SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 240

[Release No. 34-90788; File No. S7-25-20]

Custody of Digital Asset Securities by Special Purpose Broker-Dealers

AGENCY: Securities and Exchange Commission ("Commission").

ACTION: Statement; request for comment.

SUMMARY: The Commission is issuing a statement and requesting comment regarding the custody of digital asset securities by broker-dealers.

EFFECTIVE DATE: [Insert date 60 days after publication in the Federal Register].

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic comments:

- Use the Commission's internet comment form (https://www.sec.gov/rules/submitcomments.htm); or
- Send an email to *rule-comments@sec.gov*. Please include File No. S7-25-20 on the subject line.

Paper comments:

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-25-20. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (*http://www.sec.gov*). Comments are also available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE,

Washington, DC 20549, on official business days between the hours of 10:00 a.m. and 3:00 p.m. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make publicly available.

FOR FURTHER INFORMATION CONTACT: Michael A. Macchiaroli, Associate Director, at (202) 551-5525; Thomas K. McGowan, Associate Director, at (202) 551-5521; Randall W. Roy, Deputy Associate Director, at (202) 551-5522; Raymond A. Lombardo, Assistant Director, at 202-551-5755; Timothy C. Fox, Branch Chief, at (202) 551-5687; or A.J. Jacob, Special Counsel, at (202) 551-5583, Division of Trading and Markets, Securities and Exchange Commission, 100 F Street, NE, Washington, D.C. 20549-7010.

SUPPLEMENTARY INFORMATION:

I. INTRODUCTION

The Commission is issuing this statement and request for comment to encourage innovation around the application of the Customer Protection Rule to digital asset securities.[1] The Commission envisions broker-dealers performing the full set of broker-dealer functions with respect to digital asset securities – including maintaining custody of these assets – in a manner that addresses the unique attributes of digital asset securities and minimizes risk to investors and

---

[1] For purposes of this statement, the term "digital asset" refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens." The focus of this statement is digital assets that rely on cryptographic protocols. A digital asset may or may not meet the definition of a "security" under the federal securities laws. *See, e.g.*, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Exchange Act Release No. 81207 (July 25, 2017). As used in this statement, a "digital asset security" means a digital asset that meets the definition of a "security" under the federal securities laws. A digital asset that is not a security is referred to herein as a "non-security digital asset."

other market participants.[2] Consequently, as discussed below, the Commission's position in this statement is premised on a broker-dealer limiting its business to digital asset securities to isolate risk and having policies and procedures to, among other things, assess a given digital asset security's distributed ledger technology and protect the private keys necessary to transfer the digital asset security. In this way, the Commission is cognizant of both investor protection and potential capital formation innovations that could result from digital asset securities.

Rule 15c3-3 under the Securities Exchange Act of 1934 (hereinafter the "Customer Protection Rule" or "Rule 15c3-3")[3] requires a broker-dealer to promptly obtain and thereafter maintain physical possession or control of all fully-paid and excess margin securities it carries for the account of customers.[4] Market participants have raised questions concerning the application of the Customer Protection Rule to the potential custody of digital asset securities for customers by broker-dealers. The Commission is requesting comment in this area to provide the Commission and its staff with an opportunity to gain additional insight into the evolving standards and best practices with respect to custody of digital asset securities. The Commission intends to consider the public's comments in connection with any future rulemaking or other Commission action in this area.

---

2 *See* 17 CFR 240.15c3-3. The Commission staff has issued a joint statement with the Financial Industry Regulatory Authority on broker-dealer custody of digital asset securities ("Joint Statement"), as well as a no-action letter regarding the Joint Statement to broker-dealers operating alternative trading systems ("ATSs"). *See Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities*, dated July 8, 2019, *available at* https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities. *See also* Letter to Ms. Kris Dailey, Financial Industry Regulatory Authority, ATS Role in the Settlement of Digital Asset Security Trades, dated September 25, 2020 (discussing a three-step process broker-dealers use when operating an alternative trading system for the purpose of trading digital asset securities), available at https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf. Staff statements represent the views of the staff. They are not rules, regulations, or statements of the Commission. The Commission has neither approved nor disapproved their content. These staff statements, like all staff guidance, have no legal force or effect: they do not alter or amend applicable law, and they create no new or additional obligations for any person.

3 *See* 17 CFR 240.15c3-3.

4 *See* 17 CFR 240.15c3-3(b).

As an interim step, in addition to the request for comment, the Commission is issuing this statement. The Commission recognizes that the market for digital asset securities is still new and rapidly evolving. The technical requirements for transacting and custodying digital asset securities are different from those involving traditional securities. And traditional securities transactions often involve a variety of intermediaries, infrastructure providers, and counterparties for which there may be no analog in the digital asset securities market. The Commission supports innovation in the digital asset securities market to develop its infrastructure.

In particular, the Commission's position, which will expire after a period of five years from the publication date of this statement, is that a broker-dealer operating under the circumstances set forth in Section IV will not be subject to a Commission enforcement action on the basis that the broker-dealer deems itself to have obtained and maintained physical possession or control of customer fully paid and excess margin digital asset securities for the purposes of paragraph (b)(1) of Rule 15c3-3.[5] These broker-dealers will be subject to examination by the Financial Industry Regulatory Authority ("FINRA") and Commission staff to review whether the firm is operating in a manner consistent with the circumstances described in Section IV below.

The five-year period in which the statement is in effect is designed to provide market participants with an opportunity to develop practices and processes that will enhance their ability to demonstrate possession or control over digital asset securities. It also will provide the Commission with experience in overseeing broker-dealer custody of digital asset securities to inform further action in this area.

II. BACKGROUND

[5] Pursuant to the Congressional Review Act, the Office of Information and Regulatory Affairs has designated this statement as a "major rule" as defined by 5 U.S.C. 804(2). *See* 5 U.S.C. 801 et seq.

Customers who use broker-dealers registered with the Commission to custody their securities (and related cash) benefit from the protections provided by the federal securities laws, including the Customer Protection Rule and, in most cases, the Securities Investor Protection Act of 1970 ("SIPA").[6] Generally, the Commission's Customer Protection Rule requires a broker-dealer to segregate customer securities and related cash from the firm's proprietary business activities, other than those that facilitate customer transactions.[7] The rule requires the broker-dealer to maintain physical possession or control over customers' fully paid and excess margin securities.[8]

Broker-dealer custody of securities is an integral service provided to the securities markets. However, broker-dealer custody of digital asset securities raises certain compliance questions with respect to the Customer Protection Rule. More specifically, while paragraph (b)(1) of Rule 15c3-3 requires that a broker-dealer "control" customer fully paid and excess margin securities, it may not be possible for a broker-dealer to establish control over a digital asset security with the same control mechanisms used in connection with traditional securities. Moreover, there have been instances of fraud, theft, and loss with respect to the custodianship of digital assets, including digital asset securities.[9]

---

6 15 U.S.C. 78aaa, *et seq*. Under SIPA, customers' securities held by a broker-dealer that is a member of the Securities Investor Protection Corporation and customers' cash on deposit at such a broker-dealer for the purpose of purchasing securities would be isolated and readily identifiable as "customer property" and, consequently, available to be distributed to customers ahead of other creditors in the event of the broker-dealer's liquidation. *Id.*

7 *See Net Capital Requirements for Brokers and Dealers*, Exchange Act Rel. No. 21651 (Jan. 11, 1985), 50 FR 2690, 2690 (Jan. 18, 1985) (Rule 15c3-3 is designed "to give more specific protection to customer funds and securities, in effect forbidding brokers and dealers from using customer assets to finance any part of their businesses unrelated to servicing securities customers; *e.g.*, a firm is virtually precluded from using customer funds to buy securities for its own account").

8 *See* 17 CFR 240.15c3-3(b)(1).

9 *See generally*, Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (October 2020), at 15-16, available at https://www.justice.gov/ag/page/file/1326061/download.

The risks associated with digital assets, including digital asset securities, are due in part to differences in the clearance and settlement of traditional securities and digital assets. Traditional securities transactions generally are processed and settled through clearing agencies, depositories, clearing banks, transfer agents, and issuers. A broker-dealer's employees, regulators, and outside auditors can contact these third parties to confirm that the broker-dealer is in fact holding the traditional securities reflected on its books and records and financial statements, thereby providing objective processes for examining the broker-dealer's compliance with the Customer Protection Rule. Also, the traditional securities infrastructure has established processes to reverse or cancel mistaken or unauthorized transactions. Thus, the traditional securities infrastructure contains checks and controls that can be used to verify proprietary and customer holdings of traditional securities by broker-dealers, as well as processes designed to ensure that both parties to a transfer of traditional securities agree to the terms of the transfer.

Digital assets that are issued or transferred using distributed ledger technology may not be subject to the same established clearance and settlement process familiar to traditional securities market participants.[10] The manner in which digital assets, including digital asset securities, are issued, held, or transferred may create greater risk that a broker-dealer maintaining custody of this type of asset, as well as the broker-dealer's customers, counterparties, and other creditors, could suffer financial harm. For example, the broker-dealer could be victimized by fraud or theft, could lose a "private key" necessary to transfer a client's digital assets, or could transfer a client's digital assets to an unintended address without the ability to reverse a fraudulent or mistaken transaction. In addition, malicious activity attributed to actors taking

[10] The clearance and settlement of securities that are not digital assets are characterized by infrastructure whereby intermediaries such as clearing agencies and securities depositories serve as key participants in the process. The clearance and settlement of digital asset securities, on the other hand, generally rely on few, if any, intermediaries and remain evolving areas of practices and procedures.

advantage of potential vulnerabilities that may be associated with distributed ledger technology and its associated networks could render the broker-dealer unable to transfer a customer's digital assets.

The express language of the Customer Protection Rule includes cash and securities held at the broker-dealer. Therefore, customers holding digital assets that are not securities through a broker-dealer could receive less protection for those assets than customers holding securities. The potential liabilities caused by the theft or loss of non-securities property from a broker-dealer, including digital assets that are not securities, could cause the broker-dealer to incur substantial losses or even fail, impacting customers and other creditors. As a consequence, the broker-dealer may need to be liquidated in a proceeding under SIPA. SIPA protection does not extend to all assets that may be held at a broker-dealer. Consequently, in a SIPA liquidation of a broker-dealer that held non-security assets, including non-security digital assets, investors may be treated as general creditors, to the extent their claims involve assets that are not within SIPA's definition of "security."[11]

III. DISCUSSION

A broker-dealer that maintains custody of a fully paid or excess margin digital asset security for a customer must hold it in a manner that complies with Rule 15c3-3, including that

[11] Generally, SIPA defines the term "security" to include, among other things, any note, stock, treasury stock bond, debenture, evidence of indebtedness, any investment contract or certificate of interest or participation in any profit-sharing agreement, provided that such investment contract or interest is the subject of a registration statement with the Commission pursuant to the Securities Exchange Act of 1933 (15 U.S.C. 77a et seq.), and any put, call, straddle, option, or privilege on any security, or group or index of securities. *See* 15 U.S.C. 78lll(14). Generally, in a SIPA liquidation, customers' claims receive priority to the estate of customer property (generally cash and securities received acquired or held by the broker-dealer for the securities accounts of customers) over other creditors. *See* 15 U.S.C. 78fff & 78fff-2(c). In addition, to the extent that the estate of customer property is insufficient to satisfy the net equity claims of customers, the trustee can advance up to $500,000 for each customer, of which up to $250,000 can be used for cash claims. *See* 15 U.S.C. 78fff-3(a) & (d).

the digital asset security must be in the exclusive physical possession or control of the broker-dealer.[12] A digital asset security that is not in the exclusive physical possession or control of the broker-dealer because, for example, an unauthorized person knows or has access to the associated private key (and therefore has the ability to transfer it without the authorization of the broker-dealer) would not be held in a manner that complies with the possession or control requirement of Rule 15c3-3 and thus would be vulnerable to the risks the rule seeks to mitigate.

As noted above, the loss or theft of digital asset securities may cause the firm and its digital asset customers to incur substantial financial losses. This, in turn, could cause the firm to fail, imperiling its traditional securities customers as well as the broker-dealer's counterparties and other market participants. However, there are measures a broker-dealer can employ to comply with Rule 15c3-3 and mitigate these risks.

One step that a broker-dealer could take to shield traditional securities customers, counterparties, and market participants from the risks and consequences of digital asset security fraud, theft, or loss would be to limit its business exclusively to dealing in, effecting transactions in, maintaining custody of, and/or operating an alternative trading system for digital asset securities. Thus, to operate in a manner consistent with the Commission's position, the broker-dealer could not deal in, effect transactions in, maintain custody of, or operate an alternative trading system for traditional securities. In addition, by limiting its activities exclusively to digital asset *securities*, the broker-dealer would shield its customers from the risks that could arise if the firm engaged in activities involving non-security digital assets, which are not expressly governed by the Customer Protection Rule. For example, to the extent that the requirements of the Customer Protection Rule do not apply to non-security digital assets, such

[12] *See* 17 CFR 240.15c3-3(b).

assets could receive less protection than securities, which would increase the risk of theft or loss and could ultimately cause the broker-dealer to fail, impacting customers and other creditors.

A second step the broker-dealer could take is to establish, maintain, and enforce reasonably designed written policies and procedures to conduct and document an analysis of whether a digital asset is a security offered and sold pursuant to an effective registration statement or an available exemption from registration, and whether the broker-dealer has fulfilled its requirements to comply with the federal securities laws with respect to effecting transactions in that digital asset security, before undertaking to effect transactions in and maintain custody of such asset. Such policies and procedures should provide a reasonable level of assurance that any digital assets transacted in or held in custody by the broker-dealer are in fact digital asset securities. Utilizing such policies and procedures should help ensure that the broker-dealer is confining its business to digital asset securities and that such digital asset securities are being offered, sold, or otherwise transacted in compliance with the federal securities laws.

A third step the broker-dealer could take is to establish, maintain, and enforce reasonably designed written policies and procedures to conduct and document an assessment of the characteristics of a digital asset security's distributed ledger technology and associated network[13] prior to undertaking to maintain custody of the digital asset security and at reasonable intervals thereafter. The assessment could examine at least the following aspects of the distributed ledger technology and its associated network, among others: (1) performance (*i.e.*, does it work and will it continue to work as intended); (2) transaction speed and throughput (*i.e.*, can it process

[13] For the purposes of this statement, a digital asset security's distributed ledger technology and associated network includes the protocols and any smart contracts or applications integral to the operation of the digital asset security.

transactions quickly enough for the intended application(s)); (3) scalability (*i.e.*, can it handle a potential increase in network activity); (4) resiliency (*i.e.*, can it absorb the impact of a problem in one or more parts of its system and continue processing transactions without data loss or corruption); (5) security and the relevant consensus mechanism (*i.e.*, can it detect and defend against malicious attacks, such as 51% attacks[14] or Denial-of-Service attacks, without data loss or corruption); (6) complexity (*i.e.*, can it be understood, maintained, and improved); (7) extensibility *(i.e.*, can it have new functionality added, and continue processing transactions without data loss or corruption); and (8) visibility (*i.e.*, are its associated code, standards, applications, and data publicly available and well documented). The assessment also could examine the governance of the distributed ledger technology and associated network and how protocol updates and changes are agreed to and implemented. This would include an assessment of impacts to the digital asset security of events such as protocol upgrades, hard forks, airdrops, exchanges of one digital asset for another, or staking.[15] Such assessments would allow a broker-dealer to be able to identify significant weaknesses or other operational issues with the distributed ledger technology and associated network utilized by the digital asset security, or other risks posed to the broker-dealer's business by the digital asset security, which would allow a broker-dealer to take appropriate action to identify and reduce its exposure to such risks. Accordingly, if there are significant weaknesses or other operational issues with the distributed

---

[14] For the purposes of this statement, a "51% attack" is an attack on a blockchain or distributed ledger in which an attacker or group of attackers controls a majority of the network's hash rate, mining or computing power, allowing the attacker or group of attackers to prevent new transactions from being confirmed.

[15] For purposes of this statement, "hard forks" refer to backward-incompatible protocol changes to a distributed ledger that create additional versions of the distributed ledger, potentially creating new digital assets. "Airdrops" refer to the distribution of digital assets to numerous addresses, usually at no monetary cost to the recipient or in exchange for certain promotional services. "Staking" refers to the use of a digital asset in a consensus mechanism.

ledger technology and associated network, the broker-dealer would be able to determine whether it could or could not maintain custody of the digital asset security.

A fourth step the broker-dealer could take is to establish, maintain, and enforce reasonably designed written policies, procedures, and controls for safekeeping and demonstrating the broker-dealer has exclusive possession or control over digital asset securities that are consistent with industry best practices to protect against the theft, loss, and unauthorized and accidental use of the private keys necessary to access and transfer the digital asset securities the broker-dealer holds in custody. These policies, procedures, and controls could address, among other matters: (1) the on-boarding of a digital asset security such that the broker-dealer can associate the digital asset security to a private key over which it can reasonably demonstrate exclusive physical possession or control; (2) the processes, software and hardware systems, and any other formats or systems utilized to create, store, or use private keys and any security or operational vulnerabilities of those systems and formats; (3) the establishment of private key generation processes that are secure and produce a cryptographically strong private key that is compatible with the distributed ledger technology and associated network and that is not susceptible to being discovered by unauthorized persons during the generation process or thereafter; (4) measures to protect private keys from being used to make an unauthorized or accidental transfer of a digital asset security held in custody by the broker-dealer; and (5) measures that protect private keys from being corrupted, lost or destroyed, that back-up the private key in a manner that does not compromise the security of the private key, and that otherwise preserve the ability of the firm to access and transfer a digital asset security it holds in the event a facility, software, or hardware system, or other format or system on which the private keys are stored and/or used is disrupted or destroyed. These policies, procedures, and controls

for safekeeping and demonstrating the broker-dealer has exclusive possession or control over digital asset securities should serve to protect against the theft, loss, and unauthorized and accidental use of the private keys and therefore the customers' digital asset securities.

A fifth step the broker-dealer could take is to establish, maintain, and enforce reasonably designed written policies, procedures, and arrangements to: (1) specifically identify, in advance, the steps it intends to take in the wake of certain events that could affect the firm's custody of the digital asset securities, including blockchain malfunctions, 51% attacks, hard forks, or airdrops; (2) allow the broker-dealer to comply with a court-ordered freeze or seizure; and (3) allow the transfer of the digital asset securities held by the broker-dealer to another special purpose broker-dealer, a trustee, receiver, liquidator, a person performing a similar function, or another appropriate person, in the event the broker-dealer can no longer continue as a going concern and self-liquidates or is subject to a formal bankruptcy, receivership, liquidation, or similar proceeding. These policies and procedures should include measures for ensuring continued safekeeping and accessibility of the digital asset securities, even if the broker-dealer is wound down or liquidated, and thus would provide a reasonable level of assurance that a broker-dealer has developed plans to address unexpected disruptions to the broker-dealer's control over digital asset securities.

A sixth step the broker-dealer could take is to provide written disclosures to prospective customers about the risks of investing in or holding digital asset securities. The disclosures could include, among other matters: (1) prominent disclosure explaining that digital asset securities may not be "securities" as defined in SIPA[16]—and in particular, digital asset securities

[16] 15 U.S.C. 78*lll*(14).

that are "investment contracts" under the *Howey* test[17] but are not registered with the Commission are excluded from SIPA's definition of "securities"—and thus the protections afforded to securities customers under SIPA may not apply with respect to those securities; (2) a description of the risks of fraud, manipulation, theft, and loss associated with digital asset securities; (3) a description of the risks relating to valuation, price volatility, and liquidity associated with digital asset securities; and (4) a description of the processes, software and hardware systems, and any other formats or systems utilized by the broker-dealer to create, store, or use the broker-dealer's private keys and protect them from loss, theft, or unauthorized or accidental use (including, but not limited to, cold storage, key sharding, multiple factor identification, and biometric authentication). The purpose of such disclosures is to provide the prospective customers with sufficient and easily understandable information about the risks to enable them to make informed decisions about whether to invest in or hold digital asset securities through the broker-dealer.

A seventh step the broker-dealer could take is to enter into a written agreement with each customer that sets forth the terms and conditions with respect to receiving, purchasing, holding, safekeeping, selling, transferring, exchanging, custodying, liquidating, and otherwise transacting in digital asset securities on behalf of the customer.[18] This step would ensure documentation of the terms of agreement between the customer and the broker-dealer providing custody of the customer's digital asset security, which would provide greater clarity and certainty to customers regarding their rights and responsibilities under the agreement with the broker-dealer.

---

17 *See SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

18 The agreement should contain such provisions and disclosures as are required by applicable laws, rules, and regulations.

IV. COMMISSION POSITION

The Commission's position[19] is expressly limited to paragraph (b) of Rule 15c3-3 under the Securities Exchange Act of 1934 ("Exchange Act"). Furthermore, the Commission's position does not modify or change any obligations of a broker-dealer, or other party, to otherwise comply with the federal securities laws, including the broker-dealer financial responsibility rules, obligations regarding proxy voting and beneficial ownership communications, as well as the broker-dealer's obligation to become a member of FINRA and to comply with applicable anti-money laundering and countering the financing of terrorism obligations under the Bank Secrecy Act.[20] All terms used in this Commission position will have the definitions set forth in Rule 15c3-3. Finally, the Commission's position, which will expire after a period of five years from the publication date of this statement, applies only to the exercise of its enforcement discretion with respect to compliance with paragraph (b)(1) of Rule 15c3-3 under the circumstances set forth below. During this period, the Commission will continue to evaluate its position, and the circumstances set forth below, on an ongoing basis as it considers responses to the request for comments as well as further action in this area, including any future rulemaking.

---

19 The Commission's position is an agency statement of general applicability with future effect designed to implement, interpret, or prescribe law or policy.

20 *See* Heath Tarbert, Chairman, U.S. Commodity Futures Trading Commission, Kenneth A. Blanco, Director, Financial Crimes Enforcement Network, and Jay Clayton, Chairman, Commission, Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets, dated Oct. 11, 2019 (reminding persons engaged in activities involving digital assets of their anti-money laundering ("AML") and countering the financing of terrorism ("CFT") obligations under the Bank Secrecy Act, and stating that broker-dealers are required to implement reasonably-designed AML programs and report suspicious activity, and that such requirements are not limited in their application to activities involving digital assets that are "securities" under the federal securities laws), *available at* https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets.

After considering the minimum steps that can be taken to mitigate the risks posed by broker-dealer custody of digital asset securities, for a period of five years, the Commission's position is that a broker-dealer in the following circumstances would not be subject to a Commission enforcement action on the basis that the broker-dealer deems itself to have obtained and maintained physical possession or control of customer fully paid and excess margin digital asset securities:

1. The broker-dealer has access to the digital asset securities and the capability to transfer them on the associated distributed ledger technology;

2. The broker-dealer limits its business to dealing in, effecting transactions in, maintaining custody of, and/or operating an alternative trading system for digital asset securities; provided a broker-dealer may hold proprietary positions in traditional securities solely for the purposes of meeting the firm's minimum net capital requirements under Rule 15c3-1,[21] or hedging the risks of its proprietary positions in traditional securities and digital asset securities.

3. The broker-dealer establishes, maintains, and enforces reasonably designed written policies and procedures to conduct and document an analysis of whether a particular digital asset is a security offered and sold pursuant to an effective registration statement or an available exemption from registration, and whether the broker-dealer meets its requirements to comply with the federal securities laws with respect to effecting transactions in the digital asset security, before undertaking to effect transactions in and maintain custody of the digital asset security;

4. The broker-dealer establishes, maintains, and enforces reasonably designed written policies and procedures to conduct and document an assessment of the characteristics of

[21] 17 CFR. 240.15c3-1.

a digital asset security's distributed ledger technology and associated network prior to undertaking to maintain custody of the digital asset security and at reasonable intervals thereafter;

5. The broker-dealer does not undertake to maintain custody of a digital asset security if the firm is aware of any material security or operational problems or weaknesses with the distributed ledger technology and associated network used to access and transfer the digital asset security, or is aware of other material risks posed to the broker-dealer's business by the digital asset security;

6. The broker-dealer establishes, maintains, and enforces reasonably designed written policies, procedures, and controls that are consistent with industry best practices to demonstrate the broker-dealer has exclusive control over the digital asset securities it holds in custody and to protect against the theft, loss, and unauthorized and accidental use of the private keys necessary to access and transfer the digital asset securities the broker-dealer holds in custody;

7. The broker-dealer establishes, maintains, and enforces reasonably designed written policies, procedures, and arrangements to: (i) specifically identify, in advance, the steps it will take in the wake of certain events that could affect the firm's custody of the digital asset securities, including, without limitation, blockchain malfunctions, 51% attacks, hard forks, or airdrops; (ii) allow for the broker-dealer to comply with a court-ordered freeze or seizure; and (iii) allow for the transfer of the digital asset securities held by the broker-dealer to another special purpose broker-dealer, a trustee, receiver, liquidator, or person performing a similar function, or to another appropriate person, in the event the broker-dealer can no longer continue

as a going concern and self-liquidates or is subject to a formal bankruptcy, receivership, liquidation, or similar proceeding;

8. The broker-dealer provides written disclosures to prospective customers: (i) that the firm is deeming itself to be in possession or control of digital asset securities held for the customer for the purposes of paragraph (b)(1) of Rule 15c3-3 based on its compliance with this Commission position; and (ii) about the risks of investing in or holding digital asset securities that, at a minimum: (a) prominently disclose that digital asset securities may not be "securities" as defined in SIPA—and in particular, digital asset securities that are "investment contracts" under the *Howey* test but are not registered with the Commission are excluded from SIPA's definition of "securities"—and thus the protections afforded to securities customers under SIPA may not apply; (b) describe the risks of fraud, manipulation, theft, and loss associated with digital asset securities; (c) describe the risks relating to valuation, price volatility, and liquidity associated with digital asset securities; and (d) describe, at a high level that would not compromise any security protocols, the processes, software and hardware systems, and any other formats or systems utilized by the broker-dealer to create, store, or use the broker-dealer's private keys and protect them from loss, theft, or unauthorized or accidental use;[22] and

9. The broker-dealer enters into a written agreement with each customer that sets forth the terms and conditions with respect to receiving, purchasing, holding, safekeeping, selling, transferring, exchanging, custodying, liquidating and otherwise transacting in digital asset securities on behalf of the customer.[23]

---

[22] The broker-dealer will need to retain these written disclosures in accordance with the broker-dealer record retention rule. *See* 17 CFR 240.17a-4(b)(4).

[23] The broker-dealer will need to retain these written agreements in accordance with the broker-dealer record retention rule. *See* 17 CFR 240.17a-4(b)(7).

V. REQUEST FOR COMMENT

The Commission is seeking comment on the specific questions below. When responding to the request for comment, please explain your reasoning.

1. What are industry best practices with respect to protecting against theft, loss, and unauthorized or accidental use of private keys necessary for accessing and transferring digital asset securities? What are industry best practices for generating, safekeeping, and using private keys? Please identify the sources of such best practices.
2. What are industry best practices to address events that could affect a broker-dealer's custody of digital asset securities such as a hard fork, airdrop, or 51% attack? Please identify the sources of such best practices.
3. What are the processes, software and hardware systems, or other formats or systems that are currently available to broker-dealers to create, store, or use private keys and protect them from loss, theft, or unauthorized or accidental use?
4. What are accepted practices (or model language) with respect to disclosing the risks of digital asset securities and the use of private keys? Have these practices or the model language been utilized with customers?
5. Should the Commission expand this position in the future to include other businesses such as traditional securities and/or non-security digital assets? Should this position be expanded to include the use of non-security digital assets as a means of payment for digital asset securities, such as by incorporating a *de minimis* threshold for non-security digital assets?

6. What differences are there in the clearance and settlement of traditional securities and digital assets that could lead to higher or lower clearance and settlement risks for digital assets as compared to traditional securities?
7. What specific benefits and/or risks are implicated in a broker-dealer operating a digital asset alternative trading system that the Commission should consider for any future measures it may take?

By the Commission.

Dated: December 23, 2020

Vanessa A. Countryman
Secretary