ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

July 26, 2021
Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC, 20549-1090

Dear Ms. Countryman,

Anchorage Digital appreciates the opportunity to offer comment to the Securities and Exchange Commission ("the Commission") regarding the custody of digital asset securities by Special Purpose Broker-Dealers (SPBD). Anchorage Digital is comprised of many subsidiaries that provide various cryptocurrency and digital asset security services pursuant to various regulatory regimes.

On December 23, 2020, the SEC issued a statement and request for comment regarding the custody of digital asset securities by broker dealers to encourage innovation in the way that Securities Exchange Act Rule 15c3-3 ("The Customer Protection rule") is applied in relation to the safekeeping of digital asset securities.

We'd like to begin by applauding the Commission for creating the space and time for innovation to occur in the realm of digital asset securities. Observing the present trajectory of the digital asset space and acknowledging, absent some change, its likely collision with existing laws as they relate to broker dealers, we appreciate the vision that is required to create the necessary guardrails around a market still very much in its infancy.

We believe that consumer protection is of the utmost importance in the digital asset space, particularly as it relates to the custody of digital assets and digital asset securities, and that allowing a limited number of SPBDs to act as a kind of proving ground for best practices in this emerging market is the right way to both ensure consumer protection and prevent the kind of stifling of innovation that can result from a misalignment between regulation and industry.

We also applaud the Commission for acknowledging at the outset the fact that "The technical requirements for transacting and custodying digital asset securities are different from those involving traditional securities."[1] For the purposes of this discussion, this fact cannot be overstated. We bring to this conversation deep expertise in the storage, safekeeping, and handling of the kind of cryptographic keys that are integral to the workings of the digital asset

[1] Securities and Exchange Commission 17 CFR Part 240, *Custody of Digital Asset Securities by Special Purpose Broker-Dealers,* Release No. 34-90788, File No. S7-25-20, Available at https://www.sec.gov/rules/policy/2020/34-90788.pdf

space, including digital asset securities. As such, we believe that the unique qualities of digital assets must be a significant if not the primary consideration when developing policy related to the secure custody and transfer of digital assets, whether by broker-dealers, SPBDs, or any other providers of custody for digital assets. More than superficially different, digital assets are fundamentally, essentially different from traditional financial instruments.

From the deep technological differences that define digital assets follows a unique set of risks surrounding their transfer and safekeeping, whether those digital assets are legally classified as securities or non-securities. The Commission's Statement also acknowledges this fact, saying,

> "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 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."[2]

This assessment is essentially correct. Due to the immutable nature of distributed ledgers, the irreversible nature of transactions in the blockchain space, and the unique technological features of digital assets, securities or otherwise, the technological bar for securely holding, issuing, and transferring digital assets is significantly higher than what is required to handle legacy financial instruments. With the very real threat of exploits at scale, the Commission is right to highlight the financial harm that could befall consumers and the danger such exploits pose for trust in financial markets.

The Commission is also right in its instinct to isolate risk. We worry, however, that part of the specific approach to doing so suggested in the Commission's statement may inadvertently introduce a different set of security risks, as well as increase market complexity and unnecessarily limit capital formation. In its statement, the Commission suggests that,

> "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 assets could receive less protection than securities, which would

[2] Ibid.

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

> increase the risk of theft or loss and could ultimately cause the broker-dealer to fail, impacting customers and other creditors."[3]

While we understand that, for a period of five years, a broker-dealer operating under the circumstances set forth in the Commission's statement will not be subject to an enforcement action for failure to adhere strictly to the letter of Rule 15c3-3, we are of the opinion that this suspension should very much be limited to a temporary safe harbor period, for the benefit of consumers and markets alike.

In reality, the security risks surrounding any asset based on private key cryptography (which both non-security digital assets and digital asset securities are) are essentially identical. Put differently, all of the risks outlined above in the Commission's position statement apply to both non-security digital assets and digital asset securities. Even so, the primary risk cited as the driving force behind limiting SPBDs in crypto to digital asset securities is the uneven application of the Customer Protection rule—the idea that custody for non-security digital assets is held to what is in effect a lower standard for security and consumer protection than custody for digital asset securities.

For this reason, we believe that a system where consumers exposed to digital asset securities are better protected than those in non-security digital assets by virtue of the former's being beholden to the Customer Protection Rule runs counter to the best interests of consumers, the markets, and capital formation. In limiting SPBD activity to digital asset securities rather than expanding consumer protections across all digital assets, the Commission runs the risk of cementing in place a kind of two-tiered system in crypto, where some consumers (who participate in digital asset securities) are granted a greater degree of protection than others (who participate in non-security digital assets), despite the assets being subject to effectively the same risk of exploit. It also runs the risk of increasing market complexity as well as surface of attack by requiring those interested in both digital asset securities and non-security digital assets to introduce additional counterparties and vendors.

A better solution than having two tiers of security allowed for digital assets, we respectfully suggest, is to improve custody protection across digital assets by requiring all SEC regulated digital asset custody providers to meet the same high bar for consumer protection, including adherence to the SEC's formulation of the Customer Protection Rule specific to digital assets. At present, there exist clear, verifiable, and auditable means to establish the digital equivalent of "physical possession or control"[4] of customer fully paid and excess margin digital asset securities. We believe it is in the best interest of both consumers and the market to require broker-dealers, custody providers, and other entities providing foundational infrastructure for the emerging digital asset security space to comply with these best practices, which we will describe below, alongside a number of additional considerations the Commission should take into account as they continue to develop their thinking around the appropriate balance between encouraging innovation and protecting consumers.

---

[3] Ibid.
[4] SEA Rule 15c3-3

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

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? 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?

Compared to the legacy financial system, which has had more than 200 years to develop and refine and establish industry standards and best practices for securing, transferring, and otherwise dealing in traditional financial instruments, the digital asset space, securities and otherwise, is still very much in its early days. That said, we believe that there are a number of tools and processes that can and should be considered best practices with respect to protecting digital asset securities and non-security digital assets against theft, loss, and unauthorized use, as well as allowing for compliance with existing regulatory requirements, including the Customer Protection rule.

Proof of existence and exclusive control

As the Commission is very much aware, the Securities Exchange Act of 1934 §15c3-3(d) ("the Customer Protection Rule") is intended to prevent, in the event of an entity's untimely failure, the delay in or inability to return an investor's securities to them. Toward this end, the Customer Protection Rule requires broker dealers and others who provide custody services "to maintain physical possession of or control over customers' fully paid and excess margin securities."[5] Since digital assets have no physical makeup by nature, the idea of "maintaining physical possession of or control over" digital asset securities presents a number of challenges. Put differently, and to borrow the Commission's language, "the traditional securities infrastructure contains checks and controls that can be used to verify proprietary and customer holdings of traditional securities by broker-dealers."[6]

While the mechanism traditional broker-dealers use to verify proprietary and customer holdings of securities may differ from that used to verify the same for digital asset securities, we believe an effective proxy exists, and that it should be required of any custody provider in digital assets: the ability to prove exclusive control over private keys and existence of assets on-chain. The broker dealer-dealer should be able to prove that that thing exists, and that it is under the exclusive control of said broker-dealer.

The ability to prove that assets held under custody exist on a regular basis, or whenever auditors or regulators request that proof, is essential for consumer protection. We believe that a required capability for broker-dealers providing custody services for digital asset securities

[5] SEA Rule 15c3-3
[6] Securities and Exchange Commission 17 CFR Part 240, *Custody of Digital Asset Securities by Special Purpose Broker-Dealers,* Release No. 34-90788, File No. S7-25-20, Available at https://www.sec.gov/rules/policy/2020/34-90788.pdf

should be proving asset existence when requested. Being able to prove existence validates both the fact that the private keys exist and that the private keys are functional.

Beyond proof of existence, it is imperative that broker-dealers providing custody services for digital asset securities be able to prove exclusive control over private keys. As the Commission pointed out in its statement, digital assets are fundamentally different from legacy financial instruments in terms of technology. One important distinction to note is the fact that private keys, like any piece of software, are copied easily. They can exist in a number of different locations and instances. This means that it's possible, even likely for multiple copies of a given private key to exist and that proving control over one key doesn't necessarily prove exclusive control—that the key only exists within a given entity's custody. To meet the requirements under the Customer Protection rule, a broker dealer must be capable of proving exclusive control over private key material.

It is possible to achieve proof of exclusive control through a combination of software, hardware, and operational processes. That said, not all custody models are structured in such a way that this is possible. More specifically, custody providers that base their security model on the maintenance of many copies of private key material may struggle to prove that all instances of a private key exist within their control. Not only does this throw compliance with the Customer Protection Rule into doubt, but it also greatly increases consumer risk. By relying on redundant copies of private key material in the name of security, such entities actually increase risk by making their own surface of attack larger, and drastically increasing the type and number of potential chances for loss through theft or internal collusion.

Hardware security

With respect to both hardware systems currently available to broker-dealers to create, store, or use private keys and industry best practices for generating, safekeeping, and using private keys, single-purpose hardware security modules (HSMs) are existing, mature technology built for the sole purpose of securing private key material and provide both the unique security protections required of digital assets, as well as allow for compliance with the Customer Protection rule.

HSMs are mature, regularly tested, and oft-used for the sole purpose of securing private key material. In terms of standards, the National Institute of Standards and Technology established the Federal Information Processing Standards (FIPS) to govern security standards for federal computer systems, approved by the Secretary of Commerce. HSMs with a rating of FIPS 140-2 meet the rigorous security requirements NIST has specifically laid out for cryptographic modules. We believe that it is reasonable to suggest that using protocols that meet the standards for securing cryptographic modules long set by another agency of the federal government is sufficient to provide custody in the digital asset space. While we believe that regulation should be technology agnostic, we have found a technology that meets existing regulatory requirements for the secure handling of private key material and should be allowed to deploy it.

More than meeting existing standards, when HSMs are air-gapped and physically isolated from public network connectivity, they provide an arguably more secure version of offline so-called "cold" storage because it doesn't require the sharding of private keys, or any of the kinds of manual human operations required by forms of cold storage reliant on private key redundancy. Avoiding these kinds of operations means effectively eliminating vectors for compromise through theft or internal collusion that can lead to loss of assets.

Lastly, as it relates to proving existence and exclusive control, HSMs can easily facilitate both. Private key material can be generated inside an HSM without the need for that material to ever leave. In this way, HSMs ensure exclusive control because the private key is both generated and held inside the HSM indefinitely. Existence proofing via HSM-based architecture is also easily achieved. Where a traditional "broker-dealer's employees, regulators, and outside auditors can contact [third party clearing agencies, depositories, clearing banks, transfer agents, and issuers] to confirm that the broker-dealer is in fact holding the traditional securities reflected on its books and records and client statements, thereby providing objective processes for examining the broker-dealer's compliance with the Customer Protection Rule,"[7] an SPBD utilizing HSM technology for custody can provide objective proof of existence nearly instantly through challenge-response authentication and external blockchain verification. Thus, while the mechanism for proving compliance with the Customer Protection rule may differ from that used in traditional securities markets, HSMs make it possible in a completely objective way and at a level of security long set by the Federal government.

With custody integral to the operation of broker-dealers and the evolution of the digital asset security ecosystem as a whole, it is only reasonable to require those entities aiming to secure private keys meet or exceed existing SEC regulations and other Federal standards surrounding private keys.

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.

In our view, for an SPBD to be deemed technically capable of custodying digital asset securities and non-security digital assets, they must be able to proactively monitor each and every blockchain for which they wish to custody assets. This includes assessing assets and their protocols before supporting an asset for custody—assessing their vulnerability to myriad potential security exploits, including the possibility and likelihood of a 51% attack—as well as implementing processes around the regular, periodic review of changes, including developments like hard forks and airdrops.

While the specific steps for managing blockchain events may vary situationally, it is important for the broker-dealer to establish, maintain, and enforce reasonably designed written policies and procedures to follow in the wake of a wide variety of events that could have an effect on a

[7] Ibid.

broker-dealer's custody of digital asset securities, including blockchain malfunctions, 51% attacks, hard forks, and airdrops. Other events that could affect the broker-dealer's custody of digital assets and should require a written policy include the procedure to allow the broker-dealer to comply with court-ordered freezes or asset seizures, as well as deal with the transfer of digital asset securities to another comparable broker-dealer in the event of self-liquidation, bankruptcy, receivership, or other similar proceeding.

Beyond hard forks, airdrops, and hostile network takeover through mechanisms like a 51% attack, there are a large number of additional risk factors that an SPBD should be able to adequately assess on a per asset basis, all of which have the potential to affect a broker-dealer's custody of digital asset securities. We feel the best practice to date is set forth below and should be coupled with adequate customer disclosure, to inform potential and existing customers of the risks and mitigating factors present.

Technical analysis

On a per asset basis, it is imperative for an SPBD or any other entity taking custody of digital asset securities or non-security digital assets to perform a rigorous technical analysis both initially and periodically on every asset the entity aims to support. While this assessment can take a few forms, it should have three primary goals:

1) To determine whether the development of a given asset and its associated blockchain meet a level of safety and soundness consistent with a secure software development lifecycle,
2) To identify and report defects to a given asset's code base or other known vulnerabilities related to the asset or its blockchain network, and
3) To devise an overall assessment of the unique features and capabilities of a given asset and its underlying blockchain.

For assets like Bitcoin, Ethereum, or other assets native to a particular blockchain network, technical assessment involves an in-depth examination of the blockchain and the asset's source code. For assets like ERC-20 tokens (a technical standard on which a number of digital asset securities are based) which are issued on existing blockchain infrastructure (in this case the Ethereum network) in the form of smart contracts, it becomes necessary to expand technical analysis to also include the source code of the smart contract used to create, issue, and otherwise manage that asset. While there are currently few digital asset securities in existence, it is anticipated that at least initially, many of them will utilize the ERC-20 (or derivative) standard.

Rigorous technical analysis is foundational to an entity's ability to provide secure custody of digital asset securities and non-security digital assets. As such, all findings from technical analysis should inform all other areas of risk assessment for a given asset.

Blockchain governance analysis

Blockchain networks operate with a wide range of governance models and mechanisms. As such, it is imperative for would-be SPBDs and other custody providers to be able to adequately assess how network consensus is reached, how the network itself is updated, and how a given governance model functions. For our purposes, it's helpful to think of blockchain governance as falling into three main categories: permissioned networks, unpermissioned networks, and token-based digital asset networks. Each of these categories of governance models requires a different set of risk assessment, a number of which we describe below.

Permissioned networks. Permissioned networks are essentially "closed" blockchains where a core, established group of participants support blockchain operations and come to consensus with themselves. Their governance model often involves a small number of network participants managing the network as a consortium, often through a collective identity, in many ways centralizing control over an otherwise decentralized network. In networks that meet this kind of description, because network control can be and often is concentrated among a few essential service providers, it is essential for SPBDs and other custody providers to conduct due diligence on the core group of participants themselves, as well as the broader governance design, policies, and procedures.

Unpermissioned networks. Unlike their permissioned counterparts, unpermissioned networks lack restrictions around who can and cannot participate in their consensus protocols. And while there may be no single consortium with ultimate control of the network, certain individuals or groups may still exert disproportionate influence over the network based on their role in establishing it or otherwise maintaining it. In cases such as these, it's imperative for an SPBD or other custody provider to conduct due diligence on these individuals and groups to assess their overall objectives, as well as the kinds of activities that they conduct that may have an impact on the network overall and any asset that may run on it.

The lack of a centralized consortium means that the consensus mechanisms of unpermissioned networks require additional scrutiny to determine the extent of decentralization within a given network, which then becomes part of determining how resilient that network is in the face of a 51% attack or other types of malicious activity.

Token-based digital asset networks. Certain digital assets utilize smart contracts for listing on a given blockchain network. For these kinds of assets, it's important for SPBDs and other providers of custody services to conduct due diligence on the entity issuing the asset in question, both to determine whether the asset was created for a legitimate use and to ensure the implementation of adequate governance mechanisms.

Other considerations

More than technical and governance analyses, on a per asset basis, SPBDs and other custody providers must be able to satisfactorily answer a number of questions pertaining to the digital asset securities and non-security digital assets they wish to custody. Among them are those

related to ensuring compliance with BSA/AML regulations and mitigating sanctions risks, ensuring market integrity by assessing the likelihood of market manipulation taking place on a given network or with a given asset, and network compliance with all applicable laws and regulations and regulatory guidance.

Certain of this data may not be known at initial launch of the digital asset which makes ongoing blockchain monitoring of all supported assets imperative. Robust procedures to monitor the operation and activity of the digital asset protocols and customer transactions are essential to any SPBD.

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?

With respect to disclosing the risks of digital asset securities specifically and the use of private keys more generally, it should be fairly commonplace for a broker-dealer providing custody services to provide:

1. written disclosures that it is deemed to be in possession or control of Digital Asset Securities held for the customer for purposes of SEC Rule 15c3-3(b)(1) based on its compliance with the Statement;
2. written disclosures about the risks of investing in or holding digital securities that:
    a. prominently disclose that digital 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 SEC 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;
    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 used to create, store, or use the private keys and protect them from loss, theft, or unauthorized or accidental use;
    e. a set of risks relevant to any specific digital asset; and
    f. any additional risks that arise over time related to the industry at large or the protocol at issue; and
3. any unique risks specific to the applicable protocol or smart contract.

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?

Based on our comments from earlier, we believe it would be prudent for the Commission to reevaluate the decision to limit SPBD operations to digital asset securities and cash, based on the unique security considerations required to store, transfer, and otherwise handle both digital asset securities and non-security digital assets. While this limitation is not insurmountable, it does, as noted earlier, stand the chance to introduce market inefficiencies and attack vectors through requiring additional counterparties.

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?

On this point, it's helpful to begin with the Commission's statement. In it, the Commission notes that,

> "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."[8]

While it is true that "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,"[9] we believe that the level of security and consumer protection that can be offered in the realm of digital asset securities can rival that of traditional securities, even though the mechanisms for achieving it may differ substantially.

---

[8] Ibid.
[9] Ibid.

There is already some amount of overlap between the digital asset space and the traditional financial system, and it is reasonable to assume that this convergence will continue, meaning that even SPBDs may at times rely on the services of third party entities like transfer agents.

While there are no best practices to speak of in the clearance and settlement of digital asset securities, we have envisioned a system (based on our experience with non-security digital assets) that can initially utilize a transfer agent which will simultaneously confirm the ownership record in the blockchain until the Commission (and customers) gain the comfort to rely solely on the blockchain (and the records of the custodian) as the source of truth for the ownership of the digital asset securities. Some issuers may never get comfortable in relying solely on a blockchain and thus continue to use a transfer agent. Others may feel more comfortable, and we think there is room for both scenarios.

In the immediate term, we believe clearance and settlement by SPBDs should take the following form. Upon receipt of an order match with an exchange, broker, OTC desk or other counterparty, the SPBD should confirm the match with the counterparty and receive confirmation and approval from the Transfer Agent. Next, the SPBD should transfer the applicable consideration (either digital asset securities or USD) to the counterparty, and instruct the counterparty to transfer the corresponding consideration either into an account with the SPBD for the benefit of its customers, or directly into the appropriate customer account. The Transfer Agent should then record the transaction, which is reflected on the applicable blockchain, and the SPBD should report trade execution and settlement to its customers.

Settling trades on an ATS should take a similar form. In the event of a match, the ATS should send instructions both to the SPBD and the counterparty's custody provider to transfer the applicable considerations as appropriate. In this case, the ATS may be responsible for reporting the trade.The SPBD will actually transfer the applicable assets pursuant to the instructions provided.

As stated earlier, while the mechanism for objectively proving the existence and control of digital asset securities may differ from those employed to prove control over traditional securities, with the correct hardware in place (or other solutions as developed), SPBDs can easily prove exclusive control, and almost instantly grant auditors and regulators proof of existence through challenge-response authentication. In this way, SPBDs can show compliance with the Customer Protection Rule.

Lastly, the Commission is right to point out the irreversibility of transactions in digital assets, securities or otherwise as an important consideration for broker-dealers in the space. That said, where "traditional securities infrastructure has established processes to reverse or cancel mistaken or unauthorized transactions,"[10] emerging digital asset securities infrastructure has its own set of checks and controls designed to ensure that both parties to a transfer agree to its terms before the transaction is completed. This might take the form of a combination of software, hardware, and operational processes. However, because of the fact of irreversible

[10] Ibid.

transactions, when assessing SPBDs ability to operate in the space with the level of security and soundness required for the protection of consumers and the markets, the emphasis on pre-transaction controls needs to be much higher than in traditional securities. For instance, many existing custodial systems require transfer destinations to be whitelisted or for authentication at the device level. While these kinds of controls provide some level of protection against inadvertently authorizing transfers or sending assets to unauthorized wallets, much more can be done. At Anchorage, our security model layers hardware, software, biometrics, and behavioral analysis to authenticate the end users behind the device, all but eliminating any uncertainty around who authorizes a transaction and where funds are ultimately sent.

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?

To date, there has been a large amount of speculation about the future of digital asset securities. And while a few have managed to launch regulated solutions in terms of tokenized securities themselves, there is little to speak of in terms of venues for sale and resale with the appropriate regulatory oversight. We believe this is largely a function of two factors: lack of clear regulatory guidance, and a lack of infrastructure.

As compelling and potentially industry-creating digital asset securities may be, without the appropriate level of regulatory guidance and sound infrastructure, digital asset securities as a concept runs the risk of dying on the vine. For what good is a token listing if there are no regulated venues to buy or sell them? What good is attracting consumer interest if there's no clear, regulated way for consumers to participate in a market? And what good is having the technical capability to develop sound market infrastructure without the political will to allow that infrastructure to operate in a manner that aligns with the interest of consumers and markets?

In issuing its guidance and establishing the ensuing no-action period, the Commission seems to recognize the fact that this chicken-and-egg problem is of our own creation and will take practical strategies to solve. The fact is that the risks associated with leaving this problem unsolved are so much greater than those associated with digital assets themselves. In fact, in the absence of a robust digital asset securities infrastructure and regulatory framework, the Commission runs the risk of inadvertently incentivizing activity in digital asset securities to move to offshore locations, or to operate in an unregulated way, neither of which scenario aligns with the ultimate goals of capital formation and consumer protection.

We again applaud the Commission for taking an important first step in terms of clearing a regulatory space for innovation to incubate in a way that limits risk to the safety and soundness of markets overall. At this point, we would simply reiterate our concerns that limiting SPBD activity to digital asset securities runs the risk of inadvertently birthing a two-tiered system of consumer protections in the digital asset markets, as well as potentially introducing additional security concerns and contributing to unnecessary market complexity. We believe that the solutions we have laid out in answers to the preceding questions lay out a vision for compliance

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

with the Customer Protection Rule with respect to digital assets, securities or otherwise, and hope the Commission considers it informative for the formulation of the Customer Protection Rule as it relates to digital assets.

Postscript: We would also like to note the necessary collaboration of the SEC and FINRA and the need to ensure a unified voice and approach to the proposed safe harbor. While the SEC may have articulated a concept and framework, the actual application of the safe harbor will be conducted for the most part by FINRA. It is crucial that FINRA be apprised of all current thinking in this area and be empowered to approve SPBDs that meet the requirements set forth by the SEC.

Very truly yours,

DocuSigned by:
Nathan P McCauley
DBD6F19D9CCC438...

Nathan McCauley
Co-founder and CEO
Anchorage Digital

DocuSigned by:
Georgia Quinn
7F306CE45FEF49F...

Georgia Quinn
General Counsel
Anchorage Digital