



By Email Submission to IMOCC@sec.gov

November 15, 2022

Sarah G. ten Siethoff

Deputy Director
Division of Investment Management
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: Custody Rule and Digital Assets

Dear Deputy Director ten Siethoff:

The **Wall Street Blockchain Alliance** (“*WSBA*”) appreciates that the staff of the Securities and Exchange Commission’s Division of Investment Management (the “*Division*”) continues to welcome input and engagement from all interested parties regarding the potential considerations posed by digital assets with respect to Rule 206(4)-2 under the U.S. Investment Advisers Act of 1940, as amended (the “*Custody Rule*”). The Custody Rule mandates safeguards for registered investment advisers with custody of client funds and securities. These safeguards are designed to protect advisory client assets from loss, misuse, misappropriation or an adviser’s financial deterioration.

We note the Division is considering recommending that the Securities and Exchange Commission (the “*SEC*”) propose amendments to the Custody Rule in 2022.¹ We also refer to the letter dated March 12, 2019 from the Division to the Investment Adviser Association on “Engaging on Non-DVP Custodial Practices and Digital Assets” (the “*Request Letter*”).²

Introduction

The WSBA is an industry-leading non-profit trade association based in New York City. Our mission is to guide and promote the comprehensive adoption of blockchain technology and digital assets across global markets in a manner that complies with all relevant laws and regulations. The WSBA is structured into working groups that, in turn, coordinate the collaboration of leaders across industries and professions to fulfill the WSBA’s mission. Given this variety of industries and professionals within the WSBA, we would like to share our response from members of the Legal Working Group to one particular question in the Request Letter:

What considerations specific to the custody of digital assets should the staff evaluate when considering any amendments to the Custody Rule?

These comments are our own, in our personal capacity, and do not necessarily reflect the views of any member or partner of the WSBA, nor the WSBA Board of Directors.

Response

Regulation of custodians, trading platforms and other third parties involved in the safekeeping, transfer or control of digital assets continues to evolve.³ In this regulatory context, investment advisers must consider not only the application of the Custody Rule’s prescriptive requirements,⁴ but also other overlapping—and potentially conflicting—obligations.⁵ Notwithstanding the obligations to which a registered investment adviser is subject, it

nevertheless bears the burden of developing a compliance program reasonably designed to prevent violation of the Advisers Act and associated rules.

Amendments to the Custody Rule provide an opportunity for the SEC to modernize and tailor both the Custody Rule and related guidance to provide greater clarity on the safeguards investment advisers that manage digital assets may adopt to comply with the Custody Rule. Staff guidance may also encourage other prominent qualified custodians to provide custodial services for digital assets given they must balance customer interest, technical concerns and compliance with staff guidance.

Regardless which approach the Commission chooses to pursue in proposing amendments to the Custody Rule, the industry would welcome supplemental practical guidance on this topic.⁶ We believe that there are a number of factors for an investment manager to consider when evaluating custodians, trading platforms or other third parties involved in the safekeeping, transfer or control of digital assets. In this context, Exhibit A is a resource gathering some of the factors that may be useful, depending on the particular circumstances. These questions are broader in scope than the Custody Rule, but amending the Custody Rule is a meaningful first step in helping investment advisers that manage digital assets and seek to protect client assets from being lost, misused, or misappropriated. We look forward to engaging further with the Division.

We look forward to engaging further with the Division.

Respectfully Submitted,



Ron Quaranta – Chairperson and Chief Executive Officer, Wall Street Blockchain Alliance
Gavin Fearey – Principal Contributor, Of Counsel, Winstead PC
Alice Albl – Legal Working Group Associate, Wall Street Blockchain Alliance
Lindsay Danas Cohen – General Counsel, Nillion
Oscar Saunders – Counsel, Linklaters LLP
Joshua Ashley Klayman – Chairperson, Wall Street Blockchain Alliance Legal Working Group

cc: Valerie A. Szczepanik, Director, Office of Strategic Hub for Innovation and Financial Technology

Endnotes:

¹ The agenda item for amendments to the Custody Rule for Investment Advisers is available at <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=3235-AM32> (last accessed Oct. 11, 2022).

² Letter dated March 12, 2019 from the staff of the Division of Investment Management to the Investment Adviser Association on “Engaging on Non-DVP Custodial Practices and Digital Assets” (the “*Request Letter*”), a copy of which is available at <https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206> (last accessed Oct. 11, 2022).

³ For example, Senators Cynthia Lummis (R-WY) and Kirsten Gillibrand (D-NY) introduced the bipartisan *Lummis-Gillibrand Responsible Financial Innovation Act* in June 2022, a copy of which is available at <https://github.com/responsible-financial-innovation-act22/RFIA-bill> (last accessed Oct. 11, 2022).

⁴ Letter from Verady, Inc. dated May 31, 2019 to staff of the Division, a copy of which is available at <https://www.sec.gov/files/engaging-on-non-dvp-custodial-practices-and-digital-assets-053119.pdf> (last accessed October 11, 2022). This response to the Request Letter notes that, despite a long history and many complexities its application, many Custody Rule safeguards simply prescribe the controls and tools (and the frequency of their use) to independently verify

funds and securities within the custody of the investment adviser – in other words, how and when there must be “another set of eyes on client assets.”

⁵ For example, as noted by the SEC in its proposed cybersecurity compliance rules for investment advisers and others, an adviser’s fiduciary duty to act in the best interest of clients requires an adviser to take steps to minimize operational and other risks. See *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, SEC Release Nos. 33-11028; 34-94197; IA-5956; IC-34497 (Feb. 9, 2022).

⁶ Certain members of the Legal Working Group believe that both registered investment advisers and broker-dealers would be better equipped to ensure adequate protection of client assets if the staff provided supplemental practical guidance that aligns or separates its expectations for best practices for compliance by registered investment advisers with the Custody Rule and compliance by broker-dealers with Rule 15c3-3 under the Securities Exchange Act of 1934 (the “**Customer Protection Rule**”) in the context of digital assets. For instance, the Wall Street Blockchain Alliance has also provided a list of best practices to protect against certain technological risks associated with digital asset custody for broker-dealers. See Appendix A of the letter from Wall Street Blockchain Alliance dated April 27, 2021 to the U.S. Securities and Exchange Commission on “Custody of Digital Asset Securities by Special Purpose Broker-Dealers,” a copy of which is available at <https://www.sec.gov/comments/s7-25-20/s72520-8734174-237103.pdf> (last accessed Oct. 11, 2022).

Exhibit A
Resource for Evaluating Custodians of Digital Assets

This resource is for investment managers when evaluating custodians, trading platforms or other third parties involved in the safekeeping, transfer or control of digital assets. These questions are broader in scope than the custody rule to which registered investment advisers are subject.¹ Other rules, as well as compliance policies and procedures, also impact the evaluation.² It is not legal advice or guidance for any specific situation or agreement.

<p>Regulatory Status and Oversight</p>	<ul style="list-style-type: none"> ○ What are the custodian’s regulatory status and primary regulator? ○ What are the custodian’s capital requirements? ○ Where custody is present and the Custody Rule applies, does the custodian represent it is a qualified custodian under the Advisers Act? ○ Are services delivered in compliance with other Advisers Act requirements? ○ Will the custodian provide assurances to these questions? ○ Does the custodian have rating from a nationally recognized rating agency? ○ Has the custodian had any shortfalls in capital below what is required by the applicable regulator? ○ Has the custodian been the subject of any material litigation or regulatory action relating to its custodial business?
<p>Segregation of Assets</p>	<ul style="list-style-type: none"> ○ Does the custodian segregate client digital assets from assets of (1) the custodian, (2) other clients, and (3) the investment adviser? ○ Does the custodian segregate by individual wallet addresses, another technological solution, or bookkeeping practices? ○ When, if ever, does the custodian (1) pool its clients’ assets (akin to traditional finance securities operational commingling of customer omnibus accounts) or (2) hold its clients’ assets in other wallets for another purpose (such as authorized trading)? ○ If the custodian holds client assets on an omnibus basis, does the custodian provide assurances it will clearly identify client assets on its books and records as owned by the customer, separate from any proprietary assets of the custodian?³ ○ Are there mandated reviews of assets to ensure the custodian meets segregation standards?
<p>Ownership and Control of Assets</p>	<ul style="list-style-type: none"> ○ Does the custodian hold the assets of the investment adviser as bailee (using trust or fiduciary powers or on a contractual basis) or in a different capacity? ○ What type of ownership does the customer retain (<i>e.g.</i>, transfer of control but not transfer of title)? ○ Does the agreement provide that client assets always remain client property and never become an asset of the custodian? ○ Does the custodian agree to return the specific coins or tokens deposited (<i>e.g.</i>, rather than returning any fungible equivalent coins or tokens)? ○ How does the custodian ensure its control over the digital assets?

Bankruptcy Remoteness and UCC Treatment	<ul style="list-style-type: none"> ○ What private key controls or other steps does the custodian take to ensure that client assets are ‘ring-fenced’ in case of a custodian’s insolvency? ○ What is the risk of characterization as a debtor-creditor relationship in bankruptcy?⁴ Does the custodian disclose whether client assets would be available to satisfy general creditor claims in the event of a bankruptcy?⁵ ○ Does the custodian provide a standard legal opinion to its customers on the enforceability of segregation of client assets upon its insolvency? ○ Does the agreement contemplate UCC treatment for certain client assets (e.g., as “financial assets” receiving the protections and procedures for securities accounts with securities intermediaries under Article 8 of the UCC)?⁶
Apportionment of Liability	<ul style="list-style-type: none"> ○ Does the custodian expressly commit to exercise the reasonable care of a professional custodian for hire? ○ Does the custodian expressly commit to replace any loss of digital assets (without a cap) resulting from the custodian’s material breach of the agreement? ○ Does the agreement require the client to indemnify the custodian? If so, how broad is the scope and are negligence and willful misconduct carved out? ○ Does the custodian limit its liability in the agreement? ○ What kind of dispute resolution procedures does the agreement provide? ○ Are force majeure events limited to events outside the custodian’s reasonable ability to mitigate or prevent? Ideally a custodian’s excused performance for force majeure would be conditioned on its compliance with a business continuity plan and commercially reasonable efforts to recommence performance as soon as practicable. ○ May a client obtain the right to assign the agreement with notice but without consent to a successor? ○ Does the custodian have the right, without consent, to assign the agreement to another custodian? If so, is it limited to an affiliate or another custodian meeting certain credit standards? ○ Does the custodian provide any transition period in the case of assignment to another custodian or voluntary termination or termination by customer upon a breach of the agreement?
Technology to Secure Assets	<ul style="list-style-type: none"> ○ What private key management or other methods does the custodian use to ensure the security of custodied assets? <i>See also “Cybersecurity.”</i> ○ For example, does the custodian employ multi-factor or multi-party authorization of transfers, sharding of keys, address whitelisting, location verification or the like? Are the private keys maintained by the custodian generated in a secure fashion? ○ Does the custodian take responsibility for technical and other risks that it would be reasonably expected to prevent or mitigate (like losses from external hacking, phishing of the custodian’s systems, or collusion among the custodian’s employees)? ○ What fraud detection tools does the custodian employ? <i>See also ‘AML/KYC Compliance.’</i>
Segregation of Duties and Dual Controls	<ul style="list-style-type: none"> ○ Does the custodian have proper procedures in place to ensure that the critical functions and key processes are dispersed to more than one person or department?

Independent Assessments	<ul style="list-style-type: none"> ○ Has the custodian obtained independent assurances of the effectiveness of its internal controls (<i>e.g.</i>, AICPA SOC 2 Type 1 report) from independent third parties? ○ Is the focus on systems for custodial arrangements or for other related areas of its businesses?⁷ ○ Is the report over internal controls over financial reporting (SOC 1) or broader trust services (security, availability, processing, integrity, confidentiality, and privacy) (SOC 2)? ○ Is testing at a specific point in time (Type 1) or over a period (Type 2)? ○ Has the custodian obtained independent risk modeling, adversary analysis and testing of security processes, and protocols used to safeguard the digital assets held in custody? ○ Is the auditor’s report unqualified? Are there exceptions or qualifications?⁸
Independent Verification of Assets	<ul style="list-style-type: none"> ○ How and how often does a custodian independently verify its assets, and to whom does it provide results? For example, are ‘proof-of-reserves’ attestations performed by independent third parties and, if so, are the attestations performed on an ongoing basis or at a specific point-in-time? ○ Is the custodian subject to surprise verification? ○ Are these verifications to enhance investor protection or to provide periodic reports to clients?
Handling of Hard Forks and Air Drops	<ul style="list-style-type: none"> ○ Does the customer receive forked and airdropped digital assets? ○ Does the custodian notify the customer of its procedure before an airdrop or fork occurs? ○ Does the custodian commit to support at least one fork? ○ May a customer withdraw if the custodian refuses to support a fork? ○ Who retains title if the custodian elects to support the fork? ○ May the custodian amend its policy at any time, or is there a notice period?
Other Terms and Disclosures	<ul style="list-style-type: none"> ○ Does the custodian commit to a meaningful post-execution timeframe (one year or more) where it cannot increase fees without customer consent? ○ Does the custodian agree to return assets within a defined timeframe (ideally 4-6 hours, but never greater than 24 hours)? ○ Will the custodian assume responsibility for delays in deposits and withdrawals? ○ Does the custodian limit its use of a client’s personal information to circumstances necessary to delivery services under the agreement? ○ What are the regulatory requirements applicable to custodians to protect client’s personal information? ○ Does the custodian have a clear and auditable process for confirming and updating the list of persons authorized by the customer to execute transactions on the customer’s behalf? ○ Does the custodian provide disclosures that describe the types of loss or additional obligations that could occur, including customer or user discontinuation or reduction of use of services, litigation, reputational harm, and regulatory enforcement actions and additional restrictions?⁹

Insurance	<ul style="list-style-type: none"> ○ Does the custodian have insurance that covers the digital assets in its custodianship? ○ Does the policy cover storage or transfer? <ul style="list-style-type: none"> ○ If storage: does cold storage insurance have exclusion for third party hacks or losses due to compromised transaction processes? ○ If transfer: is it crime insurance for hot wallets? ○ Is there cyber liability insurance, technology E&O insurance, or any other type of insurance? ○ Is the insurance provided by a highly-rated insurer? ○ Who is the named insured? ○ What are the overall and per-incident limits? Is coverage sought in a 1:1 or another ratio? ○ How does the policy cover customers if a loss event exceeds available coverage? ○ Does the policy apply exclusively to customer assets, or is it under a parent’s policy that could face claims from other subsidiaries?
Cybersecurity	<ul style="list-style-type: none"> ○ What policies, procedures, and infrastructure does the custodian employ to prevent hacking, theft, and fraud? ○ How does the custodian specifically mitigate the increased cybersecurity risk associated with virtual currencies and other digital assets?¹⁰ ○ How do the custodian’s policies, procedures and infrastructure assess or seek to mitigate cybersecurity risk associated with third parties, as well as for the protocols, platforms and smart contracts used to implement holdings and trading “outside” the custodian’s own infrastructure? ○ Under what conditions would the custodian notify its clients of a cybersecurity incident? ○ How would the custodian notify its clients of a cybersecurity incident?
Sub-custodians and Technology Providers	<ul style="list-style-type: none"> ○ Does the custodian utilize any sub-custodians and technology providers to deliver services? ○ What is their primary role? ○ Does the custodian remain responsible for their actions? ○ Does the custodian have processes to ensure a sub-custodian’s operations have the necessary internal controls to protect client digital assets? ○ Do sub-custodians have to meet certain regulatory or credit standards? ○ Please list the domiciles of any sub-custodians used and for what type of assets would they be used.

Transaction Settlement	<ul style="list-style-type: none"> ○ What are the controls available for withdrawal limits, access frequency and transaction size? ○ Does the custodian commit to a turnaround time for transfers to and from the wallet? ○ Is settlement on-chain or off-chain? ○ Is it on a delivery-versus-payment basis? ○ Does the custodian have special settlement arrangements with other custodians or platforms? ○ Does the custodian offer trade reconciliation on a pre-trade or post-trade basis? ○ What manual processes are involved in the settlement process? ○ Are new deposit addresses created for each settlement transaction? ○ Does the custodian provide post-trade reporting necessary for audit and tax reporting?
Trade Execution Services or Brokerage	<ul style="list-style-type: none"> ○ Does the custodian or an affiliate offer trade execution services to facilitate trading, such as prime brokerage? ○ Does it operate on a principal, riskless principal, or agency basis? ○ How does it handle conflicts of interest? ○ Can a customer trade directly from its custody account, or must assets be moved to an exchange or pool? ○ Must clients pre-fund trades? <p><i>See also “Transaction Settlements”</i></p>
Lending, Rehypothecation and Leverage	<ul style="list-style-type: none"> ○ Does the custodian or an affiliate allow clients to borrow cash (secured by digital assets as client collateral), borrow digital assets, make short trades, or obtain leverage (and if so, by margin or borrowing)? What are the applicable over-collateralization percentages and interest rates charged? ○ Does the custodian or an affiliate rehypothecate client assets and, if so, with specific consent only? ○ Does the custodian take a security interest in the client assets and, if so, under which UCC provision (see above) and to secure which obligations? ○ Does rehypothecation occur between multiple digital asset types (e.g., as with a bridge or through cross-chain transactions) and is this disclosed? ○ Which party pays gas or other transaction fees?
AML/KYC Compliance	<ul style="list-style-type: none"> ○ Does the custodian have the infrastructure to support full AML/KYC compliance and the FATF’s travel rule (for instance, pursuant to interoperability among virtual asset service providers using TRISA and/or Sygna Bridge)? ○ What chain analysis is performed before accepting deposits of a digital asset (e.g., to determine ‘provenance’ and risk level)? ○ Does the custodian operate a full node for each digital asset it supports?
Events of Default; Modifications	<ul style="list-style-type: none"> ○ What situations trigger the custodian’s right to terminate the agreement (e.g., failure to pay, breach of the agreement, misrepresentation, bankruptcy, among certain other events)? ○ Does custodian retain the ability to modify legal or risk terms of the agreement without customer consent?

Endnotes:

¹ *Rule 206(4)-2* under the *U.S. Investment Advisers Act of 1940* mandates key safeguards for registered investment advisers with custody of client funds and securities (the “**Custody Rule**”). These safeguards are designed to protect advisory client assets from misuse or misappropriation. The Division of Investment Management is considering recommending that the SEC propose amendments to the Custody Rule.

² *Rule 206(4)-7* under the Advisers Act and corresponding guidance identify areas in which registered investment advisers must adopt written policies and procedures reasonably designed to prevent compliance violations. In addition, *Regulation S-P* requires registrants to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. The SEC has proposed rules on procedures and controls surrounding cybersecurity preparedness, following guidance from SEC staff of the Division of Investment Management on the same topic. The Division of Examinations has also identified exam priorities, and thus areas of focus for investment advisers, relating to digital assets in *2022 Examinations Priorities* (March 30, 2022), <https://www.sec.gov/files/2022-exam-priorities.pdf> (last accessed June 26, 2022). Similarly, with respect to safekeeping and custody, SEC exam staff have recommended that investment advisers consider (a) controls around safekeeping of digital assets, (b) arrangements for storage of cryptocurrencies on trading platform accounts and with third-party custodians, (c) software reliability for access to digital asset networks, (d) security procedures for wallets, and (e) any required updates to the business continuity plan. *Risk Alert: The Division of Examinations’ Continued Focus on Digital Asset Securities*, a copy of which is available at <https://www.sec.gov/files/digital-assets-risk-alert.pdf> (last accessed June 27, 2022).

³ Several questions are informed by *Legal & Contractual Considerations for Corporate Customers of Digital Asset Custodians*, Microstrategy Incorporated (2022), a copy of which is available at <https://www.microstrategy.com/content/dam/website-assets/collateral/bitcoin-downloads/MicroStrategy-Contractual-Considerations-for-Digital-Asset-Custodians.pdf> (last accessed June 26, 2022).

⁴ See Adam Levitin, *What Happens If a Cryptocurrency Exchange Files for Bankruptcy?*, CREDIT SLIPS (Feb. 2, 2022, 11:06 PM), significant uncertainties surrounding treatment in bankruptcy are identified in an article available at <https://www.creditslips.org/creditslips/2022/02/what-happens-if-a-cryptocurrency-exchange-files-for-bankruptcy.html>.

⁵ *SEC Staff Accounting Bulletin No. 121*, 87 Fed. Reg. 21015 (Apr. 11, 2022).

⁶ Certain state have enacted legislation addressing, among other things, the definition of virtual currency & perfection by control. Examples are Texas, Wyoming & Rhode Island. The Uniform Law Commission is in the process of approval (expected no later than July 2022) provisions providing for Article 12 for “controllable electronic records,” which would include many digital assets. Article 12 would then be submitted to the states for adoption.

⁷ Examples of systems for custody arrangements would be storage infrastructure, cryptographic key management, asset movement, operational reconciliation controls or overall end-to-end control infrastructure.

⁸ Several questions are informed by *Digital Asset Custody: An AIMA Industry Guide* (2022), a copy of which is available for download at <https://www.aima.org/sound-practices/industry-guides/digital-asset-custody-guide.html> (last accessed June 26, 2022).

⁹ See *Endnote 5*.

¹⁰ General resources for assessing cybersecurity risks and controls include, among others: compliance with FFIEC security control frameworks and standards; making updates in response to changes in threat environments, audits of third-party penetration testing and business continuity plan; monitoring for security incidents per industry best practices, establishing the notice period for a security incident affecting client, and timely restoring services.