

May 12, 2025

**Submitted via SEC Website**

Commissioner Hester M. Peirce  
Chair of SEC Crypto Task Force  
crypto@SEC.GOV  
U.S. Securities and Exchange Commission  
100 F Street NE  
Washington, D.C. 20549-1090

**Re: Investment Adviser Custody and Other Requirements**

Dear Commissioner Peirce and Members of the SEC’s Crypto Task Force:

The Digital Chamber (“TDC”) respectfully provides this submission in response to Commissioner Hester M. Peirce’s February 21, 2025 statement soliciting public input on regulatory issues related to blockchain technology and crypto assets (the “**Statement**”).<sup>1</sup> In particular, this letter addresses Questions 27, 28 and 29 of the Statement related to investment adviser custody and other requirements. TDC will also be providing responses to many of the other questions posed by the Statement in separate submissions.

**Question 27**

**What challenges do registered investment advisers (“RIAs” or “advisers”) face in complying with the Investment Advisers Act of 1940 (“Advisers Act”) as it relates to investments in crypto assets that are securities? What common practices, if any, have developed to address these challenges?**

As a preliminary matter, we believe that the Securities and Exchange Commission (“SEC” or “**Commission**”) should take immediate action to confirm the scope of the existing custody rules with respect to crypto assets. As TDC noted in the comment letter we submitted on May 8, 2023 (the “**Comment Letter**”),<sup>2</sup> with respect to the SEC’s Safeguarding Advisory Client Assets proposed rules changes (the “**Proposal**”),<sup>3</sup> we, along with many other market participants, took strong exception to the inclusion by way of almost purposefully casual dicta the statement that “most crypto assets are likely to be funds or crypto asset securities covered by the current rule.” TDC also noted its concurrence with Commissioner Peirce’s disagreement “with the main premise that most crypto assets are securities and the sub-premise that crypto assets sold in a securities

---

<sup>1</sup> Comm’r Hester M. Peirce, *There Must Be Some Way Out of Here*, U.S. Sec. & Exch. Comm’n (Feb. 21, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>.

<sup>2</sup> <https://www.sec.gov/comments/s7-04-23/s70423-185579-339822.pdf>

<sup>3</sup> See Release No. IA-6240 (Feb. 15, 2023) (the “Release”), 88 FR 14672 (March 9, 2023).

offering are necessarily themselves securities.” We also noted that there is absolutely no legislative, regulatory, or judicial support for the Proposal’s supposition that certain crypto assets might also be “funds” as that term is used under the Federal securities laws. It was then and continues to be our strong belief that this particular statement is contrary to the rules that govern the SEC’s rule making authority. Indeed, it seems that the only purpose of this statement was to convey to registered investment advisers (“**RIAs**” or “**advisers**”) the Commission’s view that it expects them to treat almost all crypto assets as securities or funds for purposes of the existing custody rule, thereby potentially warning advisers away from managing crypto assets on behalf of their clients. It is time to officially reframe the narrative around that problematic assertion and start with a clean slate.

What is now clear under the current administration is that many crypto assets, including bitcoin, ethereum, stablecoins and many other assets, do not fall within the definition of “securities” or “client funds” under the Advisers Act, and should not be pulled into the framework of the existing custody rule. We also fully support former Acting Chair Uyeda’s March 2025 directive to SEC staff to work with the Crypto Task Force to consider appropriate alternatives to the Proposal, including its withdrawal<sup>4</sup>, an action that TDC advocated for in our 2025 SEC Policy Priorities.<sup>5</sup>

We note, however, that regardless of their classification, RIAs have a fiduciary duty to safeguard all client assets under their control. With respect to crypto assets that are neither securities nor funds, this duty can and should be upheld outside the scope of the current custody rule through a principle-based framework grounded in risk management, security, and investor transparency.

### **Limited Availability of Qualified Custodians**

In respect of crypto asset securities, one of the primary challenges facing RIAs is the limited pool of qualified custodians willing to custody crypto asset securities. One significant impediment in this area was Staff Accounting Bulletin 121 (“**SAB 121**”), published by the Commission’s Office of the Chief Accountant in March 2022, and, without a comment period, effective on April 11, 2022. The negative impact of SAB 121 in its application of an asset-specific approach to the treatment of crypto assets held by banking organizations that are registered with the SEC under the Securities Exchange Act of 1934 (the “**Exchange Act**”) cannot be overemphasized. As a result, many SEC-registered banking organizations that act as qualified custodians for other asset classes were unable to provide custody services for crypto assets securities, further limiting the universe of entities that could provide custody services. Happily, SAB 121 was rescinded by the SEC on January 23, 2025.

---

<sup>4</sup> <https://www.sec.gov/newsroom/speeches-statements/uyeda-ici-031725>

<sup>5</sup> <https://digitalchamber.wpenginepowered.com/wp-content/uploads/2024/12/2025-SEC-Digital-Asset-Policy-Priorities-12.18.25.pdf>

While several qualified custodians that were not subject to SAB 121 were willing to support crypto asset securities—such as Anchorage, Fidelity, Coinbase, and BitGo—the range of supported assets is still limited. This is especially problematic in a fast-moving space where new tokens and protocols are constantly being launched. It is worth noting that every blockchain protocol generally requires the development of a custom technology build, which takes a significant amount of engineering work (often taking two to three months), by any financial institution agreeing to provide custody services for the given asset/token. That said, asset coverage has improved significantly in recent years, and custodians are generally quicker to onboard new tokens than they were in the past.

In order to provide RIAs a greater range of options, we urge the Commission to expand the definition of “qualified custodian” to expressly include state-chartered trust companies. As we noted in the Comment Letter, on November 9, 2020, the SEC published “Staff Statement on [Wyoming] Division of Banking’s ‘NAL on Custody of Digital Assets and Qualified Custodian Status’” (the “**Staff Statement on Wyoming**”). In the Staff Statement on Wyoming, the SEC solicited input on whether state-chartered trust companies possess characteristics similar to those of the types of financial institutions the Commission identified as qualified custodians. The Staff Statement on Wyoming was issued in reaction to a letter issued by the Wyoming Division of Banking indicating that, in its view, Wyoming state-chartered trust companies could serve as “qualified custodians” under the custody rule based on the definition of “bank” under the Advisers Act. To date, the Commission has not issued any guidance regarding the facts and circumstances under which a state-chartered trust company could serve as a qualified custodian, yet many of the financial institutions that custody non-security crypto assets on behalf of RIAs in the United States are state-chartered trust companies often registered with the NY Department of Financial Services under the New York Banking Law or with the Wyoming Division of Banking in the State of Wyoming.

The Commission could also consider building flexibility into the definition of “Qualified Custodian” to include other types of entities not expressly enumerated that meet substantially similar standards in order to expand the providers of qualified custody. For example, in adopting the definition, the SEC recognized that advisory clients may trade securities on foreign markets, reside overseas, or have relationships with foreign custodians for other reasons.<sup>6</sup> Consequently, the SEC permitted foreign financial institutions that customarily hold financial assets for their customers to serve as qualified custodians, provided they appropriately segregate client assets. Similarly, allowing state-chartered trust companies or other regulated entities that can meet substantially similar standards to be qualified custodians (*e.g.*, customarily providing custody of client financial assets and segregating client and proprietary assets)—especially for crypto asset securities—would acknowledge practical needs, promote greater competition and innovation, and align with established SEC precedents for custodial flexibility. Moreover, as with its selection of a foreign financial institution, an RIA’s fiduciary obligation would require it to have a reasonable basis for believing the state-chartered trust company or other regulated entity will provide the level

---

<sup>6</sup> See *Custody of Funds or Securities of Clients by Investment Advisers*, Rel. No. IA-2176 (Sept. 25, 2003), 68 FR 56692, 56694 n. 22 (Oct. 1, 2003).

of safety for client crypto asset securities similar to the level provided by other qualified custodians or fully disclose risks attendant to maintaining the crypto asset securities with the selected custodian.<sup>7</sup>

### **RIAs Must Be Able to Engage in Self-Custody Practices When Necessary**

Compounding the issue of the current limited availability of qualified custodians is the fact that there may not always be a qualified custodian prepared or available to custody a given crypto asset security—this creates a number of additional challenges for RIAs. For example, in some cases, RIAs have declined token allocations at the potential detriment of investors or asked portfolio companies to hold tokens until a custodial solution becomes available. The Commission should amend the custody rule to permit an RIA to custody a client’s crypto asset security (“**self-custody**”) in circumstances where the RIA reasonably determines, consistent with its fiduciary duty, that no qualified custodian is available or willing to custody<sup>8</sup> the given crypto asset security or when it is in the clients’ best interests for the RIA to do so.

To manage this risk, RIAs may use various measures, such as multi-party computation (“**MPC**”) cryptographic technology to fragment key control across multiple parties. This can reduce single points of failure and enhance operational security. Additional safeguards may include functional separation, formalized policies and procedures, routine reconciliations and validations, and periodic audits, as appropriate. Depending on their size and expertise, some RIAs may have the technical capabilities to do this internally. Other RIAs may utilize technology provided by third-party custodial vendors while still giving the RIA control over a client’s crypto asset securities for which it provides self-custody.<sup>9</sup>

It is critical that the Commission provide RIAs with the flexibility to utilize the best means possible to custody crypto asset securities as innovative and more secure solutions continue to evolve. As such, we recommend that the Commission issue guidance pending rule proposals to expand the optionality for RIAs under to custody rules with respect to crypto asset securities to allow for use of range of custody options, including self-custody under a principles-based approach whereby RIAs must safeguard crypto asset securities in a manner reasonably designed to protect against theft, misappropriation, and operational risk in a manner fully consistent with the RIA’s fiduciary duty.

Pending a rule amendment, the Commission should provide a non-exclusive “safe harbor” via Commission exemptive order or other binding guidance permitting an RIA to self-custody a crypto asset security focusing on principles-based concepts informed by the current custody rule such as protection of client crypto asset securities, segregation of client and proprietary assets, auditability, and disclosure of potential material risks and conflicts. As is the case with our

---

<sup>7</sup> See *id.*

<sup>8</sup> A mere assertion by a qualified custodian indicating a willingness or theoretical ability to custody a particular crypto asset security, without reasonably demonstrable evidence of its capability to provide such custody services, would be insufficient under this standard.

<sup>9</sup> Fireblocks is an example of the type of technology commonly used by RIAs for this purpose.

recommendation above, an RIA’s fiduciary obligation would require it to have a reasonable basis for believing that it will provide the level of safety for client crypto asset securities similar to the level provided by qualified custodians, or it must fully disclose risks attendant to the RIA’s self-custody of a client’s crypto asset securities. The Commission could also provide non-exhaustive examples of best practices to provide additional clear and practical guidance that RIAs can use to comply with this principles-based approach. In all cases, whether in rule amendments or guidance, the Commission should ensure the guiding principles and conditions are technology neutral ensuring maximum flexibility is provided for RIAs to adopt new technological solutions and appropriate measures to protect client assets as the market continues to develop and innovate.

- a. **Could best execution or recordkeeping obligations, or compliance with Form ADV or Form PF disclosure requirements, be clearer in the crypto asset context?**

### **Form PF**

We do not believe that RIAs generally face significant challenges with Form PF in the context of crypto asset securities. We do believe, however, that there are areas where greater clarity would be welcome. For example, for purposes of Section 5 current reports, it would be helpful if RIAs had clear guidance as to whether certain types of “operations events” unique to crypto assets give rise to a reporting requirement such as:

- A custodian withdrawal freeze that lasts longer than 24 hours;
- A protocol exploit that impacts 5% or more of net asset value; or
- A validator slashing of more than 1% of staked assets.

### **Form ADV**

We believe there are several areas in Form ADV where additional clarity would also be helpful. For example, in Part 1, Item 9A, it is unclear whether RIAs advisers should report crypto assets that are not securities or whether the item is limited strictly to securities. We assume not, but guidance making that clear would be very helpful. In Part 2, RIAs may also struggle with how to accurately disclose risks associated with using non-qualified custodians or custodial service providers, as well as centralized and decentralized trading venues. Given the evolving nature of the crypto ecosystem, it would be helpful for the Commission to provide more guidance on how advisers can meet their disclosure obligations.

Specifically, we encourage the SEC to clarify: (1) whether non-security crypto assets should be reported in Part 1; (2) which types of service providers fall within the disclosure requirements of Sections 5.K and 7.B; and (3) how advisers can satisfy risk disclosure obligations in Part 2 when engaging in custody practices that fall outside traditional frameworks. On (2), it is not clear whether software-based custodial technology solutions fall within the scope of those

sections, particularly when the technology may play a key role in self-custody asset safeguarding. If disclosure of these types of providers is required, it will be necessary to introduce a new code (perhaps “CT” for crypto technology provider) in Sections 5.K and 7.B. And to the extent that RIAs are relying on these types of providers for self-custody solutions, it would seem evident that disclosure would assist exam staff in identifying that such vendors are integral to the RIA’s ability to safeguard assets.

### **Recordkeeping**

The recordkeeping requirements under Rule 204-2 are structured around traditional broker-dealer activity and do not adequately accommodate the realities of on-chain execution. For decentralized transactions, advisers often cannot obtain conventional trade confirmations. In practice, custodians and advisers often capture the transaction hash, block-time, and a USD price from an independent pricing source, and record this data on the blotter to document execution.

We believe the SEC should formally recognize that such a record or a similar type of documentation for trading activities would meet the intent of Rule 204-2’s order ticket requirements for digital asset trades. This would ensure that advisers remain compliant while adapting to evolving execution environments, without compromising the underlying principles of transparency, auditability, or investor protection.

### **Best Execution**

As a fiduciary, an RIA has an obligation to seek to obtain the best execution of a client transactions based on “whether the transaction represents the best qualitative execution for the managed account.”<sup>10</sup> Consistent with its fiduciary duty, an RIA should be able to determine the appropriate trading venue that is in the best interests of its client.

The Commission should issue guidance that maintains the current facts-and-circumstances, principles-based, and qualitative approach for assessing an RIA’s compliance with its best execution obligations while providing practical guidance tailored for seeking best execution of crypto asset securities transactions.

Specifically, in the spirit of focusing on best qualitative execution, we encourage the SEC to provide formal guidance supporting a principles-based “all-in” best execution standard for crypto asset securities transactions—evaluating total economic outcome rather than focusing narrowly on commission costs. For advisers operating in crypto asset markets, meaningful execution factors include not only fill price, but also network fees (such as gas costs), slippage,

---

<sup>10</sup> <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20IA%20Best%20Execution.pdf>.

and trade latency. Moreover, the crypto asset market is fragmented, with varying platform reliability, fees, liquidity, and prices at any given time.

RIAs should be permitted to assess and document best execution using these aggregated metrics, drawn from reliable and independent sources. For example, an adviser might evaluate execution quality using data provided by a qualified custodian that includes fill price, gas fees, and slippage, thereby demonstrating a clear, auditable, and reasonable effort to achieve the best outcome for the client. This approach enables advisers to uphold their fiduciary duty in fast-moving or fragmented digital markets, where execution dynamics differ from traditional broker-dealer models.

Formal recognition of this “all-in” framework would not only align with emerging industry practices, but also enhance regulatory transparency and investor protection by clarifying how advisers should evaluate and report execution quality in digital asset environments.

**b. Do any crypto asset characteristics or market structures place advisory client crypto assets at a greater or different risk of theft, loss, or misappropriation? If so, how can those risks be addressed?**

Certain characteristics of crypto assets and the structure of crypto markets may expose advisory client assets to different risks than other assets when evaluating the risk of theft, loss, or misappropriation. Importantly, different does not mean greater. Unlike traditional financial instruments, crypto assets rely on private keys for control—if those keys are lost or stolen, the assets are typically irretrievable. The immutable nature of blockchain transactions further compounds this risk, as there is no mechanism to reverse unauthorized or mistaken transfers. However, these risks are not that different from the potential risk of total loss that could result a broker-dealer fraudulently commingling assets.

In addition, many crypto assets are deployed into smart contracts, which may be susceptible to bugs or exploits. The use of decentralized finance (DeFi) platforms adds another layer of risk, given the lack of regulatory oversight, the pseudonymous nature of users, and the difficulty of enforcing contractual rights or recovering assets when things go wrong. Centralized venues add counterparty and bankruptcy risk, frequently outside U.S. jurisdiction and beyond SIPC coverage. Again, these risks are not all that different from risks in the traditional securities markets such as software issues creating significant market disruption and losses (e.g., the “Flash Crash”) and counterparty default (e.g., Lehman Brothers).

As mentioned above, we recommend the SEC adopt a principles-based approach allowing RIAs a range of options to custody crypto asset securities, focusing on risk mitigation and secure safeguarding rather than mandating a single method or technology. Under this framework, RIAs

would be expected to maintain controls reasonably designed to protect client assets from theft or loss, in a manner tailored to the specific risks of the assets and platforms involved.

This approach would allow for flexible implementation of best practices—such as multi-party computation (MPC), multi-signature authorization, real-time transaction monitoring, and robust internal access controls—without prescribing specific technical solutions.

Some practices that an RIA could consider adopting to mitigate certain risks inherent in crypto asset securities might include the following:

- **Promote Shared Governance in Custody Structures:** Adoption of custody models that ensure both operational flexibility and legal oversight. For example, where multi-party computation (MPC) or multi-signature schemes are used, an RIA could require that at least one key to be held by a qualified custodian to the extent that a qualified custodian is involved in the custody of the crypto asset securities.
- **Encourage Transparent, On-Chain Asset Verification:** Use of mechanisms to independently verify that custodied assets match client entitlements. One emerging best practice is the use of proof-of-reserve attestations, which allow auditors and advisers to confirm on-chain balances relative to custodial liabilities. These attestations could be issued on a regular cadence and acknowledged by the custodian to ensure reliability and auditability.
- **Define Measurable Cybersecurity Standards Instead of Static Cold Storage Mandates:** Define expectations around cybersecurity risks and outcomes, such as strong key-shard governance, real-time transaction and anomaly monitoring, and periodic incident response testing. Such a compliance program could include, for example, annual governance drills.

**Question 28. Can RIAs trade, stake, vote, or otherwise participate without moving crypto assets outside a qualified custodian? Should the Commission amend the existing RIA custody rule to provide an exception to allow RIAs to move client crypto assets temporarily out of qualified custodial arrangements to engage in staking, voting, or other novel participatory features of crypto assets? If so, should that exception be subject to time limits or other limitations or requirements?**

RIAs should be allowed to transfer assets to exchanges or to temporarily move assets out of qualified custodians, if necessary, without being deemed in violation of the custody rule. Whether an RIA can participate in trading, staking, voting, or other on-chain activities without removing crypto assets from a qualified custodian depends largely on whether the arrangement is

custodial or non-custodial. If the activity takes place within the custodian’s infrastructure—such as through a staking or voting interface provided by the custodian—then the custodian may be able to retain possession or control, and custody compliance can be maintained.

In the case of voting, most governance protocols allow votes to be cast via signed messages without transferring the underlying asset. A qualified custodian can either provide a governance interface or execute votes based on the RIA’s instruction, allowing the asset to remain in custody throughout. Because there is no change in beneficial ownership or actual transfer of the token, this type of activity generally should not raise custody concerns.

Staking rewards and similar entitlements, such as airdrops, can often be claimed directly by the custodian or through automated smart contracts while the underlying token remains in custody.

That said, the “exclusive control” requirement under the Proposal was unclear, particularly in shared-key arrangements involving MPC or multi-signature tools. We do not believe an exclusive control requirement should be applied to crypto asset securities. Alternatively, to the extent it determines an exclusive control requirement is necessary, the Commission should provide clear guidance on what constitutes “exclusive” in the crypto asset securities context, and such guidance should be consistent with any similar concept or guidance for broker-dealer custody requirements. In all cases, the determination of what constitutes “exclusive” should be principles-based, and not prescriptive to ensure flexibility as technology develops. For instance, an RIA could have exclusive control over a client’s crypto asset securities where it has the sole ability to unilaterally transfer, trade or exchange the client’s crypto asset securities (or authorize such action) and no third-party has the ability to stop or delay the RIA’s actions.

Simply put, the Commission should permit RIAs the ability to self-custody crypto asset securities subject to having prudent safeguards. An RIA would need to determine that self-custody is appropriate consistent with its fiduciary duty. As discussed, an RIA would need to have appropriate controls to protect private keys, segregate client and proprietary crypto assets, separate functions and determine that an independent accountant would be capable of reconciling ownership and control of the assets against a third-party ledger, and be subject to periodic appropriate audits.

As stated above, we recommend that the SEC adopt a principle-based approach to allow RIAs to engage in trading, voting, staking and other activities while safeguarding assets. To provide regulatory certainty, this approach could be supplemented with non-exclusive safe harbor provisions for common use cases. For example, the SEC could establish that custody is presumed to be maintained where a qualified custodian offers a native interface for governance voting or staking, or where the custodian can execute such actions pursuant to a standing instruction from the RIA. Similarly, a safe harbor could be provided for arrangements where the custodian, through a verifiable MPC or multi-signature structure, maintains effective veto power over any transfer.

To support this, we propose a framework that focuses on the intent, controls, and documentation surrounding temporary asset movement, rather than imposing prescriptive technical restrictions. This framework could be supplemented with non-exclusive safe harbors that provide clarity for common use cases, without limiting innovation, including:

- **Custodial Involvement and Oversight**: Protocol interactions occur under arrangements where the qualified custodian retains a meaningful role in transaction execution such as maintaining co-signing authority or control through secure key infrastructure. The adviser would demonstrate that asset movement was necessary to complete a specific protocol-defined action (e.g., staking, voting, redemption), and that the structure preserves oversight and traceability.
- **Defined Purpose and Reasonable Return Timeline**: Assets return to the custodian's control as soon as reasonably practicable following completion of the protocol-defined activity. Rather than prescribing a fixed timeline, the adviser would document the intended purpose, expected duration, and rationale for the elapsed time, tailored to the mechanics of the underlying protocol.
- **Recordkeeping and Transparency**: Advisers record key transaction details, including transaction hashes and expected return windows, in a timely manner. In the event that assets do not return to the custodian within the documented time frame, the adviser (and/or custodian) would conduct an internal review or incident protocol and potentially notify clients and/or the SEC depending on the materiality of the event.
- **Diligence Requirement-Testing and Implementation Best Practices**: Protocol interactions are subject to internal controls and due diligence prior to implementation, including test transactions and risk assessments to validate smart contract behavior, withdrawal mechanics, and custodial coordination. Advisers would follow evolving best practices around protocol review, execution controls, and access management to mitigate risk.
- **Support for Off-Exchange Settlement and Future-State Auditing**: The framework should also accommodate emerging practices such as off-exchange settlement and pre-funding models that minimize counterparty and slippage risks while preserving asset custody. Looking ahead, the SEC could support transparency and enforcement by operating

or commissioning on-chain nodes or verification tools to independently confirm transaction execution, return of capital, and asset integrity across major protocols.

**Question 29. What clarifications, if any, are needed in the Advisers Act regulations to address the cold or hot storage of crypto assets held in custody on behalf of a client?**

- a. What requirements, if any, should the Commission consider for the custody of crypto assets held in each type of wallet on behalf of a client? Should the requirements be the same for both types of wallets?**

For the purposes of this question, we understand (i) a “wallet” to be a public address at which the ownership of crypto assets is, or may be, recorded, (ii) a “cold wallet” to be a wallet for which the private key necessary to initiate any transfer from the wallet is stored offline (on a device not connected to the internet), and (iii) a “hot wallet” to be a wallet for which the private key necessary to initiate a transfer from the wallet is stored on a device that is connected to the internet.

A cold wallet or hot wallet may be owned or controlled by either an investment adviser or by a custodian on behalf of an adviser or its client. The Commission should not impose uniform requirements to all wallets, as the risks associated with cold and hot wallets, and wallets controlled by an adviser or by a custodian, present materially different risk profiles. Instead, the Commission should provide principles-based guidance that takes into consideration the type of wallet (e.g., hot vs cold) and the owner/controller of the wallet.

Cold wallets controlled by qualified custodians should be subject to best practices addressing strict physical security, offline key management, tailored disaster recovery policy, and redundancy protocols, but guidance should be flexible enough for custodians to select controls and protections that are most appropriate given their operations and their clients’ use of custodial services. Cold wallets controlled by an adviser (e.g., where it is not possible or practical to hold a client’s crypto assets with a qualified custodian) should be subject to similar obligations, but guidance should contemplate flexibility for advisers to select controls and protections that are most appropriate given their operations and their trading of crypto assets.

In limited circumstances where a qualified custodian is not available for a particular asset or protocol, such as certain DeFi tokens, NFTs, or early-stage protocol assets, advisers may consider direct custody or third-party non-qualified custodian arrangements. In such cases, we recommend the SEC provide a path forward with enhanced safeguards and disclosure requirements. These could include:

- **Shared Oversight through Multi-Signature Custody Structures:** Requirements that assets held outside of a qualified custodian be secured using multi-sig or MPC structures that allow visibility and oversight by independent parties.
- **Enhanced Risk Disclosures:** Clear disclosure of the risks associated with self-custody or use of a non-qualified custodian (e.g., loss, theft, lack of regulatory protections) and the technical controls in place to mitigate those risks.

The use of hot wallets should be subject to all the obligations applicable to cold wallets, as well as additional safeguards intended to address the heightened risks of a hot wallet. Specifically, qualified custodians maintaining hot wallets should adopt enhanced cybersecurity (which may include a SOC-2 attestation), real-time monitoring of all hot wallets, and key segregation (e.g., via multi-party computation or multi-signature requirements), and as well as be subject to third-party auditing or exam at least annually (a qualified custodian might choose to implement these protections in respect of all wallets, hot or cold).

An adviser holding client crypto assets in hot wallets should be subject to corresponding requirements, depending on the circumstances, and should be required to limit the use of hot wallets to that necessary for the adviser to efficiently pursue its client’s investment objectives. Similar to the use of cold wallets, custodians and advisers holding crypto assets in hot wallets should be granted appropriate freedom to design controls and protections that satisfy principals-based requirements, rather than being subject to rigid, prescriptive obligations. In general, advisers should be encouraged to adopt a risk-based framework—where crypto assets are held in cold storage, except where the adviser determines it appropriate to hold those in hot wallets for operational needs, taking into consideration the client’s investment objectives. In some cases, it may be appropriate for an adviser to hold all of a client’s crypto assets in a hot wallet (e.g., where the account is very actively traded).

Further, advisers should be required to disclose, presumably on Form ADV and/or their prospectuses and other offering memoranda, their custody practices, including whether they use hot wallets and whether they self-custody any crypto assets. Disclosure should detail risks raised by the adviser’s custody practices.

**b. How would a requirement to maintain custody of some or all crypto assets in either cold or hot storage affect an adviser’s ability to transact in those crypto assets or otherwise implement its investment strategy?**

An adviser’s use of hot and cold wallets should be determined in the adviser’s discretion based on its client’s investment strategies and the adviser’s fiduciary duties under the Advisers Act. While crypto assets held in a hot wallet may, depending on the controls, be subject to a greater

risk of loss than those stored in a cold wallet, we do not view a requirement that crypto assets be held only in cold wallets as appropriate. However, requiring that an adviser hold all its crypto assets in cold storage could hinder the adviser's ability to implement time-sensitive strategies such as active trading, account rebalancing, staking, or using DeFi protocols. These strategies often depend on the ability to move assets quickly, something not feasible with cold storage. We believe the better approach is to allow advisers to align wallet use with the relevant account's investment strategy, subject to reasonable safeguards and disclosure discussed above in Questions 27 and 29(a).

**c. What means are available to mitigate the risks related to maintaining crypto assets in hot storage?**

Various risk mitigation strategies exist for hot wallet usage. These include adopting a strict wallet creation ceremony to ensure that the private key for each hot wallet is confidential, implementing multi-party computation or multi-signature arrangements for any transfers from the hot wallet, instituting internal policies for the initiation of any transfer from the hot wallet, which may include requiring multi-party approval for transfers, employing tools to continuously monitor and detect anomalous behavior related to hot wallets (potentially with automatic remediation initiated by attempted tamper, unexpected key exports or other anomalous activity), and undergoing regular audits or exams to reconcile crypto assets recorded on a custodian's or adviser's books and records against the on-chain data for the relevant wallet(s).

**Conclusion**

TDC acknowledges the significant efforts of Melissa Bender, Charles Humphreville, Glen Chen, and Brendan Murphy, Ropes & Gray LLP, towards the preparation of this letter. TDC also thanks the many members that contributed their time and expertise towards the development of this letter, including but not limited to, Gavin Meyers, Partner, Pierson Ferdinand LLP, and Bert Stemmler, Shareholder, Polsinelli PC.

If you have any comments or questions relating to the request or would like to arrange a meeting to discuss further, please do not hesitate to contact the undersigned at [Cody@digitalchamber.org](mailto:Cody@digitalchamber.org).

Regards,

*Cody Carbone*

Cody Carbone

cc: Annemarie Tierney, Senior Strategic Adviser, The Digital Chamber  
Melissa Bender, Partner, Ropes & Gray LLP