

UNIT 410

May 7, 2025

Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-0213

Re: Request for Regulatory Guidance – Qualified Self-Custody

Dear Crypto Task Force:

Unit 410, LLC¹ applauds the Task Force’s thoughtful, organized, and open efforts to request and receive public comment in a variety of ways and to build a record as a springboard for the SEC providing “clarity on the application of the federal securities laws to the crypto asset market” while seeking “to foster innovation and protect investors.”² We welcome this opportunity to follow up on our Task Force meeting,³ further respond to the information requests aimed at, as Commissioner Hester M. Peirce initially summarized it, “an appropriate regulatory framework within which advisers can safely, legally, and practically custody client assets themselves or with a third party,”⁴ and respectfully request regulatory guidance with the concepts proposed in **Appendix A** and discussed below.

OVERVIEW

Whether the imagery is a “crypto road trip,” “a regulatory version of an escape room,” or a game of “the floor is lava ... in the dark,” we have been inspired, by Commissioner Peirce’s statements,⁵ to respectfully submit this RFI response and proposal for regulatory guidance to facilitate safe, legal, and practical self-custody solutions for certain digital assets and address a regulatory gap.

We propose a **Qualified Self-Custodian** (“QSC”) framework designed to protect investors and address regulation of registered investment advisers (“RIAs”) that may be deemed to have custody of certain digital assets under Rule 206(4)-2 (“Custody Rule”). It starts from the premise that it is important for U.S. investors and innovation that RIAs be able to participate in new opportunities with digital assets when, in their fiduciary judgment, it is appropriate to do so to serve the objectives and best interests of their clients.⁶ It addresses certain custodial challenges arising from the rapidly evolving nature of digital assets requiring specialized technical expertise to store them and put them to use and the conundrum an RIA faces when traditional Qualified Custodian (“QC”) options are not reasonably available to support the RIA’s need to protect and invest digital assets in order to fulfill its fiduciary duties.

To fill this gap between a lack of secure and reasonable QC options and fulfilling fiduciary duties, we respectfully propose a principles-based QSC framework for RIAs to self-custody certain digital assets so long as they are appropriately qualified to do so within reasonable guardrails to safeguard the digital assets at issue and protect investors consistent with the Custody Rule’s goals and intent. Implementing such a framework for the long-term will likely require rulemaking. We would welcome that. Meanwhile, inspired by the several Staff Statements on crypto-related issues this year,⁷ we respectfully request interim regulatory guidance to address this gap in the near term and have respectfully proposed principled-based concepts in Appendix A that potentially could be adapted into a more fulsome statement or other guidance that the Commission (or its staff) deems appropriate.

¹ Unit 410, LLC is an engineering firm providing noncustodial services to institutions at the forefront of emergent blockchain technologies. It engineers secure, state-of-the-art technology solutions that provide the capabilities for such institutions to self-custody, account for, and protect digital assets and do so in a manner that can be independently audited.

² *Communicate with the Crypto Task Force* (2025), <https://www.sec.gov/about/crypto-task-force>.

³ Crypto Task Force Staff, Memorandum: Meeting with Representatives of Sidley Austin LLP and Unit 410, LLC (Apr. 15, 2025), <https://www.sec.gov/files/ctf-memo-sidley-austin-unit-410-041525.pdf>. See also Unit 410, LLC, Comment Letter, File No. S7-04-23, Proposed Rule Titled Safeguarding Advisory Client Assets (May 5, 2023), <https://www.sec.gov/comments/s7-04-23/s70423-185139-339522.pdf>.

⁴ Comm’r Peirce, *The Journey Begins* at 6 (Feb. 4, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-journey-begins-020425>; see also Comm’r Peirce: *There Must Be Some Way Out of Here* at 21, 27-29 (Feb. 21, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125> (“RFI”).

⁵ *The Journey Begins* (road trip); *There Must Be Some Way Out of Here* (escape room; hat tipping to Bob Dylan); Comm’r Peirce, *Lava and Lamps: Opening Remarks for Crypto Custody Roundtable* (Apr. 25, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-lava-lamps-opening-remarks-crypto-custody-roundtable-042525>. Hat tip to Bob Dylan. In discussing his album *Together Through Life*, Dylan reflected on the elusive nature of inspiration and seizing it when it appears: “Inspiration is hard to come by. You have to take it where you find it.” https://www.azquotes.com/author/4273-Bob_Dylan/tag/inspiration.

⁶ *Commission Interpretation Regarding Standard of Conduct for Investment Advisers*, Rel. No. IA-5248, at 6-9 (July 12, 2019) (“an investment adviser’s obligation to act in the best interest of its client is an overarching principle”) <https://www.sec.gov/files/rules/interp/2019/ia-5248.pdf> (“SEC Fiduciary Interpretation”).

⁷ *Crypto @ SEC* (2025), <https://www.sec.gov/about/crypto-task-force/crypto-sec> (e.g., Staff Statements on Offerings and Registrations of Securities in the Crypto Asset Markets, Stablecoins, Certain Proof-of-Work Mining Activities, Meme Coins).

Briefly, here is how the proposed QSC framework would work. If, in order to fulfill its fiduciary duties, an RIA needs to store and use digital assets that may fall within the Custody Rule's scope⁸ and appropriately documents that, in its fiduciary judgment, secure and reasonable QC options are not available to store and use such digital assets, then the RIA could serve as a QSC for such digital assets in limited circumstances, that is, could self-custody such digital assets so long as the RIA is qualified to do so consistent with certain safeguarding principles outlined below and in Appendix A to protect investors.

Importantly, what is "reasonable" here includes the support level that the RIA, in its fiduciary assessment, believes is appropriate for fulfilling its fiduciary duties to serve the best interests of its client. Thus, for example, if the RIA fiduciarily determines that staking the digital asset at issue is appropriate for the best interests of its client and that secure and reasonable QC options are not available to support staking, then the RIA might reasonably determine that secure and reasonable QC options are unavailable.⁹

Further, as illustrated by our proposal, we urge the adoption of a principles-based framework, rather than prescribing specific security and technological standards for digital assets as, among other reasons, there can be novel technological differences between digital assets from network to network.¹⁰ Executing fiduciary judgment within a principles-based framework is likely to produce the best, most secure, most practical, and most "future proof" regulatory outcome for encouraging RIAs to take advantage of emerging digital asset technology, enhancing investor opportunities and protections, and promoting innovation.

LEGAL BACKGROUND

RIA fiduciary duties and the Custody Rule are two key elements of RIA regulation under the Investment Advisers Act of 1940, as amended ("Advisers Act" or "Act"). Safe, legal, and practical custodying of RIA clients' digital assets should involve and balance both.

Fiduciary Duties. "The Advisers Act establishes a federal fiduciary duty" that since its 1940 outset has been "fundamental to advisers' relationships with their clients under the Advisers Act."¹¹ While this fiduciary duty "is not specifically defined in the Advisers Act or in Commission rules," it "reflects a Congressional recognition 'of the delicate fiduciary nature of an investment advisory relationship'" and "means the adviser must, at all times, serve the best interest of its client."¹² It focuses an RIA on serving "the best interest of its client, based on the client's objectives" and "must be viewed in the context of the agreed-upon scope of the relationship between the adviser and the client."¹³ Further, particularly relevant in the context of this proposal is that "the principles-based fiduciary duty imposed by the Advisers Act has provided sufficient flexibility to serve as an effective standard of conduct for investment advisers."¹⁴

The Custody Rule. Later, in 1962, the Custody Rule was issued to regulate certain custodial practices of RIAs. As amended over time, it is intended "to safeguard client funds and securities from the financial reverses, including insolvency, of an investment adviser and to prevent client assets from being misused, stolen, or misappropriated."¹⁵ In addition to the QC requirement for maintaining RIA "client funds and securities," the Custody Rule requires: (1) notice to clients on how their funds and securities are maintained, (2) account statements, and (3) verifications by an independent public accountant.¹⁶ As illustrated by our Appendix A proposal, these safeguarding protections can be adapted to an analogous QSC framework for digital assets that may come within the Custody Rule's scope and facilitate a secure, legal, and practical self-custodial framework when secure and reasonable QC options are unavailable.

⁸ To the extent particular digital assets are not subject to the Custody Rule, e.g., do not constitute "client funds or securities" (Rule 206(4)-2(a)), they would be outside the scope of the request for regulatory guidance and proposal in this letter. RIAs could, under and consistent with their fiduciary judgment, elect to utilize the self-custodial concepts in this letter for digital assets outside the Custody Rule's scope. Further, the self-custodial concepts for RIAs outlined in this letter are arguably broad and flexible enough that they might conceivably be adapted for self-custodial principles for other Commission-regulated entities that the Task Force may also be exploring. See RFI at Broker-Dealer Custody & Investment Company Custody.

⁹ See, e.g., Bain Capital Crypto, LP, Dragonfly Digital Management, LLC, Electric Capital Partners, LLC, Haun Ventures Management LP, and Ribbit Management Company, LLC, Comment Letter, File No. S7-04-23, Safeguarding Advisory Client Assets at 7, n.16 (May 8, 2023) (A "qualified custodian should not be considered 'available' if it cannot provide a full suite of custodial services beyond simply holding assets and facilitating transactions. To be 'available' in the context of crypto assets means that a custodian must be able to accommodate critical on-chain activities such as staking, voting, and other network participation.") <https://www.sec.gov/comments/s7-04-23/s70423-186379-340322.pdf>.

¹⁰ Jay G. Baris, "SEC Must Solve Its Cryptocurrency Custody Conundrum," *Financial Times* (May 2, 2019) ("As there is no single answer to what kind of security is sufficient, the SEC should take a balanced, practical approach. It should not try to prescribe specific technological standards because what is appropriate for one custodian may not work for another and today's state-of-the-art requirements may become rapidly outdated.") <https://www.ft.com/content/6411aaff-dd80-382f-ab1c-80cae225673d>

¹¹ SEC Fiduciary Interpretation at 6.

¹² *Id.* at 6 & 8.

¹³ *Id.* at 8 & 9 ("The fiduciary duty follows the contours of the relationship between the adviser and its client, and the adviser and its client may shape that relationship by agreement, provided that there is full and fair disclosure and informed consent.")

¹⁴ *Id.* at 9.

¹⁵ Proposed Rule Release, Safeguarding Advisory Client Assets, Rel. No. IA-6240 (Feb. 15, 2023), <https://www.govinfo.gov/content/pkg/FR-2023-03-09/pdf/2023-03681.pdf> ("Safeguarding Rule Proposal").

¹⁶ Rule 206(4)-2(a)(1)-(4); see also *id.* at (6). In 2023, the Commission proposed the Safeguarding Rule Proposal to extend the Custody Rule's reach. Many commenters identified the many reasons why the Safeguarding Rule Proposal was not workable for digital asset custody. A detailed discussion of the issues presented by the Safeguarding Rule Proposal for digital assets is beyond the scope of this request for regulatory guidance. This request focuses on the Custody Rule, as currently in effect.

DISCUSSION

The Regulatory Gap. The Custody Rule’s regulation of custody has not kept up with technology and the marketplace, which creates a Catch-22 for RIAs when secure and reasonable QC options are not available to support RIAs’ need to protect and invest digital assets in order to fulfill their fiduciary duties. The economic and security driver here is the gap between the RIA client objectives for an RIA to hold and participate with emerging digital assets, including the launch of new networks, and the lack of secure and reasonable QC options to support such opportunities.¹⁷

In the rapidly developing world of technology and digitization, new assets have novel and advanced technological features that QCs may not be available to securely and reasonably support—ever or at least not for extended and varying periods. This is true for, but not limited to, novel early-stage blockchain networks and their digital assets. To date, for technology, business, or other reasons, QCs have not moved fast enough to provide timely, full support for cold storage, staking, and other participation at, or even near, launch. This pattern has replayed itself network after network, year after year. The delay often exceeds a year, and can sometimes be over two years. Yet, launch is the time when the staking rewards rates are usually the highest. Network participation (*e.g.*, staking) is necessary to secure networks, and it is incentivized by digital asset rewards. Which is why for risk-appropriate clients, RIAs may, consistent with their fiduciary duties, seek and need to participate early in new networks to meet their clients’ objectives and best interests. Forcing RIAs to sit on the sidelines waiting for QCs hurts U.S. investors and innovation.

Such early opportunities are often more desirable opportunities for some, but they tend to be difficult to securely and reasonably support than later-stage opportunities with more mature networks as they become less novel, easier to support, and more broadly accepted, which may make them more economically feasible for QCs to justify building support. Digital assets have technological features that differentiate them from traditional assets.¹⁸ They rely on code, decentralized networks, cryptography, immutability, the fact that one does not need to place sole trust in any one party for a network to function, and incentivized consensus algorithms to ensure security and integrity, which leads to novel opportunities and advancements, as well as challenges in how to safeguard them.

Securing digital assets requires specialized technical knowledge and capabilities; for example, designing and utilizing cold storage for new digital assets, generating keys/wallets, encrypting of sensitive key data, split access to key material for enhanced security, and protecting the integrity of the electronic systems used against anticipated threats/hazards. Further, participating in novel networks with those digital assets requires specialized technical expertise, including in cryptography, cybersecurity, computer science, distributed networking, varying coding and programming languages, developing bespoke software and infrastructure, and other technology functions. The more nascent and novel the network, the more difficult these challenges are.

Nimble institutions with the necessary engineering resources and experience in such areas have proven able, unlike QCs, to securely support early-stage digital assets and participation in novel networks at their outset. Over time, QC options may become available, but usually only in phases of partial support. For instance, QCs may come to support cold storage for a particular digital asset, but not more advanced functionality, including participation necessary for securing the relevant network with that digital asset. That cold storage level support may be sufficient in some RIA situations, but not necessarily all, including potential hybrid approaches. Until or if QCs securely, timely, and fully support all forms of participation for a particular network, RIAs need secure and practical self-custodial options to fill the gap and serve and protect the best interest of their clients.

Also important is having the technical knowledge and capabilities to securely support necessary accounting, audit, and administrative functions for novel, complex technology environments. Developing technology to interface with a novel, early-stage network to track and account for rewards and to map complex data from the network to make it intelligible/usable for accounting, reporting, tax, and other purposes is difficult. Doing this at a level that is secure, meets RIAs’ fiduciary responsibilities, is independently verifiable/auditable, and complies with safeguards like the Custody Rule’s is possible today for novel networks at launch, but only with

¹⁷ See, *e.g.*, nn.3 & 9 *supra*; CoinFund Management LLC, Crypto Task Force Meeting Letter at § 1 (Feb. 25, 2025) (“Qualified Custodians...often only begin to support a specific digital asset after broader market adoption of the digital asset emerges, as supporting a new protocol often involves additional infrastructure investment by the custodian. In our experience, this often happens well after one of our clients has acquired a particular digital asset for its investment portfolio, and at times, custodians have only implemented custodial support for novel assets at our request for such support. This lack of ready-made qualified custodian solutions for client assets is a challenge that requires a registered investment adviser to satisfy different, and sometimes conflicting, obligations in selecting a safekeeping approach: on the one hand, a registered investment adviser is mindful of the broad application of the Custody Rule’s requirement to hold client funds and securities with Qualified Custodians within meaning of the rule; on the other hand, a registered investment adviser is obligated to evaluate and execute investments that its clients have engaged it to pursue....”) <https://www.sec.gov/files/memo-coinfund-management-llc-030425.pdf>.

¹⁸ The Division of Investment Management staff has noted some of the novel and emerging features of digital assets and their custodial challenges: “These characteristics include, for example, the use of [blockchain/distributed ledger technology (“DLT”)] to record ownership, the use of public and private cryptographic key pairings to transfer digital assets, the ‘immutability’ of blockchains, the inability to restore or recover digital assets once lost, the generally anonymous nature of DLT transactions, and the challenges posed to auditors in examining DLT and digital assets.” Paul G. Cellupica, Deputy Director and Chief Counsel, Division of Investment Management, *Engaging on Non-DVP Custodial Practices and Digital Assets* (Mar. 12, 2019), <https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206>.

specialized technical expertise. Here too, until or if QCs securely, timely, and fully support the bespoke technology for accounting, audit, and administration for novel networks, RIAs will need secure and workable self-custodial options.

The Solution = Qualified Self-Custody. RIA self-custody would fill the gap. The value of and need for RIA self-custody has become increasingly recognized.¹⁹ We accordingly appreciate that the RFIs specifically asked: “Should the Commission propose any specific changes to its rules to accommodate the self-custody of crypto assets by entities registered with the Commission?”²⁰ Answer: Yes. Likewise, Commissioner Peirce was spot on at the Task Force’s recent Crypto Custody Roundtable in observing:

*Our regulatory approach should recognize the differences across crypto assets. Qualified custodians exist for some crypto assets, but for others self-custody might be the safer option.... [W]e should acknowledge and welcome the fact that blockchain technology empowers investors by allowing them to self-custody, trade, and otherwise engage with their assets without the use of any intermediary. Our regulatory framework should not stand in the way of these innovations by forcing intermediation.*²¹

Self-custody here does not mean the Wild West, however. The relevant questions quickly become, not should RIAs self-custody digital assets, but when and how should RIAs self-custody digital assets. As the RFIs aptly asked: “what conditions should apply to self-custody arrangements to mitigate any related risks?”²²

The answer lies in a QSC framework. At a high level, it has two main objectives: (1) documented procedures to determine, consistent with the RIA’s fiduciary judgment, if secure and reasonable QC options are not available to store and use the specific digital asset in question, and, if so, if it is in the RIA client’s best interests for the RIA to self-custody and (2) safeguarding protections analogous to those under the Custody Rule. If (1) and (2) are met for a specific digital asset, then the RIA would qualify as a QSC for that digital asset, would document and disclose that to its clients, and would then be permitted to self-custody the digital asset in question, subject to periodic review and reassessment.

Specifically, it would be implemented through a principles-based approach with reasonable guardrails to safeguard the self-custodied digital assets at issue and protect investors consistent with the Custody Rule’s goals and intent. It, again, would work as follows: If, in order to fulfill its fiduciary duties, an RIA needs to store and use digital assets that may fall within the Custody Rule’s scope and appropriately documents that, in its fiduciary judgment, secure and reasonable QC options are not available to store and use such digital assets, then the RIA could serve as a QSC for such digital assets in limited circumstances, that is, could self-custody such digital assets so long as the RIA is qualified to do so consistent with safeguarding principles to protect investors.

Such principles for a broad, yet still practical principles-based approach that would govern RIAs and regulate the QSC framework can be, we respectfully submit, distilled to the following:

Each RIA that acts as a QSC for a specific digital asset that may fall within the scope of the Custody Rule must:

- 1. QC Unavailability.** *Adopt and implement written policies and procedures reasonably designed to evaluate and document, in the RIA’s fiduciary judgment and on a digital asset by digital asset basis, that secure and reasonable QC options are not available to store and use the digital asset at issue. In assessing reasonableness, an RIA may take account of the support level that the RIA, in its fiduciary judgment, believes and documents is appropriate for fulfilling its fiduciary duties to serve the best interests of its client. For example, if the RIA fiduciarily determines that staking the digital asset at issue is appropriate for the best interests of its client and that secure and reasonable QC options are not available to support staking, then the RIA may reasonably determine that secure and reasonable QC options are unavailable for purposes of the evaluation contemplated by this Paragraph.*
- 2. Qualified to Self-Custody.** *Adopt and implement written policies and procedures reasonably designed to evaluate and document, in the RIA’s fiduciary judgment and on a digital asset by digital asset basis, that the RIA is qualified to securely and reasonably self-custody the digital asset at issue; that is, the RIA has the appropriate cold storage, operational, staking, participational, and other relevant capabilities to securely and reasonably protect and use the digital asset at issue, either in-house, with the support of a*

¹⁹ See, e.g., nn.3, 9, & 17 *supra*; Paradigm Operations LP, Crypto Regulatory Reform Recommendations at 7 (Jan. 20, 2025) (“permit[] an adviser to engage in self-custody, subject to certain minimal conditions such as the existence of written risk controls, in the event that the adviser is unable to identify a qualified custodian with suitable capabilities to maintain custody of a particular crypto asset”) <https://www.sec.gov/files/memo-paradigm-operations-lp-021825.pdf>; a16z, Comments on the SEC Crypto Task Force’s Questions Concerning the Custody of Crypto Assets at 10 (Apr. 9, 2025) (“Faced with these complexities, many compliance-minded RIAs have resorted to self-custody as a potential balance between the need for secure custody and the deployment of the full range of rights associated with the asset. In custodying crypto assets, such RIAs have sought to meet the principles underlying the Custody Rule—namely security and segregation of the assets, independent audit or verification of the assets, and timely disclosures regarding the assets to RIA clients.”) <https://www.sec.gov/files/ctf-input-horowitz-040925.pdf>.

²⁰ RFI at 21; see also *The Journey Begins* at 6.

²¹ *Lava and Lamps*.

²² RFI at 21; see also *Lava and Lamps* at 10.

noncustodial technology provider, or by other secure and reasonable means that the RIA fiduciarily determines is appropriate to serve its client's best interests.

- 3. Annual Review.** *Perform a documented review, no less frequently than annually, of (a) the determinations under Paragraphs 1-2 that justified serving as a QSC for a digital asset, (b) the adequacy of the policies and procedures under Paragraphs 1-2 and the effectiveness of their implementation, and (c) the adequacy of the security protections put in place in order to serve as a QSC under Paragraph 2 and the effectiveness of their implementation.*
- 4. Recordkeeping.** *Maintain, for at least three years in an easily accessible place, a copy of (a) the policies and procedures adopted under Paragraphs 1-2 that are in effect, or within the past three years were in effect, (b) the documentation of the determinations under Paragraphs 1-2 that justified serving as a QSC for a digital asset, and (c) the documented reviews under Paragraph 3.*
- 5. Additional Protections.** *Provide, in addition to the security protections put in place in order to serve as a QSC under Paragraph 2, additional protections analogous to those in the Custody Rule:*
 - a. Notice to clients.** *The client is provided appropriate and timely written notice reasonably designed to adequately inform the client that the RIA is acting as a QSC for the digital asset at issue (cf. Rule 206(4)-2(a)(2)).*
 - b. Account statements to clients.** *The client is provided an account statement, at least quarterly, identifying the amount of digital assets in the account at the end of the period and setting forth all transactions in the account during that period (cf. Rule 206(4)-2(a)(3)).*
 - c. Independent verification.** *The digital assets at issue are verified at least once a year in a manner analogous to the requirements of Rule 206(4)-2(a)(4) and (6) (e.g., independent public account, internal control report).*

These principles are also presented in a proposal context/format in Appendix A that, again, could potentially be adapted into a more fulsome statement or other guidance as the Commission (or its staff) sees fit. They also could be repurposed for future rulemaking efforts that the Commission may be evaluating.

Two additional considerations. First, how is the RIA to determine what is a digital asset for purposes of the above QSC evaluation? Our suggestion is to define it flexibly and practically as an asset having "Technological Functions," meaning (1) functions or activities necessary to interact with, use, or support the asset with novel, advanced, or complex technological features and requiring specialized technical expertise or (2) functions, attributes, or uses of the asset that require specialized technical expertise. Such expertise may include computer coding and programming, cybersecurity, developing customized software or infrastructure, or developing customized technology solutions to map and use complex computer data.

Second, how is the RIA to make the QC unavailability and QSC appropriateness assessment under Paragraphs 1-2 above? Fiduciary responsibilities should be the guide, and we have compiled in **Appendix B** a non-exclusive list of recommended factors and best practices that institutions consider and use to make such assessments.

CONCLUSION

We respectfully submit that the proposed QSC framework provides an "appropriate regulatory framework within which advisers can safely, legally, and practically custody client assets themselves or with a third-party." We respectfully request the adoption of the QSC framework via regulatory guidance in order to provide greater clarity on the application of the Custody Rule to situations where secure and reasonable QC options are not available to support RIAs needing to protect and invest digital assets in order to fulfill their fiduciary duties. We welcome the opportunity to discuss this with you further. Please do not hesitate to reach out to me or our counsel, Jay G. Baris (jbaris@sidley.com) of Sidley Austin LLP, with questions or to schedule a follow-up meeting.

Sincerely,
UNIT 410, LLC
s/Michael J. Nelson
Michael J. Nelson
General Counsel
michael@unit410.com

cc: Rob Witoff, Co-Founder, Unit 410, LLC
Drew Rothstein, President, Unit 410, LLC
Jay G. Baris, Senior Counsel, Sidley Austin LLP
Lilya Tessler, Partner, Sidley Austin LLP
Chuck Daly, Partner, Sidley Austin LLP
Andrew J. Sioson, Partner, Sidley Austin LLP

APPENDIX A

PROPOSED CONCEPTS THAT COULD POTENTIALLY BE ADAPTED INTO A MORE FULSOME STATEMENT *(inspired by and similar to those at <https://www.sec.gov/about/crypto-task-force/crypto-sec>)*

STATEMENT ON RIA SELF-CUSTODYING DIGITAL ASSETS

Introduction

As part of an effort to provide greater clarity on the application of the Custody Rule (Rule 206(4)-2) to digital assets that may fall within the Custody Rule's scope, the Division of Investment Management is providing its views on Registered Investment Advisers ("RIAs") self-custodying digital assets.

Multiple commenters have noted, including in response to the proposed Safeguarding Rule in 2023 (Rel. No. IA-6240) and Commissioner Hester M. Peirce's February 21, 2025 [Requests for Information](#) ("RFIs"), that traditional Qualified Custodian ("QC") options (Rule 206(4)-2(d)(6)) are not always available to support RIAs needing to protect and invest digital assets in order to fulfill their fiduciary responsibilities, especially for new and emerging digital assets requiring specialized technical expertise to store them and put them to use. To fill this gap between a lack of secure and reasonable QC options and fulfilling fiduciary duties, commenters have suggested that RIAs self-custody digital assets so long as they are appropriately qualified to do so within an appropriate framework to safeguard the digital assets at issue and protect investors consistent with the Custody Rule's goals and intent.

Further, the Commission's Crypto Task Force is exploring "an appropriate regulatory framework within which advisers can safely, legally, and practically custody client assets themselves or with a third-party." (Feb. 4, 2025 [Statement](#) at No. 6; *see also, e.g., RFI* at Nos. 21, 27-29). The Division is issuing this statement to provide its views during the pendency of these deliberations.

RIA Self-Custody

It is important for U.S. investors and innovation that RIAs be able to participate in new investment opportunities with digital assets when, in their fiduciary judgment, it is appropriate to do so to serve the objectives and best interests of their clients. It is also important that RIAs have the ability to custody digital assets that may fall within the Custody Rule's scope in a manner consistent with the Advisers Act and to protect investors. If, in order to fulfill its fiduciary duties, an RIA needs to store and use digital assets that may fall within the Custody Rule's scope and appropriately documents that, in its fiduciary judgment, secure and reasonable QC options are not available to store and use such digital assets, then the Division will not object to the RIA serving as a "Qualified Self-Custodian" ("QSC") for such digital assets, that is, self-custodying such digital assets so long as the RIA is qualified to do so in a manner that is consistent with the principles outlined below to ensure protection of investors.

Principles for Serving as a Qualified Self-Custodian

Each RIA that acts as a QSC for a specific digital asset that may fall within the scope of the Custody Rule must:

- 1. QC Unavailability.** Adopt and implement written policies and procedures reasonably designed to evaluate and document, in the RIA's fiduciary judgment and on a digital asset by digital asset basis, that secure and reasonable QC options are not available to store and use the digital asset at issue. In assessing reasonableness, an RIA may take account of the support level that the RIA, in its fiduciary judgment, believes and documents is appropriate for fulfilling its fiduciary duties to serve the best interests of its client. For example, if the RIA fiduciarily determines that staking the digital asset at issue is appropriate for the best interests of its client and that secure and reasonable QC options are not available to support staking, then the RIA may reasonably determine that secure and reasonable QC options are unavailable for purposes of the evaluation contemplated by this Paragraph.
- 2. Qualified to Self-Custody.** Adopt and implement written policies and procedures reasonably designed to evaluate and document, in the RIA's fiduciary judgment and on a digital asset by digital asset basis, that the RIA is qualified to securely and reasonably self-custody the digital asset at issue; that is, the RIA has the appropriate cold storage, operational, staking, participational, and other relevant capabilities to securely and reasonably protect and use the digital asset at issue, either in-house, with the support of a noncustodial technology provider, or by other secure and reasonable means that the RIA fiduciarily determines is appropriate to serve its client's best interests.
- 3. Annual Review.** Perform a documented review, no less frequently than annually, of (a) the determinations under Paragraphs 1-2 that justified serving as a QSC for a digital asset, (b) the adequacy of the policies and procedures under Paragraphs 1-2 and the effectiveness of their implementation, and (c) the adequacy of the security protections put in place in order to serve as a QSC under Paragraph 2 and the effectiveness of their implementation.

- 4. Recordkeeping.** Maintain, for at least three years in an easily accessible place, a copy of (a) the policies and procedures adopted under Paragraphs 1-2 that are in effect, or within the past three years were in effect, (b) the documentation of the determinations under Paragraphs 1-2 that justified serving as a QSC for a digital asset, and (c) the documented reviews under Paragraph 3.
- 5. Additional Protections.** Provide, in addition to the security protections put in place in order to serve as a QSC under Paragraph 2, additional protections analogous to those in the Custody Rule:
 - a. Notice to clients.** The client is provided appropriate and timely written notice reasonably designed to adequately inform the client that the RIA is acting as a QSC for the digital asset at issue (*cf.* Rule 206(4)-2(a)(2)).
 - b. Account statements to clients.** The client is provided an account statement, at least quarterly, identifying the amount of digital assets in the account at the end of the period and setting forth all transactions in the account during that period (*cf.* Rule 206(4)-2(a)(3)).
 - c. Independent verification.** The digital assets at issue are verified at least once a year in a manner analogous to the requirements of Rule 206(4)-2(a)(4) and (6) (*e.g.*, independent public account, internal control report).

APPENDIX B

SAMPLE FACTORS AND BEST PRACTICES TO ASSESS QC UNAVAILABILITY AND QSC APPROPRIATENESS

1. The best interests of the RIA client.
2. Consistency with the purposes of the Custody Rule and the RIA's fiduciary responsibilities.
3. Use of industry-leading administrative, technical, and physical safeguards for novel networks to protect the security and integrity of the electronic systems used and to protect against anticipated threats/hazards to such systems.
4. Industry-leading competence and knowledge regarding security practices for digital assets and networks.
5. Ability to generate cryptographic keys that allow use of the digital asset at issue.
6. Ability to securely and durably encrypt and maintain sensitive information using industry standard encryption keys generated with leading cryptographic methods.
7. Ability to decrypt keys in order to securely use the digital asset.
8. Ability to support participation in the network at issue fully, including staking, governance, and other forms of current and expected participation on the network.
9. Ability to support key management consistent with best practices around multi-party computation, offline signing, hardware signing modules, and co-signer workflows.
10. Ability to support reasonable reporting requirements around key access, key reconstitution, and key usage.
11. Ability to support reasonable documentation requirements for key backup and recovery scenarios across fault domains.
12. Ability to support accounting, audit, and administrative solutions to appropriately and securely interface with the network to produce institutional-grade accounting data to support at least quarterly account statements to RIA clients and at least annual audits by an independent public accounting firm.
13. Ability to support large nodes on a novel network, consistent with the best interests of RIA clients.
14. Ability to receive airdrops or other yet-to-be-conceived network opportunities.
15. Ability to provide 24/7 monitoring for chain stoppages, forks, missed blocks, and other novel challenges to minimize risks of loss, including slashing and opportunity costs.
16. Ability to identify and segregate digital assets for the network consistent with the Custody Rule.
17. Ability to ensure the security, authenticity, and accuracy of cryptographic operations, factoring in the risks/complexities of a network and to ensure no single party or device has the ability to initiate/finalize a cryptographic operation.
18. Ability to identify and mitigate/stop new security threats.
19. Ability to securely split access to keys and physically distribute them at-rest for enhanced security purposes.
20. Whether there is a concentration of QC options that could unreasonably increase security risks.
21. Whether the foregoing abilities can be appropriately provided with industry-leading security, infrastructure, software, speed, reliability, responsiveness, and reasonableness.
22. Whether relevant, reasonable, and appropriate insurance coverage is in place.
23. Whether there are secure and reasonable options to outsource certain noncustodial support functions (*e.g.*, engineering, software design, infrastructure design, running nodes) and whether any such QSC-RIA outsourcing is in RIA clients' best interests.
24. If QC options have some, but not all, of the foregoing abilities, then the RIA should consider whether it is in the best interests of its clients for the RIA to act as a QSC until secure, timely, and fulsome QC options are available or if a hybrid approach is in the best interests of its clients.