MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Fireblocks Inc.

On April 17, 2025, Crypto Task Force Staff met with representatives from Fireblocks Inc.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Fireblocks Inc. representatives provided the attached documents, which were discussed during the meeting.

Fireblocks

SEC Crypto Task Force - Agenda

- Follow-up on February 20, 2025, SEC Crypto Task Force discussion
- Walk-through of digital asset-specific considerations and best practices related to digital asset custody and ancillary activities

Proposed Participants

1. Michael Shaulov, Co-Founder and CEO
2. Jason Allegrante, Chief Legal Officer
3. Peter Marton, Sr. Director, Digital Identity, Compliance Advisory, US Policy

April 8, 2025

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

To: SEC Crypto Task Force
Re: Crypto Task Force Meeting Request

Fireblocks Inc. ("Fireblocks" or "we") appreciate the opportunity to engage with the staff of the U.S. Securities and Exchange Commission ("SEC") Crypto Task Force as it relates to approaches on critical infrastructure issues, such as digital asset custody and safekeeping. We support the SEC's overall mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. As discussed herein, and building upon our previous submission to the SEC Crypto Task Force in our submission dated February 20, 2025 (here), we strongly believe a robust and resilient infrastructure layer is a critical component to all of the SEC's goals in this space.

As digital assets become an increasingly accepted mainstream asset class, we applaud the SEC's recent commitments to create a regulatory environment more responsive to issues posed by the deployment of novel technologies. Recent measures, including the Staff Accounting Bulletin No. 122[1] the announcement by Commissioner Peirce of the Crypto Task Force,[2] its recent initial agenda setting,[3] and call to action,[4] among other steps, mark a pivotal turn in the oversight and regulation of the digital asset ecosystem within the United States. These developments herald a new age of leadership for the United States – and underscore the need for the development of a broad-based understanding on critical infrastructure issues in this rapidly evolving sector.

To continue the transition to digital asset readiness for financial intermediaries, it is critical that market participants, including broker-dealers, investment advisors, and investment companies (defined here as "Covered Entities"), have clarity around how existing requirements align to digital asset custody and safekeeping and ancillary activities.[5] Such obligations should recognize digital asset-specific risks and vulnerabilities and integrate new risk mitigants, to help ensure that new actors can operate safely and legally, taking account nuances specific to digital asset custody technologies. Existing guidance related to the risk management of third party providers to regulated entities is a suitable starting point. Similarly, the SEC itself has advanced certain rule-making and guidance including around cybersecurity and data

[1] SEC. Staff Accounting Bulletin No. 122. January 23, 2025.
[2] SEC. SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force. January 21, 2025.
[3] SEC. The Journey Begins. February 4, 2025.
[4] SEC. There Must Be Some Way Out of Here. February 21, 2025.
[5] Consider, as examples, how such activities are consistent with existing requirements in particular related to Rule 206(4)-2 under the Investment Advisers Act of 1940 (the "Custody Rule") and Rule 15c3-3 under the Securities Exchange Act of 1934 (the "Customer Protection Rule").

privacy that may warrant further tailoring against digital asset-specific considerations.[6] However, new technologies – which will underpin digital asset securities, real world asset tokenization, and other emergent use cases – warrant new supervisory approaches as well.

As such, our aim for this discussion is to provide an overview of policy principles and technical standards related to custody technology solutions in a manner that harmonizes best practices from our customers' deployments globally. In particular, as part of our proposed discussion, we intend to engage with Task Force staff around principles to support safe and sound practices, including cybersecurity; privileges and access management; detection, response, and investigation management; business continuity, disaster recovery, and resolvability; and key management. For example, Covered Entities obligations related to business continuity, disaster recovery, and resolvability and related policies and processes may have different features than in traditional financial services to ensure availability and functionality of the Covered Entity's services in the event of an emergency or other disruption.

We are grateful for the opportunity to contribute to this discussion. If there are any further measures we can take to support the Task Forces's work in this area, from Commissioner Peirce's recent announcement related to market structure and innovation to other technical assistance, we remain available to support in any way that is helpful.

Best,

Jason P. Allegrante
Chief Legal Officer
Point of Contact

E: jason@fireblocks.com
T: (516) 441-2738
441 9th Avenue
New York, New York 10001

[6] For example, note Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (2024), Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (2024), Identity Theft Red Flags Rules (2023), and Business Continuity Planning for Registered Investment Companies (2016), among others, in the contexts of digital asset market participants.