

MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Sidley Austin LLP and Unit 410, LLC

On April 15, 2025, Crypto Task Force Staff met with representatives from Sidley Austin LLP and Unit 410, LLC.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Sidley Austin LLP and Unit 410, LLC representatives provided the attached documents, which were discussed during the meeting.

March 12, 2025

Crypto Task Force
U.S. Securities and Exchange Commission
100 F. Street, NE
Washington, DC 20549

Agenda:

- To discuss a proposal for a method of custody of innovative and technology-driven digital assets when a traditional custody arrangement as contemplated by rule 206(4)-2 is not available or practical.

Attendees:

- Jay G. Baris, Senior Counsel, Sidley Austin LLP
- Michael Nelson, General Counsel, Unit 410, LLC
- Drew Rothstein, President Unit 410, LLC
- Rob Witoff, Co-Founder and Board Member, Unit 410, LLC

Discussion Areas:

- The Gap – To date, QCs under Rule 206(4)-2 are generally unable to move fast enough to provide full technology support for cold storage and staking when new blockchain networks launch. Requiring registered investment advisers (RIAs) to sit on the sidelines for months or years waiting for QCs to catch up hurts US investors and US innovation.
- The Solution – “Qualified Self-Custody” or “QSC” (e.g., [Comment letter dated May 5, 2023](#)). When a traditional custody arrangement is not available or practical, QSC is an approach for RIAs to self-custody digital assets, but only if they do so within a secure and reasonable framework to protect investors.
- The Relief – We request this Task Force meeting to explore pro-investor and pro-innovation options and relief in this area for both the near and long term. We hope to seek regulatory guidance to support QSC solution through SEC or staff guidance or rulemaking (including interim guidance in the form of a no-action letter).

Analysis:

- See attached PowerPoint presentation.



Framework for Custody of Digital Assets by Investment Advisers: Promoting Innovation with Investor Protection

Unit 410



INTRODUCTION

Summary

- We propose an additional framework to regulate custody of certain client assets by registered investment advisers (RIAs)
- Specifically, the framework is designed to provide a custody rule-compliant solution for new or emerging digital assets that require complex “Technology Functions” (defined below) that QCs may not be available to timely, securely, and reasonably support
- The framework provides a regulatory structure that enhances investor protection and encourages investment advisers to take advantage of emerging digital asset technology
- Primary goals:
 - Foster innovation in emerging digital assets that require emerging “Technology Functions” to address current regulatory requirements
 - Encourage RIAs to adopt new practices to best serve their clients
 - Addresses public policy concerns by increasing protection of digital assets through regulatory oversight and internal compliance policies and procedures designed to prevent overreaching by bad actors

The Challenge

- Rule 206(4)-2, the “custody rule”, has requirements for RIAs to custody funds and securities with a “qualified custodian” (“QC”)
- While QCs custody arrangements may work in traditional settings, many QCs lack the capacity to provide timely, secure, and reasonable support for digital assets with emerging Technology Functions
 - Technology Functions include
 - Functions or activities necessary to interact with, use or support an asset with novel, advanced, or complex technological features and require specialized technical expertise and
 - Functions, attributes or uses of a digital asset that require specialized technical expertise
- As new digital assets and novel network protocols and blockchains evolve, QC custody is not available – at least not for a long time
- As a result, RIAs often need to self-custody digital assets, which is an area in need of regulatory clarity
 - See, e.g., #6 on the Task Force’s 2/4/25 policy listing: *“an appropriate regulatory framework within which advisers can safely, legally, and practically custody client assets themselves or with a third-party”* ([link](#))

The Solution – Qualified Self-Custody

- We propose a regulatory hybrid to authorize an RIA to serve as a **Qualified Self-Custodian** (“QSC”) under certain conditions
- A QSC solution allows RIAs to self-custody certain early-stage technological assets when secure and reasonable QC custody is unavailable, *but* only if the RIAs do so within a secure and reasonable framework to protect investors

Regulatory Gap

- As new digital assets and networks rapidly develop and evolve, QC custody may be unavailable because they cannot support Technology Functions
 - QCs often lack capacity to provide timely technical support for emerging networks that become available to RIAs
 - Safeguarding emerging digital assets requires specialized technical knowledge and capabilities, including, among others
 - Generating, encrypting and decrypting keys to protect and use emerging digital assets in cold storage
 - Staking and otherwise participating in novel networks with emerging digital assets requires specialized technical expertise, including
 - Cryptography
 - Cybersecurity
 - Computer science
 - Distributed networking
 - Varying coding and programming languages
 - Developing bespoke software and infrastructure
- RIAs that cannot find a QC capable of securely and fully supporting an emerging digital asset will forgo staking and other participation opportunities, thereby denying investors access to emerging digital assets and hurting US innovation

The Solution: Qualified Self-Custodian

- A QSC solution would **fill the regulatory gap** by allowing an RIA to self-custody digital assets, subject to safeguards that are analogous to those provided by a QC, but only when an appropriate QC is not available to securely and reasonably provide support for digital assets
- An RIA could serve as a QSC, provided the QSC reasonably demonstrates and documents that:
 - QC options are not reasonably available
 - It is in the client's best interests to maintain digital assets with a QSC
 - The QSC establishes and implements specific policies and procedures designed to safeguard client assets
- How does an RIA assess a QC's ability to provide required Technology Functions?
 - RIAs first evaluate whether a QC is capable of supporting the Technology Functions needed to provide secure and reasonable support for an emerging digital asset
 - The RIA will evaluate the QC's ability to provide, among other factors:
 - state-of-the-art cold storage
 - highly functional wallets
 - full ability to stake and participate in networks
 - ensure security, authenticity and accuracy of cryptographic functions
 - security interface with networks to produce institutional-grade accounting data
 - claim airdrops
 - 24/7 monitoring to minimizing slashing risks
 - Independent audits
- *See Appendix A for a more complete list of standardized factors and practices*

QSC Safeguards

- When the RIA completes and documents its evaluation that serving as a QSC is necessary and appropriate, it may serve as a QSC on its own and/or by engaging a qualified provider to support the required Technology Functions
- The QSC would have:
 - Documented safeguarding policies and procedures
 - The client's written consent for an RIA to serve as the QSC
 - Requirements for the RIA to implement written policies and procedures reasonably designed to determine, periodically reassess, and document whether an asset is an asset with technology functions, whether the asset is appropriate for the client, and whether the asset's technology functions are not securely and reasonably supported by qualified custodians
 - Periodic independent audits of effectiveness of policies and procedures and existence of digital assets themselves

Benefits of a QSC framework

- Promotes innovation of technology and markets
- Promotes competition
- Improves overall network security by not centralizing assets with a limited number of custodians
- Avoids off-shore alternatives
- Empowers US investors

The Role of Technology Function Support Services

- Supporting Technology Functions that facilitate custody and safe transactions involving digital assets that QCs cannot or will not provide
 - Provides a higher level of safety and security than QCs provide
- Not a custodian
- Adapts rapidly to changing markets and technologies

Next Steps

- We encourage active engagement of industry stakeholders
- To achieve these objectives, the Commission and its Staff can proceed in any of several paths
 - No-action letter (short term relief)
 - Staff interpretive guidance (short term relief)
 - Issue custody concept release and request for comment, either as part of an effort to address custody of assets overall or limited to this issue (longer term relief)
 - Exemptive rule (longer term relief)

Appendix A – Best Practices for QSC

- Must be in the best interests of the RIA client.
- Consistency with the purposes of the Proposed Safeguarding Rule and the RIA's fiduciary responsibilities
- 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
- Industry-leading competence and knowledge regarding security practices for digital assets and Networks
- Ability to generate cryptographic keys that allow use of the digital asset at issue
- Ability to securely and durably encrypt and maintain sensitive information (e.g., login passwords, RSA tokens, and private keys) using industry standard encryption keys generated with leading cryptographic methods
- Ability to decrypt keys in order to securely use the digital asset
- Ability to support participation in the Network at issue fully, including staking (including auto-restaking and future Network functions to best serve RIA clients' interests), validating, collating, delegating (including the ability to delegate to someone other than the QC/QSC if it is in RIA client's best interests to do so), voting, and/or other forms of current and expected participation on the Network
- 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

Appendix A – Best Practices for QSC (continued)

- Ability to support large nodes on a novel Network, consistent with the best interests of RIA clients
- Ability to receive airdrops or other yet-to-be-conceived Network opportunities
- 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
- Ability to identify and segregate digital assets for the Network consistent with the Proposal
- 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
- Ability to identify and mitigate/stop new security threats
- Ability to securely split access to keys and physically distribute them at-rest for enhanced security purposes
- Whether there is a concentration of QC options that could unreasonably increase security risks
- Whether the foregoing abilities can be appropriately provided with industry-leading security, infrastructure, software, speed, reliability, responsiveness, and reasonableness
- Whether there are secure and reasonable options to outsource certain noncustodial support functions (e.g., engineering software design, infrastructure design) and whether any such QSC-RIA outsourcing is in RIA clients' best interests
- 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