all resulting receipt tokens returned to and held within the vault and attributed to the client's account, satisfies Rule 206(4)-2 without triggering inadvertent custody status, provided that the adviser's authority is limited to strategy direction within the vault and does not extend to withdrawal of assets or receipt tokens to any unauthorized address.
- **Clarify the custodial treatment of DeFi receipt tokens within vault structures.** Confirm that a vault architecture in which both undeployed base assets and DeFi receipt tokens (including LP tokens, staking receipts, lending receipts, and vault share tokens) are held within the vault and attributed to the client's account satisfies the custody requirement with respect to both instruments, provided the vault's structural guardrails ensure that neither the base assets nor the receipt tokens can be transferred to any unauthorized address.
- **Recognize privacy-preserving cryptographic verification.** Confirm that zero-knowledge proof systems and selective disclosure mechanisms that provide cryptographically rigorous proof of holdings to authorized regulators and independent auditors, and real-time self-verification to individual clients, satisfy the independent verification requirements of Rule 206(4)-2 as an alternative to full public on-chain transparency, provided the anti-misappropriation and anti-commingling safeguards of the vault architecture are preserved.
- **Coordinate with the CFTC under the 2026 MOU.** Develop a joint SEC-CFTC vault custody standard through the Joint Harmonization Initiative, using Veda's guardrail framework as the starting point, to reduce compliance friction for dually regulated digital asset managers and ensure that a single structural compliance pathway satisfies both agencies' customer asset protection objectives.
- **Draft in technology-neutral terms.** Ensure that any compliance pathway conditions are drafted by reference to functional and structural characteristics rather than by reference to specific protocols, token standards, or blockchain networks, so that the framework remains durable as cryptographic technology evolves.
- **Clarify "control" in the crypto asset context.** Align regulatory interpretations of "control" in the crypto asset custody context with the concepts established under Uniform Commercial Code Article 12, including the ability to transfer assets, the ability to exclude

others from transfer, and identifiability of the controlling party by name, number, cryptographic key, or account number, to provide legal certainty regarding the enforceability of vault-based custody arrangements and to harmonize federal regulatory standards with evolving state law frameworks.

- **Promote alignment with international regulatory frameworks.** Develop the vault custody standard with awareness of, and appropriate alignment with, applicable international frameworks, including the International Organization of Securities Commissions (IOSCO) Policy Recommendations for Crypto and Digital Asset Markets and the EU Markets in Crypto-Assets Regulation (MiCA) framework's emphasis on segregation, liability, and authorization, to reduce regulatory fragmentation and promote market stability for globally active investment managers and their institutional clients operating across multiple jurisdictions.

VII. CONCLUSION

The Custody Rule's core objectives of preventing misappropriation, prohibiting commingling, and protecting client assets from intermediary insolvency, are as important in digital asset markets as in any other. Vault architectures satisfying Veda's structural guardrails address each of those objectives through mechanisms that are purpose-built for the technical architecture of digital asset markets. A guardrail-based compliance pathway would extend the protective logic of Rule 206(4)-2 to digital asset markets without displacing existing qualified custodian frameworks and without implicitly endorsing any particular investment strategy or protocol.

Wave respectfully submits that the additional recognition of the SMA vault model in which individual client receipt tokens provide direct, cryptographically enforceable redemption rights, and the adoption of a privacy-preserving verification standard would materially strengthen the framework Veda proposes and extend its benefits to the institutional segment of the digital asset management industry. Wave looks forward to engaging with Commission and CFTC staff on the matters raised in this letter and in the Veda Letter, and stands ready to provide additional materials, participate in staff discussions, or respond to any questions the staff may have.

Wave appreciates the Commission's and the CFTC's consideration of these matters.

Respectfully submitted,

Nicole Trudeau
General Counsel
Wave Digital Assets LLC
legal@wavegp.com

cc:

Tuongvy Le, General Counsel, Veda Tech Labs Inc.