April 12, 2021

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090
Submitted VIA EMAIL to: rule-comments@sec.gov

Re: File No. S7-25-20, Custody of Digital Asset Securities by Special Purpose Broker-Dealers

Dear Commission,

The following is co-authored by the following individuals (the "Co-Authors" or "We"). Co-Author Nicholas Bruno is a third-year law student at Maurice A. Deane School of Law. Mr. Bruno is the Co-Chair of the Blockchain Subcommittee of the Information Technology and Cyber Law Committee of New York City Bar Association. Mr. Bruno is also the Editor-in-Chief of the Journal of International Business and Law.

Co-Author Tyler Yagman is a third-year law student at Maurice A. Deane School of Law with experience in both capital markets trading and in the digital asset space. Mr. Yagman is the Co-Chair of the Blockchain Subcommittee of the Information Technology and Cyber Law Committee of New York City Bar Association.[1]

Co-Author Philip Dursey currently serves as Head of Cybersecurity & Security Architect at a boutique secure cloud services provider; Cyber Auxiliarist with USMC; and Founder of Keyed, a premier cryptocurrency security consultancy. Mr. Dursey is also a Stanford University- and MIT- trained and certified professional in multiple disciplines related to cyber security. Mr. Dursey is currently on track to distinction in the MSc in Software & Systems Security at the University of Oxford, where he previously earned the UGAD in IT Systems Analysis & Design. Mr. Dursey also serves as Technology Director of the Oxford University Strategic Studies Group (OUSSG).

Co-Author Ariel Deschapell is the Head of Engineering for the Lincoln Network, with extensive experience leading software development efforts across a variety of verticals, including blockchain development. Mr. Deschapell has many published pieces covering blockchain technology on outlets such as Coindesk, and is well versed in the creative applications of general cryptographic primitives such as public/private key infrastructure, hashing, checksums, etc. at projects such as Callisto, and ongoing work with Keyed, a premier cryptocurrency security consultancy.

[1] The SEC previously cited a comment letter co-authored by Mr. Bruno and Mr. Yagman. S*ee* SEC Accredited Investor, 17 C.F.R. § 230.215 (2020) (citing to n.231 within the Final Rule).

Co-Author David T. Ackerman, Esq. is the Regulatory Subject Matter Expert for NICE and NICE Actimize, and the head of the NICE Financial Markets Regulatory Outreach Program. Mr. Ackerman is an internationally recognized compliance and financial regulation expert, industry influencer, published author, and FINRA Arbitrator.

The Co-Authors fully support the Securities and Exchange Commission (the "SEC") in its proactive, forward-thinking approach towards the potential regulation of digital assets. We agree with the SEC's recognition for modern, effective policies that permit the trade of new digital financial instruments while simultaneously benefiting from the security and uniformity provided by prudent regulations. The Co-Authors also greatly appreciate the SEC's decision to solicit public comment to gain better understanding of the "wild west" of digital assets.

The Co-Authors hope the SEC considers the following responses to the questions posed within the Policy Statement on the Custody of Digital Asset Securities by Special Purpose Broker-Dealers (the "Statement")[2]: (1) the industry best practices for generating and securing private keys; (2) the industry best practices the affect custody of digital assets; (3) the processes, software, and hardware systems that secure private keys; (4) the accepted model practices and language with respect to risk disclosure.

I. INDUSTRY BEST PRACTICES FOR GENERATING & SECURING PRIVATE KEYS STEM FROM PROTOCOLS THAT FACILITATE THE DIVISION OF LABOR AND THE MITIGATION OF RISK

A. Security Practices[3]

Account security is necessary for the safety and custody of any digital asset. The use of accounts connected to the internet facilitate the custody and exchange of clients' funds, be they fiat or digital assets.[4] Commonly accessible through a financial institution's web portals, these accounts utilize usernames and passwords as a standard security measure, which, without additional security measures, leaves the funds susceptible to security breaches/failures. The following three factors determine the overall security of the assets secured using hot storage[5]: (1) the strength of the password; (2) the number of parties with access to the username and password associated with the account; (3) the security of the institution with which the account is created.

---

[2] *See* Custody of Digital Asset Securities by Special Purpose Broker-Dealers [*hereinafter* Statement], Release No. 34-90788, File No. S7-25-20, at 16-17 (2020).

[3] The Co-Authors acknowledge that account security does not directly relate, or apply, to the creation and security of private keys. The Co-Authors respectfully submit the belief, though tangential to the request, that the security protocols and practices concerning digital assets outlined herein are most effective when implemented with account security measures. Therefore, We briefly discuss and suggest account security practices. As further discussion is beyond the scope of this comment, We recommend the SEC refer to many of the sources cited below, or to this footnote for a general overview of the topic. *See generally, e.g.*, PAYWARD, INC., *Account Security*, KRAKEN, https://support.kraken.com/hc/en-us/categories/360000036266-Account-Security (last visited Apr. 5, 2021).

[4] Fiat refers to non-digital assets, such as stocks, bonds, and dollars.

[5] *See infra* at III.A (Cold Storage).

1. *Password Strength & Security*

Password strength is the first line of defense for asset protection. Passwords are also "considered one of the most significant risk factors in terms of security in information systems as they are vulnerable to common attacks. The vulnerability is mainly due to user behaviors and practices and not related to the password system itself."[6] The following factors determine password strength: (1) the number of characters; (2) the characters used; (3) the order in which the characters are used. There is a direct correlation between the strength of the password and the complexity of the password. The most secure passwords are those that contain many characters (more than eight) and use a randomized combination of alpha-numeric and special characters.[7]

While the complexity of strong passwords provides increased security, their complexity may also invite poor user behavior and practices that negate the increased security. This may include the recording and sharing of passwords via insecure applications and communication channels. To maintain password security, the best practice is to limit the number of parties with access to this information.

Password management software ("PM") works to solve the problems that stem from strong, complex passwords. PMs' primary function is to securely generate, store, and control access to complex passwords.[8] But not all PMs provide the same level of security and reliability. If a PM's security architecture is flawed and suffers a security breach, then the user's account information may be compromised. The Co-Authors recommend the use of PMs that provide a "zero knowledge solution," which means the individual account holder is the only party with access to the passwords maintained by the PM.[9] Therefore, even if the PM provider is compromised, the user's account information remains protected.

2. *Two-Factor Authentication*

An added security component limiting the number of parties with access to an account is through the use of two-factor authentication ("2FA"). 2FA increases confidence that the individual attempting to login to an account is an authenticated user. There are currently three means of authentication. First, a temporary one-time password ("TOTP") may be sent as a SMS message, phone call, or email. Second, a third-party authenticator[10] creates a one-time password ("OTP") that expires after a short, predetermined

---

[6] *See* M. Yildirim & I. Mackie, *Encouraging Users to Improve Password Security and Memorability*, 18 INT'L J. OF INFO. SEC. 741, 741 (2019).
[7] *See id.* at 742.
[8] When you sign up for an online account, the PM will randomly generate and store a complex password. Usually, the PM autofills the username and complex password so the user does not need to retype them during each login.
[9] *See, e.g.*, BITWARDEN, *Encryption*, https://bitwarden.com/help/article/what-encryption-is-used/ (last visited Feb. 19, 2021).
[10] *See, e.g.*, TWILIO, INC., *Authy*, https://authy.com/ (last visited Apr. 5, 2021).

amount of time. Third, a physical hardware security device ("HSD") may be used to create a TOTP or human-based authentication code ("HMAC") or a one-time password ("HOTP").[11]

An HSD is the most secure form of 2FA. OTPs sent via email may be compromised if the individual's email account is compromised. OTPs sent via SMS message or phone call may be compromised if the individual's phone number is compromised (e.g., a SIM-swap attack).[12] Third-party authenticators are more secure than phone- or email-based authentication because the authentication remains localized to the individual's authentication application.[13] Use of an HSD is the most secure method to verify the account user attempting to login. The upshot of an HSD is that the account cannot be accessed without the timely use of the cryptographic key material stored on the HSD, which must be physically inserted into the computer on which the individual accesses the account. Generally, HSDs may also be used as an extra layer of security when layered with a third-party PM. For example, if a broker-dealer[14] ("BD") has stored a strong, complex password within the PM and wishes to access a client's account, the BD must access the PM, enter the master password, then plug the HSD into the computer to authenticate her identity. These steps must be completed before the account may be accessed.

3. *Institution-Side Security*

A third factor considered to determine the safety and custody of assets is the security of the institution with which the account is created and held. Nearly all financial institutions use some form of 2FA to secure accounts. Unfortunately, most use phone- or email-based 2FA.[15] This practice poses a significant security risk. If, for example, an institution (or third-party) has a data breach in which client names, usernames, phone numbers, and email addresses are compromised, bad actors may use that information to reset client passwords and gain access to accounts. Use of HSDs may mitigate this threat because, even if a bad actor has a client's information, the account cannot be accessed without the physical hardware device, activated manually at the precise time required.

---

[11] *See, e.g.*, YUBICO, *Product Briefs*, https://www.yubico.com/resources/product-briefs/ (last visited Feb. 19, 2021). While Yubikey is not the only HSD on the market, it is one of the most trusted because it is FIDO certified. The FIDO certification carries significant weight in the security industry. *See* FIDO ALLIANCE, *How FIDO Works*, https://fidoalliance.org/how-fido-works/ (last visited Mar. 25, 2021).

[12] *See* NORTON LIFELOCK INC., *SIM Swap Fray Explained and How to Help Protect Yourself*, https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html (last visited Feb. 19, 2021).

[13] *See generally* Can Ozkan & Kemal Bicakci, *Security Analysis of Mobile Authenticator Applications*, INT'L CONF. ON INFO. SECURITY & CRYPTOLOGY, 18 (2020), available at: https://ieeexplore.ieee.org/abstract/document/9308020?casa_token=mDjXDLTLWmgAAAAA:FXUKL7fd7-WylIoQV69HTwNBXdUoDqNY4bA8W9tfw-qYVXhOVbMz5mv65l1yMJC1ySOLf3iVzUk1BQ (analyzing the means by which various mobile authenticator applications may be compromised).

[14] For brevity and clarity, the Co-Authors conflate broker-dealers with individual financial advisors and SEC registered representatives unless otherwise specified.

[15] *See* Robert D. Lee, *Authentication in Internet Banking: A Lesson in Risk Management*, FDIC (Dec. 10, 2007), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/article05_authentication.html.

Despite their positives, there are downsides to using HSDs for 2FA. The attribute that makes HSDs the most secure form of 2FA also creates a security issue; the HSD is physical and, therefore, may be misplaced, lost, or stolen. A common remedy to this issue is the use of a second HSD that is linked to the first HSD and serves as a failsafe backup. If the first HSD is lost, misplaced, or stolen, then the backup HSD may be used to access the relevant accounts and can then be used to disassociate the first HSD from the accounts. This prevents an unauthorized user from accessing accounts via the first HSD. Despite this security issue, use of HSDs for 2FA remains the best way to secure an account. Accordingly, the Co-Authors propose the SEC encourage all relevant institutions to implement the use of HSDs as a means of 2FA.[16]

4. *Cold Storage*[17]

When assets are in cold storage (also referred to as being air-gapped), they never connect to a computer network (assets stored on networked devices are considered hot storage).[18] Cold storage significantly reduces the threat of an account being hacked remotely, the most likely means of attack. Cold storage methods are unique to digital assets and are the most secure way to store private keys. Products known as hardware wallets serve as cold storage devices for private keys. Hardware wallets are secured by numeric passcodes and may be further secured with HSD integration.[19] Like HSDs, the most significant security issue that affects hardware wallets is the threat that it may be lost, misplaced, misconfigured, or stolen. As with HSDs, the threat may be mitigated by using a second hardware wallet as a backup. Use of a second hardware wallet that is also protected by an HSD is the most secure way to store digital assets.

B. Security Standards

The Co-Authors proposed that the SEC implement the above-mentioned security practices in accordance with the security guidelines promulgated by the National Institute of Standards and Technology[20] ("NIST"), the National Association of Corporate Directors[21] ("NACD"), the Open Web

---

[16] YUBICO, *Protecting Financial Organizations from Cyber Security Threats: Prevent Fraud and Lost Revenue*, https://www.yubico.com/solutions/industries/finance/ (last visited Feb. 19, 2021).

[17] The Co-Authors refer to "cold storage" in different contexts and with different meanings throughout the comment. For sake of brevity and clarity, "cold storage" refers to *private keys that are not connected to the internet* unless otherwise specified.

[18] *See infra* at III.A (Cold Storage).

[19] *See, e.g.*, LEDGER, *Beyond Crypto: Securing Accounts with U2F*, https://www.ledger.com/academy/beyond-crypto-securing-accounts-with-u2f (last visited Feb. 19, 2021); SATOSHILABS, *Use FIDO2 With Trezor Model T*, TREZOR, https://trezor.io/fido2/ (last visited Feb. 19, 2021).

[20] *See generally*, ELAINE BARKER, ET AL., NAT'L INST. OF STANDARDS AND TECH., A FRAMEWORK FOR DESIGNING CRYPTOGRAPHIC KEY MANAGEMENT SYSTEMS, NIST SPECIAL PUBL'N 800-130 (2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf.

[21] NATIONAL ASSOCIATION OF CORPORATE DIRECTORS [*HEREINAFTER* NACD], DIRECTOR'S HANDBOOK ON CYBER-RISK OVERSIGHT (2020).

Application Security Project Foundation [22] ("OWASP"), and the CryptoCurrency Certification Consortium[23] ("C4"). The SEC may use these guidelines in conjunction with existing regulations to create comprehensive policies concerning BD digital asset custody.

C. Proposal

1. *Security Protocols*

First, the Co-Authors propose the following protocols to assist BDs with securing custody of digital assets. The Co-Authors propose the SEC encourage all passwords and usernames used to access client accounts, alternative trading systems ("ATS"), or other sensitive information be stored and/or generated on a PM. The PM should then be authenticated against an HSD for additional security.

Second, the Co-Authors propose two HSDs secure each hardware wallet. The Co-Authors suggest the SEC encourage or require those individual BDs who manage clients' portfolios to maintain possession of one HSD. The Co-Authors further suggest the use of a lockbox, safe, or other secure, accessible location to house HSDs associated with their clients' accounts. The second HSD, which operates as a backup to the first HSD (held by the representative), should be located in a lockbox, safe, or other secure location to which the representatives do not have, and cannot, access. The individual(s) who manage(s) or supervise(s) the representatives should be the only employee(s) at the BD firm who have access to the location in which the second HSDs are kept.

Third, the Co-Authors propose the following steps by which BDs should secure seed words.[24] First, it is necessary to identify the individuals who will have access to the seed words. As will be discussed in greater detail below, those with access to the seed words should be different than those with access to the HSDs and hardware wallets.[25] This will mitigate the risk of improper access to client funds.[26] Second, the seed words should be non-traceably transcribed on paper or, preferably, on a more durable material.[27] Third, once the seed words are transcribed, the words should be split into two groups and distributed to

---

[22] OWASP FOUNDATION, INC., OWASP SAMM v2.0 – CORE MODEL DOCUMENT (2020), *available at* https://github.com/OWASP/samm/blob/master/Supporting%20Resources/v2.0/OWASP-SAMM-v2.0.pdf.
[23] CRYPTOCURRENCY CERTIFICATION CONSORTIUM [*HEREINAFTER* C4], *Cryptocurrency Security Standard*, https://cryptoconsortium.github.io/CCSS/Details/ (last visited Feb. 19, 2021).
[24] *See infra* at III.B (Wallet Backup, Redundancy & Safety).
[25] *See infra* at III.E (Operational Context & Recommended Controls).
[26] *See* FFIEC IT Examination Handbook II.C.7(c) & ISO 27002 https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(c)-segregation-of-duties.aspx.
[27] *See, e.g.*, https://jlopp.github.io/metal-bitcoin-storage-reviews/.

different secure locations,[28] such as a bank vault or safe.[29] Finally, the groups of seed words must be effectively catalogued and secured with tamper-proof bags or containers.[30]

Security risks unique to digital assets necessitate these protocols that are otherwise unneeded with fiat assets. The security practices and protocols stated above are the industry best practices to generate, transfer, and secure private keys.

II. INDUSTRY BEST PRACTICES THAT AFFECT CUSTODY OF DIGITAL ASSETS

Historically, market volatility or internal factors (i.e., poorly managed trading risk, managerial oversight issues, and internal fraudulent activity) paved a BD's path to insolvency.[31] These types of insolvency triggers are, to an extent, avoidable. For example, BDs often have thorough contingency plans to counteract a spectrum of market volatility scenarios in order to prevent insolvency and to preserve client assets. Another prime example is the evolution of managerial oversight within BDs. Through countless iterations of best practices standards, trading oversight protocols, and compliance monitoring, the list of variables that lead to insolvency has diminished over time.

Recently, the focus on risk derived from unprecedented market volatility and operational shortfalls has shifted as these risks have been trumped by a new, dynamic category of risk—cybersecurity. Cybersecurity risk involves complex mechanics that may damage a BD remotely, anonymously, and most concerning, instantaneously. Since the mainstream adoption of institutional and retail digital-asset-based investment strategies, the financial industry now must tackle a new sub-category of cybersecurity risk that was once novel and considered implausible—cryptographically-based cybersecurity risk of the transmission and storage of digital assets. In order to fully comprehend the cybersecurity risk derived from trade and storage of digital assets, it is imperative to distinguish this risk from conventional cybersecurity risk mitigation approaches and prevention methods.

To understand why risks associated with digital assets are more significant, consider digital-asset-based cybersecurity from the perspective of a black hat hacker.[32] In short, hacking is a business with a balance sheet like any local retailer. If the vulnerable party makes it particularly difficult for the hacker to infiltrate their ecosystem, and thus more costly, the hacker will likely shift her efforts to a more vulnerable

---

[28] This process is referred to as "sharding."

[29] Since a hardware wallet and its backup hardware wallet already exist, the seed words do not need to be as accessible but should remain somewhat easily accessible if both hardware wallets become compromised.

[30] *See* FFIEC IT Examination Handbook II.C.7(c) & ISO 27002 https://ithandbook.ffiec.gov/it-booklets/operations/risk-identification/technology-inventory/hardware.aspx.

[31] *See, e.g.*, Julie Steinberg, et al., *Greensill Faces Possible Insolvency After Credit Suisse Suspends Investment Funds*, THE WALL STREET JOURNAL (Mar. 1, 2021), https://www.wsj.com/articles/credit-suisse-suspends-funds-tied-to-softbank-backed-greensill-11614599752.

[32] *See* NORTONLIFELOCK INC., *What is the Difference Between Black, White and Grey Hat Hackers?*, (Jul. 24, 2017), https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.

and less costly target. If the hacker uses her time efficiently, she will likely decide to shift her efforts in the pursuit of maximizing her profit. As the saying goes, "time is money," or in this scenario, "time is crypto." Accordingly, BDs that transact in digital assets must focus on the creation of security protocols that make the BD's ecosystem as secure as possible to increase the amount of time needed to hack the system and subsequently deter hackers[33].

It is important to note that, because of the value associated with digital assets, the stakes are heightened for hackers. If a hacker obtains personally identifiable information via a data breach, that information must still be monetized to turn a profit; this is not the case with digital assets. Hackers understand that once they have access to a user's digital assets, the funds (and the hackers) may vanish in a way nearly impossible to trace.

Cryptography-based attacks were, at one time, considered the work of sophisticated black hat hackers, but, today, cryptography-based cyber-attacks have become more commonplace.[34] Despite the sophisticated nature of cybersecurity attacks, hackers gain most of their opportunities from human error.[35] (Human error as the cause of many digital-asset-based attacks is well documented.)[36] Vulnerabilities like mishandling private keys or having poor password hygiene (i.e., using the same password for multiple accounts or not using 2FA) are equally dangerous because they are innately careless.

A. Risks

1. *Risks that are "Less Likely"*

Many of the risks mentioned in the second question of the Statement are, arguably, not the largest source of vulnerabilities that could render a BD insolvent and expose a client's digital assets. The occurrences of unplanned hard forks and 51% attacks are lower in more established digital assets but are more common in digital assets of lower quality.[37] That being said, the Co-Authors propose the SEC discourage or prevent BDs from trading digital assets that do not meet certain benchmarks of liquidity, network stability, adoption, and trading volume.

---

[33] *See* Brandon Valeriano, *Cost Imposition is the Point: Understanding U.S. Cyber Operations and the Strategy Behind Achieving Effects*, LAWFARE (Mar. 27, 2020), https://www.lawfareblog.com/cost-imposition-point-understanding-us-cyber-operations-and-strategy-behind-achieving-effects.

[34] *See also, e.g.*, Anna Baydakova, *Hackers Mines Crypto on GitHub's Servers: Report*, COINDESK, (Apr. 5, 2021), https://www.coindesk.com/hackers-mined-crypto-on-githubs-servers-report.

[35] *See, e.g.*, Kevin Poulsen, Robert McMillan, & Dustin Volz, *SolarWinds Hack Victims: From Tech Companies to a Hospital and University*, THE WALL STREET JOURNAL (Dec. 21, 2020), https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402.

[36] *See, e.g.*, BBC, *Major US Twitter Accounts Hacked in Bitcoin Scam*, (Jul. 16, 2020), https://www.bbc.com/news/technology-53425822.

[37] Generally, those assets with the largest market caps are considered of the best quality. *See generally also* COINGECKO, *Cryptocurrency Prices by Market Cap*, https://www.coingecko.com/en (last visited Mar. 25, 2021).

2. *Hard Forks*

Hard forks occur when a software update for the peer-to-peer nodes of the digital asset network makes the newly updated nodes incompatible with older versions.[38] Hard forks can be either purposeful changes to a blockchain network, or accidental. When a hard fork is required on major blockchain networks, it is organized via the developer community and demands months of preparation leading to ample time for stakeholder notification.[39] This preparation centers around ensuring the entirety of the network updates to the new ruleset in tandem, negating an undesirable split of the network. However, unplanned hard forks, better known as accidental forks, may also occur when a software update unintentionally impacts consensus rules when released. When this occurs, direct intervention is required by the developers to release a "hot fix" for the issue and bring the network back to consensus.

To negate the risk of an accidental fork, the Co-Authors propose BDs control a full node of the blockchain on which the digital asset is built, which BDs should actively monitor and keep up to date with latest patches as required to address vulnerabilities. We strongly recommend running a full node, or maintaining complete control of an independent node, for each digital asset type/blockchain traded or stored for clients. As a result, a registered representative at a BD will likely have sufficient time to prepare her clients and operations for shifts stemming from hard fork changes.

Running a full node also provides the added benefit of being able to monitor the existence of orphan blocks and chains, which while not considered hard forks, can also temporarily split the chain (i.e., accidental forks). This occurs when two miners of the same blockchain produce a new block nearly simultaneously. This relatively uncommon occurrence forces one chain to become the dominate chain, thereby inadvertently leaving the network to abandon the blocks not on the non-dominate chain (i.e., orphaned blocks).

3. *Airdrops*

An airdrop is a release of a certain number of coins/tokens by the creator to the public to create interest around budding digital asset projects.[40] Airdrops are commonly used as a marketing tool by digital asset creators. While airdrops draw attention from individual investors, they are commonly used as (highly) speculative-grade digital assets that are typically not suitable for the average investor.

---

[38] Not all software updates to a digital assets result in a hardfork. Hard forks specifically occur when a software update changes the fundamental "consensus rules" of the network in a way that is incompatible with the previous rules. One concrete example includes increasing the maximum allowed block size of a digital asset's blockchain beyond the former limit. If not all nodes update, then a block mined that is larger than the previous limit will not be recognized by non-updated nodes and force the block to split off the network from the point of that block.

[39] *See, e.g.*, COINBASE, *November 2020 BCH Hard Fork*, https://tinyurl.com/uwv3jb67 (last visited Mar. 25, 2021).

[40] *See, e.g.*, Anna Baydakova, *The IRS Just Issued Its First Cryptocurrency Tax Guidance in 5 Years*, COINDESK, (Oct. 9, 2019), https://www.coindesk.com/the-irs-just-issued-its-first-cryptocurrency-tax-guidance-in-5-years.

The Co-Authors propose the SEC limit or prevent interaction between BDs and creators who use airdrops. We also propose the SEC limit or prevent client purchases of airdrop-prone digital assets because of the additional uncontrollable risk surrounding the digital asset. Further, We recommend the SEC discourage BDs from exchanging digital assets that engage in airdrops. Airdrops present many technical complexities and security risks which are non-trivial to navigate, and to date no airdropped cryptocurrency has demonstrated any lasting traction.

4. *51% Attacks*

A 51% attack is orchestrated by a group that possesses a majority (unintuitively, sometimes as low as 33%) of a blockchain network's hash rate and can manipulate the blockchain's transaction ordering, which affects the function of the digital assets that sit on that network.[41] A 51% attack may harm investor confidence by causing havoc through a sudden liquidity constraint or sudden market value erosion. However, 51% attacks are less of a concern for more-established digital assets with diversified hash power as it becomes more difficult for a 51% attack to occur with digital assets that's hash power is less concentrated.

The Co-Authors recommend the SEC encourage BDs to run a full node of the digital asset/blockchain to independently monitor the network. It's important to note that so long as a BD runs a full node and independently monitors the network and validates network rules, a 51% attack cannot introduce invalid transactions to the network and can only create unpredictability in transaction ordering and confirmation. The cost of a 51% attack increases non-linearly for every new block produced in a chain, meaning the havoc that can be caused in transaction ordering can be circumvented by waiting for a sufficiently large number of blocks to be produced since a transaction's initial confirmation before considering it final and settled. As such, We further recommend the SEC encourage BDs to maintain a conservative confirmation time for transaction settlements of 100 blocks for bitcoin and equivalent elsewhere as an additional precautionary measure for these attacks. We also recommend the SEC discourage BDs from transacting in more speculative, unestablished digital assets until their hashing power is stable and diversified.

5. *Monitoring These Risks*

The Co-Authors propose the SEC encourage or require BDs that handle digital assets to have a contingency plan for when the assets in the BDs' custody engage in a hard fork, are at risk for of a 51% attack, or are subject to a potential air drop (among other more prevalent risks).

---

[41] *See, e.g.*, Adam B. Levine, *The 51% Attack Nightmare Scenario (Isn't That Bad)*, COINDESK, (Sep. 27 2020), https://www.coindesk.com/51-percent-attack-explained-podcast.

6. *The Risks that are "More Likely"*

Although the risks mentioned above are within the realm of concern, there are more prevalent risks about which firms must be cognizant. These include the following: (1) Ransomware attacks; (2) Malware on Compromised Devices; (3) Supply Chain Attacks ("MITM Attacks"); (4) Compromised Private Keys (Human Behavioral Issue); (5) subpar "know your client" verification standards ("KYC"); (6) Phishing/Spear Phishing; (7) restricting physical access to sensitive areas of the broker dealer.

7. *The Human Element*

As easily as human behavior may contribute to cybersecurity risk, it may contribute to mitigating cybersecurity risk. In today's complex age of industry, business no longer operates using analogue means. For example, today, an agriculture-based business is no longer in the business of only agriculture; it is also a technology business. Likewise, a BD is no longer just a financial business; it is also technology business. Normalizing the technology conversation and having employees understand this "business category" shift and promoting a change in perspective from operating as a trader or financial advisor to operating as a technology user can promote significant security buy-in. Building and maintaining a strong security culture means using tools like experimental learning and gamification, proper analogies and "horror stories," micro and nano learning platforms and teaching programs, and, most importantly, open dialogue about technology and security.[42]

B. <u>Proposal</u>

The Co-Authors propose the SEC require BDs dealing in digital assets to train employees, at minimum annually. We recommend that training focus on the mitigation of reasonably preventable attacks stemming from human error, lack of technological literacy, and blatant carelessness.[43]

Digital asset trading and storage requires protocols that are diligently followed. Digital asset storage requires a deep understanding of the technology behind blockchain technology and foundational cryptography. Employees of BDs who transact and store digital assets should possess a deep understanding of the heightened risk involved as well as the heightened responsibility that accompanies trading and storage of clients' digital assets. Accordingly, those BDs who are unwilling to make the substantial investment in time, training, education, and solutions required to safely trade and store digital assets for clients should not be allowed to do so.

The Co-Authors further propose the SEC require the relevant BDs to submit quarterly security and training protocols (in some cases quarterly depending upon volume or exposure) as well as annual

---

[42] *See* Jinan Budge, et al., *How to Manage the Human Risk in Cybersecurity: Continuous Improvement: The S&R Practice Playbook*, FORRESTER RESEARCH, INC. (Jan. 13, 2021).

[43] We propose the SEC define what a reasonably preventable attack is as well as define carelessness with regard to BDs' digital-asset-based cybersecurity risk in order to communicate to BDs the severity and what is expected of them.

security audits from independent cybersecurity and digital asset security auditors. We also propose relevant BDs be encouraged to maintain a required capital allocation reserved for *only* the immediate need to finance security infrastructure updates in response to sudden shifts in security standards, which are inevitable. Additionally, We propose the SEC create a unique licensing examination required for principles, registered representatives, as well as other relevant employees of a BD who want to engage in digital-asset trading and storage. This license should include, at minimum, tested material concerning foundational cybersecurity literacy and the unique technology that makes up the digital asset industry. We believe that the exam should include hypothetical risk scenarios that test on compliance, general trading and storage of digital asset protocols, risk mitigation, human behavior/carelessness mitigation, and proper reporting practices to compliance and governing authorities. Additionally, because the digital asset space evolves rapidly, the Co-Authors propose annual completion of CLE's on digital asset industry updates.

Holding BDs to a high standard creates a level of respect and appreciation for the technology and, thus, a level of respect for following strict security protocols. We propose this high bar primarily for consumer protection purposes. If a trading or storage error occurs, a diligent and well-trained BD can act swiftly to correct the error, thereby giving clients the protection they deserve.

III. PROCESSES, SOFTWARE & HARDWARE SYSTEMS THAT SECURE PRIVATE KEYS

To secure any cryptocurrency, BDs must focus on the design, implementation, and maintenance of a system that secures, maintains, and permits continuous use of private keys that remain in the custody of BDs. The established, and recommended, industry systems that securely address this challenge include the following components:

- Cold storage or "offline" wallets
- Wallet backup, redundancy, and safety
- Hierarchical Deterministic Wallets
- Multi-signature schemes
- Operational Context and Recommended Controls

All institutional-grade transactional and storage infrastructure uses some combination of all of these technologies and systems to securely manage private keys.

A. Cold Storage

Cold storage or "offline wallets" increase the likelihood that private keys never connect to a networked computer. Cold storage is the cornerstone of any secure custody solution because it significantly mitigates threats that stem from internet connectivity, which is the most significant attack surface in regard to private key security. Many known remote malware and intrusion techniques exploit internet connectivity, which may result in the compromise of private keys and associated funds. For the highest degree of security for the full lifecycle of key material, those with custody of private keys must, from their

inception, isolate the private keys from any networked computer. This is accomplished by securing an off-the-shelf computer, loading it with known sanitized wallet software via trusted physical USB,[44] and proceeding to generate corresponding private and public keys. This process and all ongoing management of the BD's keys requires no internet connection at any time.

To maintain the isolation of private keys as they are used by different BDs, the Co-Authors suggest the SEC encourage the physical removal of all onboard Wi-Fi, Bluetooth, and other wireless and network interfaces. To further protect the offline wallet from unwanted intrusion and the tail risk of corruption by EMP signals, the Co-Authors also suggest the use of a faraday enclosure (e.g., faraday cage, bags, case, etc.).

To facilitate the BDs' operations, three types of data must be transferred to and from the secure cold storage via means of a USB. First, public key derived addresses facilitate the deposit of digital assets to the BD from any party. Second, to facilitate outbound transfers of digital assets, unsigned transactions are safely prepared on a networked computer. Third, those unsigned transactions are manually transferred to the cold storage wallet and signed with the private keys necessary to authorize them. Finally, after these three types of data are transferred, the BD re-uploads the transactions to a networked computer to broadcast to the respective peer to peer network that initiated the transaction. All of these data types and properly-authorized operations may be batched to simplify procedures. This practice improves operational efficiency and limits access to the cold storage wallet, which may be supervised and scheduled at predetermined intervals (the industry standard is once every 24 hours).

B. Wallet Backup, Redundancy & Safety

Next, the Co-Authors suggest it is an industry best practice to back up the data used to recover a wallet into multiple secured copies. This practice protects the funds from events that may lead to the loss or inaccessibility of an offline wallet. It is standard practice to store these backups on paper or other material in the form of "seed words."[45] While not standard practice, the Co-Authors strongly suggest the SEC encourage institutions to use more durable archival materials, such as non-corrosive metals, instead of paper.[46] The transcription of the seed words on a durable, non-computational medium, such as stainless steel, mitigates the possibility of backup failure caused by data degradation, EMP, or fire/water damage.

The Co-Authors recommend seed words be halved, securely catalogued, geographically distributed to secure locations by trusted couriers, and appropriately secured at registered financial institutions. These

---

[44] *See* RICHARD KISSEL, ET AL., NAT'L INST. OF STANDARDS AND TECH., GUIDELINES FOR MEDIA SANITIZATION, NIST SPECIAL PUBL'N 800-88 9-11 (2014), http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[45] *See*, *infra*, at Section III.C (Hierarchical Deterministic Wallets).

[46] *See* Jameson Lopp, *Metal Bitcoin Seed Storage Reviews*, https://jlopp.github.io/metal-bitcoin-storage-reviews/ (last visited Mar. 16, 2021).

protocols are necessary because they make it more difficult for a bad actor to obtain an entire seed phrase, which would permit the theft of funds from the private keys. Additionally, the seed words need not be as accessible as their corresponding cold wallet because the seed words merely provide a means by which the cold wallet may be restored in the event of a problem. Any two corresponding backup halves may be used to restore the wallet by repeating the cold storage procedure (i.e., importing the reconstituted seed phrase in place of generating a new wallet) before resuming normal operations.

C. Hierarchical Deterministic Wallets

There are various types of wallets used to manage digital assets. One of the most popular, and the one that the Co-Authors suggest, is the Hierarchical Deterministic ("HD") wallet, which provides a set of unique features. HD wallets consist of a single "seed" of 12 - 24 words. The single seed of words may be used to create simple backups or, alternatively, may be used to derive an infinite number of private and public key pairs. Additionally, HD wallet software, defined by BIP 32 and BIP 44, can export an arbitrary number of these public keys and the derived digital asset addresses from cold storage without exposure of the associated private keys.[47] This feature permits a BD to easily pre-generate any number of required addresses to facilitate deposits from clients and institutions, such as an ATS, without compromising the isolation of the BD's offline wallet. To then send these funds to other firms and institutions, pending transactions are prepared using a networked hot wallet,[48] collected into a device such as a sanitized USB,[49] and physically connected to the cold storage wallet in order to authorize the transaction using the associated private keys.

D. Multiple Signature Scheme

Digital asset wallets may also employ multiple signature schemes, which require multiple digital signatures from distinct private keys housed in separate wallets in order to authorize a transaction. The exact schemes vary widely; the most popular implementations are often comprised of two of three total private key signatures, or three of five total private key signatures. The Co-Authors propose the SEC encourage BDs implement this additional layer of authorization to finalize any set of transactions to protect against internal unauthorized or accidental use of funds. Each set of independent private keys may be secured through the same cold storage and redundancy recommendations stated above.

E. Operational Context & Recommended Controls

Desirable cryptographic systems properties, such as those exhibited by digital assets, rely heavily on factors beyond the aforementioned technical components and depend on myriad human- and

[47] *See* ANTONOPOULOS, *supra* note 17, at 285-287.
[48] *See* Will Kenton, *Hot Wallet*, INVESTOPEDIA (last visited Mar. 16, 2021), https://www.investopedia.com/terms/h/hot-wallet.asp.
[49] *See* KISSEL, ET AL., *supra* note 26, at 9-11.

operations-centric mechanisms that are effective in a variety of contexts. Security professionals successfully apply to financial services time-tested principles and security controls groups, which include, but are not limited to, the following: (1) least privilege; (2) segregation of duties;[50] (3) dual control;[51] (4) split knowledge; (5) tamper resistance, (6) tamper evidence;[52] (7) chain of custody; (8) privacy by design[53] (for privacy & operations security); (9) logical & physical access controls, including logging; (10) threat management, risk modeling, and secure reference architectures.

The following are examples of how some of the principles and controls listed above may be implemented: (1) management ensures that sensitive digital asset processes and procedures are conducted on a need-to-know basis by security vetted personnel; (2) segregating duties, such as authorization, accounting and transactions, helps control for accidental and malicious insider threats; (3) requiring two or more managers to authorize a digital asset transaction or procedure is recommended security and business practice; (4) splitting keys, or key phrases, for secure (redundant) storage provides for defense-in-depth[54] across time, space and emergencies; (5) tamper resistant and tamper evident packaging provides an additional layer of protection and detection for key material during storage and transit; (6) custody of key material and key material access, in whole or in part, should be logged, monitored and regularly audited; (7) robust physical access controls to sensitive digital assets (key material) should include appropriate physical security, printer security, barriers and protections and the strict control of removable media and recording devices during key handling and processing (i.e. CCTV, smartphones, cameras, notepads, etc.).

The Co-Authors recommend Security Operations[55] and Operations Security[56] be expertly designed and independently tested as complimentary, yet distinct, capabilities for BDs working with digital assets. Security and privacy should include the maintenance and protection of information in addition to digital asset confidentiality, integrity and availability. The Co-Authors further suggest the SEC encourage

---

[50] *See* FFIEC IT EXAMINATION HANDBOOK [*hereinafter* Exam. Handbook], FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL [*hereinafter* FFIEC] § II.C.7(c) (*available at*: https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(c)-segregation-of-duties.aspx).

[51] *See* ELAINE BARKER, ET AL., NAT'L INST. OF STANDARDS AND TECH., RECOMMENDATION FOR KEY MANAGEMENT—PART 2: BEST PRACTICES FOR KEY MANAGEMENT ORGANIZATION, NIST SPECIAL PUBL'N 800-57 14 (2005) (defining "dual control" as: "A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single entity is able to access or use the materials, e.g., cryptographic keys.").

[52] *See* DYLAN YAGA, ET AL., NAT'L INST. OF STANDARDS AND TECH., BLOCKCHAIN TECHNOLOGY OVERVIEW, Internal Report No. 8202, 54 (2018), https://doi.org/10.6028/NIST.IR.8202.

[53] *See* PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE [*hereinafter* FTC Report], F.T.C. 22-30 (2012).

[54] *See Defense-in-Depth*, NAT'L INST. OF STANDARDS AND TECH., (last visited Mar. 16, 2021), https://csrc.nist.gov/glossary/term/defense_in_depth.

[55] *See* JOHN WARSINSKE, ET AL., THE OFFICIAL (ISC)2 GUIDE TO THE CISSP CBK, (ISC)2 758 (2019).

[56] *See* SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS, NAT'L INST. OF STANDARDS AND TECH, NIST SPECIAL PUBLICATION 800-53 323-24 (2020), https://doi.org/10.6028/NIST.SP.800-53r5.

BDs pay particular attention to the comprehensive threat modeling, privacy, authentication, authorization and accountability requirements for all purchasing, custodianship, and delivery and operations interfacing systems.

The Co-Authors propose the SEC prioritize the design and deployment of the following Security Operations: (1) key compromise protocol training and rehearsals;[57] (2) key management runbooks and workflow integrated checklists; (3) ongoing security audits, assessments, wargames and penetration tests; (4) data sanitization and audits;[58] (5) application and protection of audit logs and security monitoring.

The Co-Authors also propose the SEC prioritize the design and deployment of the following Specific Operations Security[59] and Privacy Engineering[60] processes and targets: (1) Threat Intelligence & Threat Analysis; (2) Vulnerability Analysis; (3) Risk Assessment; (4) Countermeasures (e.g., data minimization, strong (metadata) differential privacy and anonymity, forward secrecy, decentralized UTXO mixing (i.e., CoinJoin[61]), strong auth, and collection limitations).

F. Security Oversight and Governance

The Co-Authors propose the SEC encourage BD firms develop an expert-advised, board-level information and cybersecurity oversight function[62] to align the organizations' corporate governance structures with management, compliance and operations and direct them towards an enhanced security posture. Within the context of cyber risk oversight, We recommend the SEC encourage management, with expert guidance, (re)design an organizational information security policy model.[63] Ideally, this model enforces the rigorous application of protection properties across security targets, programs, protection mechanisms/controls and protection profiles.[64] Such information security policy portfolios should be consistent with industry standards of information security, cybersecurity, privacy engineering, cryptographic engineering, and key management generally, such as ISO/IEC 27000, and, specifically, to digital asset security standards, which are outlined below.

The Co-Authors also suggest the SEC require BD firms make best efforts to harmonize their organizational policies, processes and procedures with a security model that includes, but is not limited to,

---

[57] *See* C4, *supra* note 15, at 1.05 (Key Compromise Protocol).
[58] *See* C4, *supra* note 15, at 2.02 (Data Sanitization Policy).
[59] *See generally* JOINT CHIEFS OF STAFF, JP 3-13.3, OPERATIONS SECURITY (2016).
[60] *See generally* NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, NAT'L INST. OF STANDARDS AND TECH., Version 1.0 (2020), https://doi.org/10.6028/NIST.CSWP.01162020.
[61] *See CoinJoin*, RIVER FINANCIAL INC., (last visited Mar. 16, 2021), https://river.com/learn/terms/c/coinjoin/.
[62] *See* NACD, *supra* note 13, at 20-23.
[63] *See* ROSS ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 316-17 (3RD ED. 2020).
[64] INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—EVALUATION CRITERIA FOR IT SECURITY, INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM., ISO/IEC No. 15408-1, 31-32 (2014) (corrected version of 3rd ed. 2009).

the following security properties: identification, prevention, protection, detection, response and recovery.[65] These properties are fundamental to the design of adequate security controls, threat models, procedures, and the related structures required to interface securely with cryptographic key management systems ("CKMS").[66]

The following two sources provide instruction and guidance concerning industry standards, control sets, and procedures for the protection of private digital asset key material generation, safekeeping and use against theft, loss, unauthorized, or accidental misuse:

1) CryptoCurrency Security Standard from The CryptoCurrency Certification Consortium[67]
2) #SmartCustody from Blockchain Commons[68]

The following are relevant industry standards and procedures, which include, but are not limited to, the following:

A. Key Security Practice Areas[69]
    1) Governance
    2) System Architecture & Design
    3) Implementation
    4) Verification & Validation
    5) Operations
B. Key Capabilities
    1) Risk Modeling[70]
    2) Threat Modeling, informed by digital asset specific cyber threat intelligence
C. Key Control Groups
    1) Key/Seed Generation Controls[71]
    2) Wallet Creation Controls
    3) Key Storage Controls
    4) Key Usage Controls
    5) Key Compromise Protocols and Emergency Procedures[72]
    6) Keyholder Grant/Revoke Policies and Procedures
D. Recommended Operational and Validation Security Control Groups
    1) Security Audits, Security Reviews, Cyber Wargaming, Red Teaming, Penetration Testing & Adversary Simulation Testing
    2) Data Sanitization Controls
    3) Proof of Reserve Controls

---

[65] *See* FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VERSION 1.1, NAT'L INST. OF STANDARDS AND TECH. 6-19 (2018).
[66] *See, e.g.*, ELAINE BARKER, ET AL., *supra* note 12, at 14-16.
[67] *See* C4, *supra* note 15.
[68] *See generally* CHRISTOPHER ALLEN & SHANNON APPELCLINE, *supra* note 66.
[69] *See generally* OWASP FOUNDATION, INC., *supra* note 14.
[70] *See* CHRISTOPHER ALLEN & SHANNON APPELCLINE, #SMARTCUSTODY: THE USE OF ADVANCED CRYPTOGRAPHIC TOOLS TO IMPROVE THE CARE, MAINTENANCE, CONTROL, AND PROTECTION OF DIGITAL ASSETS 23-56 (2019).
[71] *See* ELAINE BARKER & JOHN KELSEY, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS, NAT'L INST. OF STANDARDS AND TECH., NIST SPECIAL PUBLICATION 800-90A 17-21 (2015), http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.
[72] *See* CHRISTOPHER ALLEN & SHANNON APPELCLINE, *supra* note 66, at 61-92.

4) Audit Logs Controls

IV. ACCEPTED MODEL PRACTICES AND LANGUAGE WITH RESPECT TO RISK DISCLOSURE

A. Disclosure of Digital Asset Risk

Disclosure is and has been a central aspect of national policy in the field of securities regulation. An examination of disclosure policy as applied to the sale of digital asset securities is appropriate for similar reasons the Wheat Report was announced in 1967.[73] Among them are: (1) the rapid increase in the American shareholder population interested in digital assets and the accompanying increase in the number of investment decisions; (2) the trend toward a greater measure of stability in the securities business when applied to digital assets, with the accompanying demand for more information about issuers of digital assets or tokens; (3) the expansion in the coverage of the '34 Act's reporting and registration provisions effected by changes in national and state policy as applied to digital assets; (4) technological advances that enable users unprecedented information access from a variety of sources and on a variety of devices at less expense than was previously possible; and (5) the growing criticism of the status quo in disclosure and lack of overall transparency into digital based assets.

Consistency of disclosure is haphazard at best in an environment devoid of regulation, principles-based expectations, and subsequent enforcement. The Co-Authors respect and support the SEC's decision to strengthen the disclosure process surrounding this rapidly growing area of investing.

B. General Disclosure and Evaluation Criteria

The SEC's 1969 Wheat Report viewed disclosure as necessary, first, for the prevention of fraud and manipulation and, second, to provide investors and speculators with enough information to enable them to arrive at their own rational decisions. The Co-Authors suggest the SEC evaluate any generally accepted practices with respect to disclosing the risks of digital asset securities through this lens. Due to the highly complex nature of the risks associated with the sale or purchase of any digital asset security, the Co-Authors propose the SEC encourage or require the following umbrella of best practices when disclosing risks and/or conflicts:

- Wherever possible, disclosure should be in plain English. Limit the use of industry-specific jargon or undefined terms, and include short, declarative sentences.
- Focus should be drawn to the most critical information a reasonable investor would use to make an informed decision. This information should be prominently displayed on the page.

[73] SEC, DISCLOSURE TO INVESTORS – A REAPPRAISAL OF FEDERAL ADMINISTRATIVE POLICIES UNDER THE '33 AND '34 ACTS 10 (1969) [hereinafter cited as WHEAT REPORT] *available at* http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1960/1969_Wheat_CH01.pdf.

- Best efforts should be made to explain how risks associated with digital assets are particularly unique to investing—highlighting common occurrences such as volatility or exchange arbitrage.

Furthermore, the Co-Authors suggest it prudent for firms to publicly disclose on their website policies specifically related to the purchase, sale, or custody of digital asset securities. This may potentially include, but is not limited to, policies and procedures related to[74]:

- Governance
- Key Management
- Backup and Recovery
- Environmental/physical security
- Vulnerability Management

C. Situational Disclosure

To effectively analyze any recommended model language, the Co-Authors will analyze disclosure delivery in two parts. First, when a client is introduced to the concept of a sales strategy or investment plan inclusive of digital asset securities, and second when a specific recommendation is made.

Disclosure should be made at the time a client is introduced to the concept of digital based asset investing, be that at the onset of the client relationship or after a long-existing repour. Assuming all applicable suitability procedures are satisfied, disclosure of the material facts and risks associated with digital based assets should be explained at a high level with particular emphasis on differences between more traditional investments like equities, and that of assets containing digital underpinnings. Example language may read:

> A Cryptocurrency's value is derived exclusively by the market forces of supply and demand, unlike a stock which represents fractional ownership in a corporation. Cryptocurrencies are not generally backed or supported by any government or central bank, and as a result can be highly volatile.

Explaining the differences between digital based assets and more traditional investments becomes exponentially more important as greater numbers of complex investment products incorporate digital assets into their structure. At a minimum, it is particularly important to explain the following:

- The risks of fraud, manipulation, theft, and loss associated with digital asset securities.
- A description of the risks relating to valuation, price volatility, and liquidity associated with digital asset securities.
- Procedures to ensure best execution.

At the time a specific investment is recommended, additional disclosure should be provided to the client. Assuming all applicable suitability procedures are satisfied, disclosure of the material facts and risks

[74] The Co-Authors respectfully recommend that the SEC require details concerning the following topics remain highly confidential in order to maximize security.

associated with digital based assets should be explained at a granular level with particular emphasis on any conflicts and risks present at the time of the recommendation. This should include disclosure related to, but not limited to:

- volatility of the recommended product;
- liquidity;
- the risk of fraud or manipulation in light of the liquidity and number of exchanges accessible; and
- any additional material information necessary for a reasonable person to make an informed investment decision.

Example language may read:

> Although you can always exit a position, you may find it difficult or impossible to liquidate a position quickly at what you consider a reasonable price. Events such as recent news, market conditions, or unusual trading activity can affect your ability to sell a position or cause you to incur a loss.

D. Current Industry Disclosure Policies

As noted above, disclosure protocols related to digital asset securities are largely inconsistent from firm to firm. Specifically, the timing and frequency by disclosure must be delivered is unpredictable. Many firms make best efforts to include information related to the risk and complexity of these investments, however some firms make disclosure documents difficult to find. SEC-directed guidance on timing and frequency of disclosure delivery would make great strides towards harmonization across firms. Guidance of this nature is consistent with previous actions of The Commission, including insurance products, equities, mutual funds, and many other examples.

The Co-Authors propose the SEC require BDs present adequate disclosure when the option of trading in digital assets is first presented to a client, and again if the client takes an action. This ensures a reasonable investor would have access to the information necessary to make an informed decision. This problem could potentially be dealt with by a new Commission rule establishing that

1) brokers should provide reasonable measures for requesting applicable disclosures;
2) brokers should take reasonable steps provide disclosures to all who ask for them; and
3) in the event an online or mobile platform is utilized, reasonable measures should be taken to alert the investor at the time position is taken or liquidated.

Whether or not the investor decides to avail themselves of that information remains a choice, but in the instant case the investor need not hunt for it. This method provides a reasonable measure of security for the firm in fulfilling existing regulatory obligations and helps to inform an ever-increasing population of investors seeking out digital asset securities.

V. CONCLUSION

The Co-Authors reiterate their hope that the SEC views the suggestions above as achievable, reasonable, and effective. The digital asset industry has quickly propelled itself onto the main stage of institutional investing. The SEC has exemplified its foresight and diligence through its current pursuit to regulate digital assets. We hope the SEC continues its progressive stance during its review of the above proposals. Throughout the writing process, the Co-Authors discussed, among other things, the industry best practices for generating and securing private keys, the industry best practices that affect custody of digital assets, the processes, software, and hardware systems that secure private keys, and the accepted model practices and language with respect to risk disclosure. The Co-Authors hope our comment will assist the SEC as it strives to effectively regulate the custody and use of digital assets. Thank you for the opportunity to comment on this important issue.