GUEST COLUMN

How the Characteristics of Digital Assets Affect Compliance with the Custody Rule

By Michael S. Didiuk, Joshua L. Boehm and Michael S. Selig, Perkins Coie LLP*

Posted to IAA Today on July 27, 2020

When a mysterious individual, or group, under the moniker of Satoshi Nakamoto published a white paper describing an "electronic peer-to-peer cash system" called Bitcoin to an obscure cryptography mailing list in 2008, the last thing on his, her, or their mind was likely the U.S. federal securities laws, much less a rule under the Investment Advisers Act of 1940 ("Advisers Act"), known as the "Custody Rule." But with the popularity of Bitcoin and other digital assets, registered investment advisers must now consider application of the Custody Rule, among other federal securities laws and regulations, to investments in these new assets on behalf of clients.

Today, there are thousands of different types of digital assets, from cryptocurrencies like Bitcoin to non-fungible tokens like CryptoKitties. These digital assets are a form of virtual property that exists as data in a ledger safeguarded by a peer-to-peer virtual network of connected computers, known as a blockchain. Subject to local laws, anyone can establish a "digital wallet" address on a public blockchain and hold a variety of digital assets. Each digital wallet is associated with an alphanumeric code, known as a private key, that the wallet holder must keep secret like a password. Possession of this private key enables one to access and transfer the digital assets maintained in the digital wallet.

Custody of digital assets, both fungible and non-fungible, is a function of possession of the private key associated with the digital wallet that the digital assets are assigned to on the relevant blockchain. If a third party can obtain the private key associated with a digital wallet, the third party will be able to take possession of the digital assets in that account because the private key, like a password, grants access to the contents of the digital wallet. In the traditional securities context, by comparison, custody is generally a function of possessing a physical certificate or notation in a centralized computer database.

Michael S. Didiuk, Perkins Coie LLP

Joshua L. Boehm, Perkins Coie LLP

Michael S. Selig, Perkins Coie LLP

"Registered investment advisers that provide advice to clients about digital assets … face novel questions in determining how to custody such digital assets."

Registered investment advisers that provide advice to clients about digital assets therefore face novel questions in determining how to custody such digital assets. In particular, they must consider whether these assets are subject to the Custody Rule and, if so, how to maintain custody of this new type of asset in compliance with the Custody Rule. In March 2019, the SEC's Division of Investment Management circulated a request for public input on, among other things, "whether and how characteristics particular to digital assets affect compliance with the Custody Rule."

This article discusses how the characteristics of digital assets present important considerations for investment advisers when complying with the Custody Rule, particularly with the requirement that specified assets be maintained with a "qualified custodian." As this becomes more mainstream, the SEC will need to work through policy and practical considerations to address these issues.

I. Custody Considerations

Compliance with the Custody Rule presents several important considerations for investment advisers, including:

Continued on page 18

Continued from page 17

A. Classification of Digital Assets

The Custody Rule requires registered investment advisers to maintain client "funds" and "securities" with a "qualified custodian," such as a broker-dealer, futures commission merchant, or bank, which includes a trust company meeting certain standards with proper regulatory oversight. This requirement minimizes the risk of an investment adviser misappropriating "investable assets."

While the term "security" is defined in the Advisers Act and has been interpreted by federal courts in numerous decisions, the term "funds" is not defined in the Advisers Act or the Custody Rule. To date, neither the SEC nor federal courts have addressed whether, or to what extent, virtual currencies may be "funds" under the Custody Rule. The SEC has historically regarded cash and bank deposits as funds, but left the door open for classification of other assets as such. Some digital assets, in particular dollar-backed "stablecoins," are akin to cash or bank deposits because they similarly function as a liquid medium of exchange, store of value and unit of account. Until the SEC provides clarity, investment advisers might find that the prudent and cautious course is to prophylactically treat, at a minimum, dollar-backed stablecoins, and, potentially, other virtual currencies as funds for purposes of the Custody Rule.

The SEC's Strategic Hub for Innovation and Financial Technology has indicated that the Supreme Court's test for whether an instrument is an "investment contract," as set forth in the 1946 case *SEC v. Howey*, will generally control when evaluating the status of a given digital asset as a "security." The "*Howey* test" calls for an assessment of the facts and circumstances unique to each digital asset, making it difficult to determine whether a given digital asset is a security absent a judicial opinion or an SEC staff no-action letter. Other parts of the definition of security, such as "notes" or "transferable shares," can also apply to digital assets that are not investment contracts. To date, there are very few digital assets that have been intentionally issued as securities.

"[W]ith the popularity of Bitcoin and other digital assets, registered investment advisers must now consider application of the Custody Rule, among other federal securities laws and regulations, to investments in these new assets on behalf of clients."

If assets are neither funds nor securities, the technical provisions of the Custody Rule do not apply to them, but the adviser still owes a fiduciary duty to its clients to take reasonable steps to safeguard such client assets. Nevertheless, investment advisers typically maintain their digital assets with a qualified custodian as a prudent means of safekeeping, or because sophisticated investors have come to expect this as a best practice, or as a prophylactic matter in case the assets are deemed securities.

B. Storage and Security of Digital Assets

A cyberattack could result in the theft of private keys, and thereby customers' digital assets. Investment advisers must consider new technological and practical considerations relating to the storage and security of digital assets to mitigate against this risk. Many traditional custodians, including banks and broker-dealers, are not familiar with digital assets and the best practices for their safekeeping. Although the Office of the Comptroller of the Currency clarified in July 2020 that national banks are permitted to custody digital assets, the most popular digital asset custodians are newly-chartered state trust companies. Many of these trust companies are chartered in New York and South Dakota, where regulators have established frameworks for chartering and supervising digital asset trust companies, beginning with New York in 2015. These digital asset custodians offer security features such as cold storage and multi-signature digital wallets that are not part of a typical broker-dealer's existing custodial processes.

1. Hot vs. Cold Storage

As a technological matter, digital asset custody can be evaluated along a spectrum, with so-called "cold" storage at one end and "hot" storage at the other. Cold storage means that the private key information associated with a digital wallet is kept offline. This can be the most secure way to maintain digital assets because the private key information is much less susceptible to remote theft or misappropriation since it is not on a computer connected to the Internet. However, digital assets held in cold storage remain susceptible to internal risks (*e.g.,* theft by custodial employees; physical destruction of the holding place) especially if the custodian has an insufficient control framework. Cold storage can also require lengthy waiting periods for withdrawals (*e.g.,* 24 hours' notice) since digital asset custodians typically need to retrieve private keys through a secure, manual process. Accordingly, cold storage is typically most appropriate for digital assets that are not transacted frequently.

Hot storage means that the private key information associated with a given digital wallet is maintained on a computer that is connected to the Internet. Maintaining private key information online, even in an encrypted form, can be the least secure way to custody digital assets because cyber criminals may be able to find a way to gain access to this data via the Internet. In many cases

Continued on page 19

Continued from page 18

where a digital asset exchange or custodian suffered a loss of customer assets, the digital assets were held in a hot storage arrangement that was hacked by an external attacker. Nonetheless, for some investors (*e.g.,* those with active trading strategies), the ability to transact digital assets instantaneously can justify the increased operational risks of hot storage.

As a practical and prudential matter, investment advisers might determine to store the greatest possible amount of their assets in cold storage, while keeping the minimum needed amount of such assets in hot storage to facilitate timely withdrawals (based on typical withdrawal volume and frequency).

2. Multi-Signature Digital Wallets

Just like a nuclear missile silo that requires multiple keys to be turned simultaneously by more than one person, it is possible to establish a digital wallet that requires multiple private keys to initiate a transaction. Multi-signature technology effectively breaks up a private key into multiple private keys so that all or a quorum of keyholders must agree to initiate a transaction. Multi-signature digital wallets offer enhanced security against cyberattacks and rogue keyholders. Multi-signature arrangements exist in a variety of forms, and can be programmed with certain criteria (transaction threshold limits for example). Leading custodians often use some form of multi-signature technology in hot and cold storage custodial arrangements, as discussed above.

Advances are also being made with secure multi-party computation ("MPC"), which is a form of technology that achieves a similar result to multi-signature technology (the signing of a transaction by multiple parties) but does not require a custodian to maintain individual private keys. If successfully implemented, MPC-based custodial arrangements could enhance customer digital asset security by removing private key misappropriation as a potential risk vector.

"[I]nvestment advisers typically maintain their digital assets with a qualified custodian as a prudent means of safekeeping, or because sophisticated investors have come to expect this as a best practice, or as a prophylactic matter in case the assets are deemed securities."

3. Segregation and Settlement Mechanics

Digital asset custodians employ varying operational practices in their segregation and settlement of digital assets.

Some custodians hold customer assets in digital wallets that contain only the assets of a particular customer, which legally and operationally segregates such assets from the digital assets of other customers. This practice typically occurs only in cold storage arrangements. Other custodians combine the digital assets of multiple customers within an omnibus digital wallet, but legally segregate them by keeping track of customer ownership in a separate ledger. This practice is especially common in hot storage arrangements, but is increasingly used for cold storage arrangements as well. Historically, full operational segregation has been viewed as a best practice from an asset security perspective, since the compromise of one customer's digital wallet would not necessarily affect the assets of another customer. However, with robust internal controls, omnibus storage of digital assets (in both cold and hot environments) can be provided in a manner that mitigates risk of loss to a commensurate degree.

Whether customer digital assets are held in an operationally segregated or omnibus manner also has implications for reporting and auditing. Although digital asset custodians currently follow traditional account statement practices under the Custody Rule, blockchain technology could theoretically enable custodians to provide more frequent (potentially even real-time) visibility to customer digital assets under custody where assets are stored in individual digital asset wallets. By contrast, omnibus storage arrangements likely would not permit customers to independently verify their storage of digital assets with the custodian using blockchain technology, given that their assets would be pooled with other customers' assets in a single digital wallet. While robust auditing is essential to all custodial arrangements, it is especially important to omnibus digital asset arrangements since a customer's ownership of digital assets is not independently verifiable at a single blockchain address. The Custody Rule's provisions on maintaining separate accounts for client funds and securities would also be relevant.

C. Capitalization, Insurance and Audit

Regulators of digital asset custodians typically impose capitalization standards that, among other purposes, require custodians to have enough capital to absorb unexpected losses, including losses of customer assets. Custodian capitalization requirements have been viewed as an important protection against customer digital asset losses, in part, because traditional forms of depositor and investor insurance (*i.e.,* FDIC and SIPC coverage) are generally not available to cover such losses.

In determining appropriate capitalization requirements for digital asset custodians, regulators have taken differing approaches. Some have applied a fixed net worth requirement. Others require the greater of (a) a floor net worth amount or (b) an amount that, according to a formula, increases with the custodian's assets under custody (and increases more rapidly if assets are held in hot rather than cold storage). Many digital

Continued on page 20

Continued from page 19

asset custodians are non-depository institutions, and generally treat customer assets under custody as remaining the property of the customer. As is typical of traditional non-depository custodians, even well-capitalized digital asset custodians have capital levels that are a fraction of total customer assets under custody. For that reason, while a digital asset custodian's capitalization is an important signal of its financial wherewithal, it is not full protection against the possibility of customer asset loss.

Custodian and customer demand for additional protection against risk of digital asset loss has led to private insurance options, as well. A number of the leading digital asset custodians offer third-party insurance coverage as an element of their service to customers. The costs of insurance coverage vary considerably between digital assets stored in hot and cold storage for the reasons mentioned above. Costs may also vary based on other factors, such as the jurisdiction, operational processes and security protections of the custodian, as well as the third-party insurance provider. There are also other forms of insurance coverage of relevance to custodians' security procedures that are applicable to the risks of holding a digital wallet's private key, such as kidnap and ransom insurance.

With the increasing visibility in digital assets including among institutional customers, some digital asset custodians have obtained SOC ("System and Organization Controls") reports from independent auditors to demonstrate that their controls meet the standards and requirements expected by institutional customers. As most digital asset custodians provide trust services, the categories and criteria applicable to trust services contained within a SOC 2 report (such as security, availability, processing integrity, confidentiality and privacy) may be reassuring to prospective customers.

"The unique characteristics of digital assets present important practical and technological issues for investment advisers, who are likely to look to the SEC for guidance and clarity on the application of the Custody Rule and related securities laws to this novel technology."

II. Policy Recommendations

While some of the new digital asset custodians that have emerged to serve the needs of investors in the asset class are "qualified custodians" for purposes of the Custody Rule, these custodians vary in their approaches to maintaining custody of digital assets on behalf of their customers. Many of the risks inherent in maintaining custody of digital assets may be mitigated by requiring investment advisers to use only qualified custodians that comply with certain principles-based standards for safekeeping digital assets. Because blockchain technology is constantly developing and improving, the best-in-class security features of today may be obsolete tomorrow. The Division of Investment Management might therefore consider certain technology-agnostic guidelines for digital asset safekeeping that will keep up with the pace of innovation.

The Division might wish to develop a set of general principles that define acceptable cold storage, hot storage and hybrid practices, including with respect to the maintenance of private keys, that all qualified custodians must satisfy. This would provide investment advisers with more confidence that their clients' digital assets are safe while not giving a roadmap for wrongdoers to attack specific required methods of safekeeping. Alternatively, the SEC's Office of Compliance Inspections and Examinations might consider incorporating this guidance into its Cybersecurity and Resiliency Operations report.

Similarly, the Division might consider voluntary audit and cybersecurity standards for digital asset custodians. Finally, the SEC might consider establishing minimum standards for the use of blockchains and distributed ledger technology more broadly for purposes of evidencing ownership of securities. This technology can be used to establish an immutable record of ownership of securities in a transparent, tamper-resistant and privacy-preserving way.

****

As blockchains become more mainstream and new use cases for blockchain technology continue to emerge, the digital asset market is likely to become more relevant. The unique characteristics of digital assets present important practical and technological issues for investment advisers, who are likely to look to the SEC for guidance and clarity on the application of the Custody Rule and related securities laws to this novel technology. The considerations and recommendations in this article may assist investment advisers, custodians and other industry participants regarding any guidance or proposed rules regarding digital asset custody.

**Michael Didiuk* is a partner, Joshua Boehm is a counsel, and Michael Selig is an associate at Perkins Coie LLP.* *The authors thank their colleagues Jesse Kanach, Dana Syracuse, Andrew Cross and Conor O'Hanlon for their contributions.* *This article is for general information purposes and is not intended to be and should not be taken as legal or other advice.*