2.0 Hours CLE credit in Enhanced Ethics for Delaware and Pennsylvania Attorneys

MATERIALS PACKET

10:00 a.m. – 11:00 a.m.

Blockchain and Banking

Moderator:

Greg Strong, Esquire

DLx Law LLP

Panelists:

Angela Angelovska-Wilson, Esquire

Co-Founder, DLx Law LLP

Robert A. Glen, Delaware State Bank Commissioner

Office of the State Bank Commissioner

State of Delaware

Chris Land, Esquire, General Counsel

The Office of U.S. Senator Cynthia Lummis

Office of the Comptroller of the Currency

Washington, DC 20219

Interpretive Letter #1170
July 2020

July 22, 2020

Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers

Dear **[ ]**,

I. Introduction and Summary Conclusion

This letter responds to your request regarding the authority of a national bank to provide cryptocurrency custody services for customers. For the reasons discussed below, we conclude a national bank may provide these cryptocurrency custody services on behalf of customers, including by holding the unique cryptographic keys associated with cryptocurrency.[1] This letter also reaffirms the OCC's position that national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law.[2]

II. Background

Cryptocurrencies—also known as "digital currencies" or "virtual currencies"—are designed to work as a medium of exchange and are created and stored electronically.[3] Depending on the type of cryptocurrency, it may have characteristics of either fiat money or money backed by some underlying asset(s) or claim(s). Fiat money refers to instruments that do not have intrinsic value but that individuals and institutions are willing to use for purposes of purchase and investment because they are issued by a government. Government-issued currencies, including the U.S. dollar following abandonment of the gold standard, are traditional fiat money. Some types of cryptocurrencies may have similar characteristics as fiat money

[1] As discussed further below, this conclusion also applies to Federal savings associations (FSAs).

[2] Banks determine the levels and types of risks that they will assume. Banks that operate in compliance with applicable law, properly manage customer relationships and effectively mitigate risks by implementing controls commensurate with those risks are neither prohibited nor discouraged from providing banking services. As the federal banking agencies have previously stated, banks are encouraged to manage customer relationships and mitigate risks based on customer relationships rather than declining to provide banking services to entire categories of customers. See Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision, at 2 (July 22, 2019), available at https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf.

[3] The term "cryptocurrency" as used in this letter also encompasses digital assets that are not broadly used as currencies.

because they are not backed by any other assets. Other types of money may be backed by assets (such as a commodity). The U.S. dollar was a type of asset-backed money prior to abandonment of the gold standard. Some types of cryptocurrencies may have similar characteristics to this type of money. For example, stablecoin is a type of cryptocurrency that is backed by an asset, such as a fiat currency or a commodity.

While cryptocurrency shares certain characteristics of these traditional types of money, the exchange mechanism is novel. The exchange mechanism for most cryptocurrencies is based on two separate underlying technologies. The first is advanced cryptography, which is used to protect information related to the cryptocurrency. Cryptography allows the creation of digital code that generally cannot be altered without the permission of the creator.

The second type of technology underlying cryptocurrencies' exchange mechanism is known as "distributed ledger technology," and consists of a shared electronic database where copies of the same information are stored on multiple computers. This shared database functions as both a mechanism to prevent tampering and as a way to add new information to the database. Information will not be added to the distributed ledger until consensus is reached that the information is valid. Furthermore, attempts to change the information on one computer will not impact the information on the other computers. Some distributed ledgers are known as "blockchains" because the transactions stored on the ledger are sequentially grouped together in blocks, thus creating a chronological record of all transactions to that point.[4]

Cryptocurrencies do not exist in any physical form. They exist only on the distributed ledger on which they are recorded. A particular unit of cryptocurrency is assigned to a party through the use of a set of unique cryptographic keys. Those keys allow that party to transfer the cryptocurrency to another party.[5] If those keys are lost, a party will generally be unable to access its cryptocurrency. Furthermore, if a third party gains access to those keys, that third party can use the keys to transfer the cryptocurrency to themselves.

The first widely-adopted cryptocurrency, Bitcoin, was introduced in 2008.[6] Since the creation of Bitcoin, hundreds of additional virtual currencies have been created, all of which have different characteristics and potential uses. Some cryptocurrencies may have characteristics of currency or cash, including as a medium of exchange, but with a new exchange mechanism

---

[4] See, e.g., How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), https://bitcoin.org/en/how-it-works (describing Bitcoin's shared public ledger as a blockchain).

[5] See, e.g., FAQs, How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), https://bitcoin.org/en/faq#how-does-bitcoin-work (from a user perspective, Bitcoin is nothing more than an application that provides a digital wallet); How does Bitcoin work?, bitcoin.org (last visited July 20, 2020), https://bitcoin.org/en/how-it-works (describing use of keys to sign transactions); How do Bitcoin Transactions Work?, Coindesk.com (last visited July 20, 2020), https://www.coindesk.com/information/how-do-bitcoin-transactions-work/.

[6] See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, available at https://bitcoin.org/bitcoin.pdf (Bitcoin Whitepaper).

(i.e., electronic transfer without an intermediary). This letter expresses no opinion on whether cryptocurrencies may be exchange for purposes of 12 U.S.C. 24(Seventh).

Cryptocurrencies have been used for a variety of payment and investment activities. Bitcoin remains the most widely used and valuable cryptocurrency, with a current market capitalization approximately $170 billion.[7] Bitcoin is now accepted as payment by thousands of merchants worldwide; customers may even purchase Bitcoin for cash at various retail locations.[8] Contracts on Bitcoin futures have been established and options on Bitcoin futures are now trading.[9] The SEC recently approved a Bitcoin futures fund.[10] Although transactions in cryptocurrencies can occur directly between parties via decentralized, peer-to-peer cryptocurrency transactions, many cryptocurrencies may also be traded through centralized, online cryptocurrency exchanges where parties trade one cryptocurrency for another or trade for fiat currencies such as the U.S. dollar through a financial intermediary.[11] Some centralized cryptocurrency exchanges have obtained state banking licenses as trust banks.[12]

---

[7] See Top 100 Cryptocurrencies by Market Capitalization, Coinmarketcap.com, (last visited July 20, 2020), https://coinmarketcap.com/.

[8] See Maddie Shepherd, How Many Businesses Accept Bitcoin? (last visited July 20, 2020), https://www.fundera.com/resources/how-many-businesses-accept-bitcoin (reporting that nearly 15,174 merchants worldwide accept bitcoin as of December 31, 2019). See also Turner Wright, LibertyX Allows BTC Purchases in Cash at 7-Eleven, CVS, and Rite Aid, Cointelegraph.com (June 23, 2020), https://cointelegraph.com/news/libertyx-allows-btc-purchases-in-cash-at-7-eleven-cvs-and-rite-aid.

[9] See CME Group, Bitcoin futures and options on futures (last visited July 20, 2020), https://www.cmegroup.com/trading/bitcoin-futures.html.

[10] In December of 2019, the SEC approved an investment fund that invests in bitcoin futures contracts. See Kevin Helms, SEC Approves Bitcoin Futures Fund, Bitcoin.com (Dec. 7, 2019), https://news.bitcoin.com/sec-approves-bitcoin-futures-fund/.

[11] See Top Cryptocurrency Spot Exchanges, Coinmarketcap.com (last visited July 20, 2020), https://coinmarketcap.com/rankings/exchanges/ (listing over 300 separate cryptocurrency exchanges). "Decentralized" in this context refers to the lack of a third-party intermediary; instead, buyers and sellers exchange cryptocurrency directly. "Centralized" refers to a third-party intermediary (such as a banking organization) that facilitates trades between buyers and sellers. See Dylan Dedi, Centralized Cryptocurrency Exchanges, Explained, Cointelegraph.com (March 10, 2018), https://cointelegraph.com/explained/centralized-cryptocurrency-exchanges-explained.

[12] See, e.g., New York Department of Financial Services, Financial Services Superintended Linda A. Lacewell Announces Grant of DFS Trust Charter to Enable Fidelity to Engage in New York's Growing Virtual Currency Marketplace (Nov. 19, 2019), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1911191; New York Department of Financial Services, NYDFS Grants Charter to "Gemini" Bitcoin Exchange founded by Cameron and Tyler Winklevoss (Oct. 5, 2015), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1510051.

As of June 2020, a majority of states have adopted laws and regulations pertaining to cryptocurrencies.[13] Recent survey evidence suggests that almost 40 million Americans own cryptocurrencies.[14] Institutional investors also have invested in cryptocurrencies.[15]

III. The Proposed Activities

The bank has proposed to offer cryptocurrency custody services to its customers as part of its existing custody business. We understand that there is a growing demand for safe places, such as banks,[16] to hold unique cryptographic keys associated with cryptocurrencies on behalf of customers and to provide related custody services.[17] These services are in demand for several reasons. First, because the underlying keys to a unit of cryptocurrency are essentially irreplaceable if lost, owners may lose access to their cryptocurrencies as a result of misplacing their keys, resulting in significant losses of value.[18] Second, banks may offer more secure

---

[13] Numerous states have adopted or proposed legislation that relates to cryptocurrency, usually exempting digital currencies from money transmitter licensing requirements and securities laws or recognizing that records secured through blockchain technology have the same legal status as written records. See Dale Werts, Blockchain & Cryptocurrency: State Law Roundup 2019 (July 18, 2019), https://www.jdsupra.com/legalnews/blockchain-cryptocurrency-state-law-59816/.

[14] See Helen Partz, 11% of Americans Own Bitcoin, Major Awareness Increased Since 2017, Yahoo! Finance (Apr. 30, 2019), https://finance.yahoo.com/news/11-americans-own-bitcoin-major-164400483.html.

[15] See, e.g., Olga Kharif, Fidelity Says a Third of Big Institutions Own Crypto Assets (June 9, 2020), BNN Bloomberg, https://www.bnnbloomberg.ca/fidelity-says-a-third-of-big-institutions-own-crypto-assets-1.1447708 (reporting that, according to a survey by Fidelity Investments, 36 percent of institutional investors in the U.S. and Europe report holding crypto assets); Luke W. Vrotsos and Cindy H. Zhang, Harvard Invests Millions in New Cryptocurrency, The Harvard Crimson, April 12, 2019, available at https://www.thecrimson.com/article/2019/4/12/hmc-crypto-investment/; Jonathan Watkins, The Institutional Crypto Backers: How Endowments are Allocating to Cryptocurrency Investments (Apr. 2019), available at https://www.globalcustodian.com/wp-content/uploads/2019/04/The-institutional-crypto-backers-How-endowments-are-allocating-to-cryptocurrency-investments.pdf.

[16] States are beginning to recognize the growing demand for safe locations to hold cryptocurrencies. At least one state has passed legislation and promulgated regulations allowing state-chartered banks to opt-in to providing custody services for digital assets. See, e.g., Wyo. Admin. Code 021.0002.19. These regulations were promulgated pursuant to Wyoming Statute ("W.S.") 34-29-104, Digital asset custodial services. Under W.S. 34-29-104, banks that elect to provide digital asset custodial services must comply with all provision of W.S. 34-29-104 and the new regulations (known as the enhanced digital custody opt-in regime). The states of Hawaii and Rhode Island have also recently proposed legislation on digital asset custody. See Hawaii SB2594 (introduced Jan. 17, 2020), available at https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=2594&year=2020; Rhode Island HB7989, available at https://legiscan.com/RI/bill/H7989/2020 (introduced Mar. 11, 2020).

[17] See, e.g., Melanie Kramer, Will Cryptocurrency Custody Services Fuel Institutional Demand?, Bitcoinist.com (July 22, 2018), https://bitcoinist.com/crypto-custody-services-fuel-institutional-demand/ (describing how institutional investors may feel more comfortable maintaining cryptocurrencies in the custody of banks than exchanges).

[18] One empirical analysis of the bitcoin blockchain calculated that roughly 20% of all currently outstanding bitcoin have been lost. See Jeff John Roberts and Nicolas Rapp, Nearly 4 Million Bitcoins Lost Forever, New Study Says, Fortune (Nov. 25, 2017), available at http://fortune.com/2017/11/25/lost-bitcoins/; see also, Alison Sider and Stephanie Young, Good News! You Are a Bitcoin Millionaire. Bad News! You Forgot Your Password, The Wall Street Journal (Dec. 19, 2017), available at https://www.wsj.com/articles/good-news-you-are-a-bitcoin-millionaire-

storage services compared to existing options.[19] Third, some investment advisers may wish to manage cryptocurrencies on behalf of customers and may wish to utilize national banks as custodians for the managed assets.

Providing custody for cryptocurrencies would differ in several respects from other custody activities. Cryptocurrencies are generally held in "wallets," which are programs that store the cryptographic keys associated with a particular unit of digital currency. Because digital currencies exist only on the blockchain or distributed ledger on which they are stored, there is no physical possession of the instrument. Instead, the right to a particular unit of digital currency is transferred from party to party by the use of unique cryptographic keys. Therefore, a bank "holding" digital currencies on behalf of a customer is actually taking possession of the cryptographic access keys to that unit of cryptocurrency. Those keys are held in a "wallet" that protects the keys from discovery by a third party.[20] Keys can be stored in "hot" wallets or "cold" wallets. Hot wallets are connected to the internet, which makes them convenient to access but more susceptible to hacking. Cold wallets are physical devices that are completely offline (for example, paper or hardware wallets that can be stored in a physical vault). Currently, cold storage is considered the most secure method of storing cryptographic keys.[21]

The OCC recognizes that, as the financial markets become increasingly technological, there will likely be increasing need for banks and other service providers to leverage new technology and innovative ways to provide traditional services on behalf of customers. By providing such services, banks can continue to fulfill the financial intermediation function they have historically played in providing payment, loan and deposit services. Through intermediated exchanges of payments, banks facilitate the flow of funds within our economy and serve important financial risk management and other financial needs of bank customers.[22]

---

bad-news-you-forgot-your-password-1513701480 (reporting numerous examples of individuals losing access to significant value in bitcoin as a result of lost passwords).

[19] Some cryptocurrency exchanges that store access to cryptocurrency on behalf of customers have proven vulnerable to hacking and theft. See Steven Russolillo and Eun-Young Jeong, Cryptocurrency Exchanges Are Getting Hacked Because It's Easy, The Wall Street Journal (July 16, 2018), available at https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000 (detailing light security and regulatory gaps at some cryptocurrency exchanges).

[20] See, e.g., Aziz, Guide to Cryptocurrency Wallets: Why Do You Need Wallets? (last visited July 20, 2020) https://masterthecrypto.com/guide-to-cryptocurrency-wallets/ (holding cryptocurrency at an exchange means having the exchange host the wallet).

[21] See, e.g., Hot wallet vs cold wallet in cryptocurrency storage, Coin Insider, https://www.coininsider.com/hot-vs-cold-wallets-cryptocurrency/ (last visited July 16, 2020).

[22] See, e.g., OCC Interpretive Letter No. 1110 (Jan. 30, 2009); OCC Interpretive Letter No. 1101 (July 7, 2008); OCC Interpretive Letter No. 1079 (April 19, 2007).

IV. Discussion

National banks have long provided safekeeping and custody services for a wide variety of customer assets, including both physical objects and electronic assets. These functions of national banks are well established and extensively recognized as permissible activities for national banks.[23] The OCC concludes, for the reasons discussed below, that providing cryptocurrency custody services, including holding the unique cryptographic keys associated with cryptocurrency, is a modern form of these traditional bank activities.

Safekeeping services are among the most fundamental and basic services provided by banks.[24] Bank customers traditionally used special deposit and safe deposit boxes for the storage and safekeeping of a variety of physical objects, such as valuable papers, rare coins, and jewelry.[25] As the banking industry entered the digital age, the OCC recognized the permissibility of electronic safekeeping activities. Specifically, the OCC has concluded that a national bank may escrow encryption keys used in connection with digital certificates,[26] finding that the key escrow service is a functional equivalent to physical safekeeping, except it uses electronic technology suitable to the digital nature of the item to be kept safe. The OCC has also concluded that a national bank may provide secure web-based document storage, retrieval and collaboration of documents and files containing personal information or valuable confidential trade or business information because these services are the electronic expression of traditional safekeeping services provided by banks.[27] The OCC codified these interpretive rulings in 12 CFR Part 7.[28]

Traditional bank custodians frequently offer a range of services in addition to simple safekeeping of assets. For example, a custodian providing core domestic custody services for

---

[23] See OCC Conditional Approval 479 (July 27, 2001) (Conditional Approval 479). "Safekeeping" implies the basic service of a bank holding on to an asset for a customer (e.g., gold or securities). "Custody" is a broader term that may involve all aspects of bank services performed for customers in relation to items they are holding for them (i.e., processing, settlement, fund administration). Historically, banks only offered safekeeping services, which then evolved into banks providing custodial services to their customers. See Comptroller's Handbooks on Custody Services (Jan. 2002) (Custody Handbook).

[24] Colorado Nat. Bank of Denver v. Bedford, 310 U.S. 41, 50 (1940) (finding that providing safe deposit boxes is "such a generally adopted method of safeguarding valuables [that it] must be considered a banking function authorized by Congress" under the National Bank Act). The safekeeping of valuable personal property is a traditional function that banks have performed since the earliest times. "Originally the business of banking consisted only in receiving deposits, such as bullion, plate and the like for safe-keeping until the depositor should see fit to draw it out for use. . . ." Oulton v. German Savings and Loan Soc'y, 84 U.S. 109, 118 (1872); see also Bank of California v. City of Portland, 157 Ore. 203, 69 P.2d 273 (1937).

[25] See Conditional Approval 479; Comptroller's Handbook on Custody Services (Custody Handbook) (Jan. 2002) at page 15 (jewelry listed as one of the miscellaneous assets that banks hold via on-premises custody).

[26] See OCC Conditional Approval 267 (Jan. 12, 1998) (Conditional Approval 267).

[27] See Conditional Approval 479.

[28] See 12 CFR §§ 7.5002(a)(4) and 7.5005(a).

securities typically settles trades, invests cash balances as directed, collects income, processes corporate actions, prices securities positions, and provides recordkeeping and reporting services.[29] It is well-established that national banks may provide custody services to their customers in either a fiduciary or non-fiduciary capacity. 12 U.S.C. 92a expressly authorizes the OCC to grant fiduciary powers to national banks.[30] National banks may also provide non-fiduciary custody services to their customers.[31] The OCC has determined national banks may act as non-fiduciary custodians pursuant to the business of banking and their incidental powers.[32] OCC guidance has recognized that banks may hold a wide variety of assets as custodians, including assets that are unique and hard to value.[33] These custody activities often include assets that transfer electronically.[34] The OCC generally has not prohibited banks from providing custody services for any particular type of asset, as long as the bank has the capability to hold the asset and the assets are not illegal in the jurisdiction where they will be held.[35]

Providing custody services for cryptocurrency falls within these longstanding authorities to engage in safekeeping and custody activities. As discussed below, this is a permissible form of a traditional banking activity that national banks are authorized to perform via electronic

---

[29] See Custody Handbook at 2.

[30] "The Comptroller of the Currency shall be authorized and empowered to grant by special permit to national banks applying therefor, when not in contravention of State or local law, the right to act as trustee, executor, administrator, registrar of stocks and bonds, guardian of estates, assignee, receiver, or in any other fiduciary capacity in which State banks, trust companies, or other corporations which come into competition with national banks are permitted to act under the laws of the State in which the national bank is located." 12 U.S.C. 92a(a). 12 CFR Part 9 implements 12 U.S.C. 92a. The fiduciary capacities defined under Part 9 are "trustee, executor, administrator, registrar of stocks and bonds, transfer agent, guardian, assignee, receiver, or custodian under a uniform gifts to minors act; investment adviser, if the bank receives a fee for its investment advice; any capacity in which the bank possesses investment discretion on behalf of another; or any other similar capacity that the OCC authorizes pursuant to 12 USC 92a." See 12 CFR 9.2(e).

[31] National banks do not need the trust or fiduciary powers found in sections 92a to offer these custodial services. Thus, no trust powers are necessary in order to conduct these activities. See Conditional Approval 267.

[32] See, e.g., Conditional Approval 267 (agency services such as custody that do not involve fiduciary powers are performed by banks as part of their incidental powers); OCC Interpretive Letter 1078 (April 19, 2007) (authority of national banks to engage in custody activities derives from general business of banking, and from incidental powers language in 12 U.S.C. § 24(Seventh)).

[33] See, generally, Comptroller's Handbook, Unique and Hard-to-Value Assets (August 2012) (providing guidance on bank management of unique assets and listing examples of such assets, including real estate, closely held businesses, mineral interests, loans and notes, life insurance, tangible assets, and collectibles). See also Comptroller's Handbooks on Custody Services (Jan. 2002) (Custody Handbook), Asset Management (Dec. 2000), Asset Management Operations and Controls (Jan. 2011), Retirement Plan Products and Services (Feb. 2014), Conflicts of Interest (Jan. 2015); OCC Bulletin 2013–29, "Third-Party Relationships—Risk Management Guidance" (Oct. 30, 2013).

[34] See Custody Handbook at 19, 70 (describing book-entry securities as securities that transfer electronically and stating that banks should assess their technological readiness to maintain a competitive position).

[35] See Custody Handbook at 7.

means.[36] Providing such services is permissible in both non-fiduciary and fiduciary capacities. A bank that provides custody for cryptocurrency in a non-fiduciary capacity would essentially provide safekeeping for the cryptographic key that allows for control and transfer of the customer's cryptocurrency. In most, if not all, circumstances, providing custody for cryptocurrency will not entail any physical possession of the cryptocurrency. Rather, a bank "holding" digital currencies on behalf of a customer is actually taking possession of the cryptographic access keys to that unit of cryptocurrency.[37] As described above, the OCC has found that the authority to provide safekeeping services extends to digital activities and, specifically, that national banks may escrow encryption keys used in connection with digital certificates because a key escrow service is a functional equivalent to physical safekeeping. Holding the cryptographic access key to a unit of cryptocurrency is an electronic corollary of these traditional safekeeping activities. The OCC's regulations in Subpart E of Part 7 explicitly authorize national banks to perform, provide or deliver through electronic means and facilities any activities that they are otherwise authorized to perform.[38] Because national banks are authorized to perform safekeeping and custody services for physical assets, national banks are likewise permitted to provide those same services via electronic means (i.e., custody of cryptocurrency).[39]

---

[36] 12 CFR 7.5002(a) provides that a national bank may perform, provide, or deliver through electronic means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver. This regulatory provision is based on the longstanding "transparency doctrine," under which the OCC looks through the means by which a product is delivered and focuses instead on the authority of the national bank to offer the underlying product or service. See 67 FR 34992, 34996 (May 17, 2002). See also OCC Conditional Approval 369 (Feb. 25, 2000) (national bank may host a virtual mall consisting of a web page with links to third-party merchants arranged according to product or service offered); OCC Conditional Approval 304 (Mar. 5, 1999) (electronic bill presentment is part of the business of banking); Conditional Approval 267 (a national bank may store electronic encryption keys as an expression of the established safekeeping function of banks); OCC Conditional Approval 220 (Dec. 2, 1996) (the creation, sale, and redemption of electronic stored value in exchange for dollars is part of the business of banking because it is the electronic equivalent of issuing circulating notes or other paper-based payment devices like travelers checks).

[37] Banks may offer different methods of providing cryptocurrency custody services, depending on their expertise, risk appetite, and business models. Some banks may offer to store copies of their customers' private keys while permitting the customer to retain their own copy. Such services may be more akin to traditional safekeeping and would permit the customer to retain direct control over their own cryptocurrencies. Other banks may permit customers to transfer their cryptocurrencies directly to control of the bank, thereby generating new private keys which would be held by the institution on behalf of the customer. Such services may be more akin to traditional custody services, but as with traditional custody, would not permit the customer to maintain direct control of the cryptocurrency. Banks may also offer other custody models that may be appropriate. Banks acting as fiduciaries for cryptocurrency should consider how to ensure their custody models comply with requirements of 12 CFR 9.13 and 12 CFR 150.230-250.

[38] See 12 CFR 7.5002(a).

[39] The services national banks may provide in relation to the cryptocurrency they are custodying may include services such as facilitating the customer's cryptocurrency and fiat currency exchange transactions, transaction settlement, trade execution, recording keeping, valuation, tax services, reporting, or other appropriate services. A bank acting as custodian may engage a sub-custodian for cryptocurrency it holds on behalf of customers and should develop processes to ensure that the sub-custodian's operations have proper internal controls to protect the customer's cryptocurrency. See, e.g., Custody Handbook at 15-16. As set forth below, banks should develop and implement new activities in accordance with OCC guidance.

To the extent that a national bank with trust powers conducts cryptocurrency custody activities in a fiduciary capacity, such activities would be permissible if conducted in compliance with 12 CFR Part 9, applicable state law, and any other applicable law, such as the instrument that created the fiduciary relationship. A national bank holding cryptocurrencies in a fiduciary capacity—such as a trustee, an executor of a will, an administrator of an estate, a receiver, or as an investment advisor—would have the authority to manage them in the same way banks can manage other assets they hold as fiduciaries.[40]

These conclusions apply equally to federal savings associations (FSAs). Like national banks, FSAs may provide custody services in either a fiduciary or non-fiduciary capacity. The OCC may grant fiduciary powers to an FSA under 12 U.S.C. 1464(n).[41] These fiduciary activities of an FSA must be conducted in compliance with 12 CFR Part 150. In addition, FSAs have authority to act as a non-fiduciary custodian under 12 U.S.C. 1464.[42] Similar to national banks, FSAs are authorized to "use, or participate with others to use, electronic means or facilities to perform any function, or provide any product or service, as part of an authorized activity."[43] Accordingly, for the same reasons described above with respect to national banks, providing custody services for cryptocurrency falls within an FSA's established authority to provide custody services.

A national bank or FSA engaging in new activities should develop and implement those activities consistent with sound risk management practices and align them with the bank's overall business plans and strategies as set forth in OCC guidance.[44] There may be services that banks may provide in connection with cryptocurrencies that are unique to cryptocurrency.[45] As with all other activities performed by national banks and FSAs, a national bank or FSA that provides cryptocurrency custody services must conduct these activities in a safe and sound

---

[40] National banks acting as fiduciaries are usually subject to heightened standards of care under applicable law in comparison to non-fiduciaries. Given the continued evolution of the cryptocurrency sector, banks managing cryptocurrency as fiduciaries should ensure they keep abreast of best practices to ensure they continue to meet these heightened standards.

[41] 12 U.S.C. 1464(n)(1) states, "The Comptroller may grant by special permit to a Federal savings association applying therefor the right to act as trustee, executor, administrator, guardian, or in any other fiduciary capacity in which State banks, trust companies, or other corporations which compete with Federal savings associations are permitted to act under the laws of the State in which the Federal savings association is located."

[42] See Testimony of John Bowman, Chief Counsel, Office of Thrift Supervision, before the Senate Committee on Banking, Housing, and Urban Affairs (June 22, 2004) (HOLA allows thrifts to provide trust and custody services on the same basis as national banks).

[43] See 12 CFR 155.200(a).

[44] See OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" (Oct. 20, 2017).

[45] Custody agreements are an important risk management tool and should clearly establish the custodian's duties and responsibilities. See Custody Handbook at 8. The handling, treatment, and servicing of cryptocurrencies held in custody may raise unique issues that should be addressed in the agreement, such as (for example) the treatment of "forks" or splits in the code underlying the cryptocurrency being held.

manner, including having adequate systems in place to identify, measure, monitor, and control the risks of its custody services. Such systems should include policies, procedures, internal controls, and management information systems governing custody services. Effective internal controls include safeguarding assets under custody, producing reliable financial reports, and complying with laws and regulations. The OCC has previously described that custody activities should include dual controls, segregation of duties and accounting controls.[46] A custodian's accounting records and internal controls should ensure that assets of each custody account are kept separate from the assets of the custodian and maintained under joint control to ensure that that an asset is not lost, destroyed or misappropriated by internal or external parties. Other considerations include settlement of transactions, physical access controls, and security servicing. Such controls may need to be tailored in the context of digital custody. Specialized audit procedures may be necessary to ensure the bank's controls are effective for digital custody activities. For example, procedures for verifying that a bank maintains access controls for a cryptographic key will differ from the procedures used for physical assets. Banks seeking to engage in these activities should also conduct legal analysis to ensure the activities are conducted consistent with all applicable laws.

Consistent with OCC regulations and guidance on custody activities, the risks associated with an individual account should be addressed prior to acceptance.[47] A custodian's acceptance process should provide an adequate review of the customer's needs and wants, as well as the operational needs of the account. During the acceptance process, the custodian should also assess whether the contemplated duties are within its capabilities and are consistent with all applicable law. Understanding the risks of cryptocurrency, the due diligence process should include a review for compliance with anti-money laundering rules. Banks should also have effective information security infrastructure and controls in place to mitigate hacking, theft, and fraud. Banks should also be aware that different cryptocurrencies may have different technical characteristics and may therefore require risk management procedures specific to that particular currency. Different cryptocurrencies may also be subject to different OCC regulations and guidance outside of the custody context, as well as non-OCC regulations.[48] A national bank should consult with OCC supervisors as appropriate prior to engaging in cryptocurrency custody activities. The OCC will review these activities as part of its ordinary supervisory processes.

I trust this is responsive to your inquiry.

---

[46] See Custody Handbook at 6-8. Banks with fiduciary powers that hold assets as fiduciaries are subject to the requirements of 12 CFR Part 9 (for national banks) and Part 150 (for FSAs). These regulations include specific provisions governing the custody of fiduciary assets. See 12 CFR 9.13 (national banks); 12 CFR 150.230-250 (FSAs).

[47] See 12 CFR 9.6(a) (requiring bank fiduciaries to perform a pre-acceptance review before accepting a fiduciary account to determine whether the bank can properly administer it); Custody Handbook at 7-8.

[48] For example, cryptocurrencies that are considered "securities" for purposes of the Federal securities laws may be subject to the OCC's regulations on recordkeeping and confirmation requirements for securities transactions, 12 CFR Part 12, as well as the Federal securities laws administered by the SEC.

Sincerely,

/s/

Jonathan V. Gould
Senior Deputy Comptroller & Chief Counsel

Office of the Comptroller of the Currency

Washington, DC 20219

Interpretive Letter 1174
January 2021

OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities

January 4, 2021

I. Introduction and Summary Conclusion

This letter addresses the legal permissibility of certain payment-related activities that involve the use of new technologies, including the use of independent node verification networks (INVNs or networks) and stablecoins, to engage in and facilitate payment activities. National banks and Federal savings associations (collectively referred to as "banks") may use new technologies, including INVNs and related stablecoins, to perform bank-permissible functions, such as payment activities.

An INVN consists of a shared electronic database where copies of the same information are stored on multiple computers. One common form of an INVN is a distributed ledger.[1] Cryptocurrency transactions are recorded on these ledgers.[2] An INVN's participants, known as nodes, typically validate transactions, store transaction history, and broadcast data to other nodes.[3]

---

[1] See OCC Interpretive Letter 1170 (Jul. 22, 2020) (IL 1170) (describing distributed ledger technology as a shared electronic database where copies of the same information are stored on multiple computers. This shared database functions as both a mechanism to prevent tampering and as a way to add new information to the database. Information will not be added to the distributed ledger until consensus is reached that the information is valid. INVNs represent one of the key technologies that support the novel exchange mechanism underlying cryptocurrency. The other key technology is advanced cryptography.).

[2] The OCC described many features of cryptocurrency in IL 1170. In addition, the OCC recently addressed the permissibility of a national bank holding reserves for stablecoins that are backed by fiat currency on at least a 1:1 basis in situations where there is a hosted wallet. See OCC Interpretive Letter 1172 (Sept. 21, 2020) (IL 1172).

[3] Nodes are generally either full nodes or light nodes. Full nodes verify transactions, maintain consensus between other nodes, and contain a full copy of the ledger's entire history. Light nodes generally consist of wallets that download only the headers of blocks to validate their authenticity and save hard drive space for users by not storing a full copy of the ledger's history. One example of a light node may be a customer's digital wallet on the customer's mobile phone. See, e.g., Josh Evans, Blockchain Nodes: An In-Depth Guide, Nodes.com (Sept. 22, 2020), available at https://nodes.com/; Blockchain: What are nodes and masternodes?, Medium.com (Sept. 22, 2020), available at https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f. A bank may want to serve as a full node on an INVN due to the wider range of capabilities on a full node as compared to a light node, as described above.

A stablecoin is a type of cryptocurrency that is designed to have a stable value as compared with other types of cryptocurrency.[4] Some stablecoins are backed by a fiat currency, such as the U.S. dollar. Fiat-backed stablecoins can typically be exchanged for the underlying fiat currency, where one unit of the stablecoin can be exchanged for one unit of the underlying fiat currency.[5] In this regard, the stablecoin represents a mechanism for storing, transferring, transmitting, and exchanging the underlying fiat currency value, all of which are key to facilitate payment activities. One example of stablecoin as a mechanism to facilitate payment activities is the payment of remittances, which often involve cross-border transfers of money.[6]

Courts and the OCC have long recognized that the primary role of banks is to act as financial intermediaries, facilitating the flow of money and credit among different parts of the economy.[7] "The very object of banking is to aid the operation of the laws of commerce by serving as a channel for carrying money from place to place, as the rise and fall of supply and demand require, and it may be done by rediscounting the bank's paper or by some other form of borrowing."[8] The precedents and history[9] reflect that a bank's role as financial intermediary can

---

[4] See IL 1172. See also *President's Working Grp. on Fin. Markets Releases Statement on Key Regulatory & Supervisory Issues Relevant to Certain Stablecoins*, Treas. SM-1223 (Dec. 23, 2020) (providing an initial assessment of regulatory and supervisory considerations for participants in certain stablecoin arrangements and clarifying expectations for the retail payment application of stablecoins), available at https://home.treasury.gov/news/press-releases/sm1223.

[5] IL 1172 noted that other types of cryptocurrencies described as "stablecoins" may be more complex, backed by commodities, cryptocurrencies, or other assets but with values that are pegged to a fiat currency or managed by algorithm.

[6] Facilitating cross-border payments in stablecoin may improve the speed and cost of transferring funds anywhere in the world; traditional remittances often come with high fees and may take several days to complete. See Hugo Renaudin, Driven by Financial Institutions, Stablecoin Acceptance Turns a Corner, Cointelegraph.com (June 14, 2020), available at https://cointelegraph.com/news/driven-by-financial-institutions-stablecoin-acceptance-turns-a-corner.

[7] See, e.g., OCC Interpretive Letter 1102 (Nov. 2008) (IL 1102); see also NationsBank of North Carolina, N.A. v. Variable Life Annuity Co., 513 U.S. 251, 252 (1995) ("VALIC"); OCC Interpretive Letter 499 (Feb. 12, 1990).

[8] Auten v. U.S. Nat'l Bank of New York, 174 U.S. 125, 143 (1899).

[9] See IL 1102; OCC Interpretive Letter 892 (Sept. 8, 2000). The OCC's view of banks as financial intermediaries comports with the historical role of banks in the economy. See Peter Olson, Regulation's Role in Bank Changes, 18 ECON. POL'Y REV. 13, Federal Reserve Bank of New York (2012), available at https://www.newyorkfed.org/medialibrary/media/research/epr/2012/EPRvol18n2.pdf. As early as the Roman Empire, banks served as intermediaries that mediated between borrowers and lenders, obviating direct contact between them. These banks dealt with the day to day needs of their clients for cash. See Peter Termin, Financial Intermediation in the Early Roman Empire, 64 J. ECON. HIST. 705 (2004). In the 17th century, Dutch merchant banks, such as the Bank of Amsterdam, held deposits and transferred money between accounts; in 18th century England, merchant banks accepted deposits and loaned money to landowners and merchants. Id. Besides deposit taking and lending, another crucial component of financial intermediation is connecting participants in the financial system through the processing of payments. As financial intermediaries, banks have processed payments on behalf of their customers for centuries. For example, in ancient Mesopotamia and Egypt, customers would deposit goods (such as grains) in palaces, temples, and private houses that served as banks. Deposit receipts for these goods were transferable and facilitated transactions and payments between customers. See Chao Gu, Fabrizio Mattesini, Cyril Monnet, & Randall Wright, Banking: A New Monetarist Approach, 80 REV. ECON. STUD. 636 (2013). During the era of Medici banking in the 15th century, Italian bankers facilitated payments by book transfer on the instruction of oral or written orders. See Raymond de Roover, The Rise and Decline of the Medici Bank, Harvard University

take many forms: providing payments transmission services, borrowing from savers and lending to users, and participating in the capital markets. As the recognized intermediaries between other, non-bank participants in the financial markets and the payment systems, banks possess the expertise to facilitate the exchange of payments and securities between, and settle transactions for, parties and to manage their own intermediation position.

Over time, banks' financial intermediation activities have evolved and adapted in response to changing economic conditions and customer needs. Banks have adopted new technologies to carry out bank-permissible activities, including payment activities.[10] The emergence of new technologies to facilitate payments, support financial transactions, and meet the evolving financial needs of the economy has led to a demand for banks to use INVNs to carry out their traditional functions. The changing financial needs of the economy are well-illustrated by the increasing demand in the market for faster and more efficient payments through the use of decentralized technologies, such as INVNs, which validate and record financial transactions, including stablecoin transactions.[11]

Industry participants recognize that using stablecoins to facilitate payments may combine the efficiency and speed of digital currencies with the stability of existing currencies.[12] As discussed below, stablecoins can provide a means of transmitting value denominated in an

---

Press, at 2 (1963). In medieval times, Venetian bankers accepted commodities on deposit that were used to facilitate transactions, and deposit receipts began circulating in place of cash for payments in early 17th century. See Gu, Mattesini, Monnet, & Wright, supra. During the second half of the 17th century, goldsmith bankers in London operated a system of payments through mutual debt acceptance and interbanker clearing. See Stephen Quinn, Goldsmith-Banking: Mutual Acceptance and Interbanker Clearing in Restoration London, 34 EXPLORATIONS IN ECON. HIS. 411 (1997).

[10] For example, and as discussed below, banks have adopted new technologies in their development and operation of electronic funds transfer systems, real-time settlement systems, and stored value systems. See OCC Interpretive Letter 890 (May 15, 2000) (IL 890): OCC Interpretive Letter 854 (Feb. 25, 1999) (IL 854); OCC Interpretive Letter 1157 (Nov. 12, 2017) (IL 1157); OCC Interpretive Letter 1140 (Jan. 13, 2014) (IL 1140); OCC Conditional Approval Letter 220 (Dec. 2, 1996); OCC Conditional Approval Letter 568 (Dec. 31, 2002); OCC Interpretive Letter 737 (Aug. 19, 1996) (IL 737).

[11] See, e.g., Michael del Castillo, Visa Partners with Ethereum Digital-Dollar Startup that Raised $271 Million (Dec. 2. 2020), available at https://www.forbes.com/sites/michaeldelcastillo/2020/12/02/visa-partners-with-ethereum-digital-dollar-startup-that-raised-271-million/?sh=30afc9ac4b1f; Advancing Our Approach to Digital Currency: Visa's Outlook on New Digital Currency Payment Flows (July 22, 2020), available at https://usa.visa.com/visa-everywhere/blog/bdp/2020/07/21/advancing-our-approach-1595302085970.html; Helen Partz, Japanese Banking Giant to Issue Its Own Stablecoin in Late 2020, Cointelegraph.com (July 14, 2020), available at https://cointelegraph.com/news/japanese-banking-giant-mufg-to-issue-its-own-stablecoin-in-h2-2020; Marie Huillet, Japanese Banking Giant Mizuho to Launch Its Yen-Pegged Stablecoin in March (Feb. 21, 2019), available at https://cointelegraph.com/news/japanese-banking-giant-mizuho-to-launch-its-yen-pegged-stablecoin-in-march; Press Release, Wells Fargo & Co., Wells Fargo to Pilot Internal Settlement Service Using Distributed Ledger Technology (Sept. 17, 2019), available at https://newsroom.wf.com/press-release/innovation-and-technology/wells-fargo-pilot-internal-settlement-service-using; Press Release, JP Morgan Chase & Co., J.P. Morgan Creates Digital Coin for Payments (Feb. 14, 2019), available at https://www.jpmorgan.com/global/news/digital-coin-payments. These examples are descriptive only. This letter expresses no view on the permissibility of, or other considerations related to, the activities described therein.

[12] See, e.g., Advancing Our Approach to Digital Currency: Visa's Outlook on New Digital Currency Payment Flows (July 22, 2020).

existing currency using INVN technology. Stablecoins thus provide a means by which participants in the payment system may avail themselves of the potential advantages associated with INVNs. Billions of dollars' worth of stablecoin trade globally, and demand for stablecoin continues to grow.[13]

As discussed below, INVNs and related stablecoins represent new technological means of carrying out bank-permissible payment activities. We therefore conclude that a bank may validate, store, and record payments transactions by serving as a node on an INVN. Likewise, a bank may use INVNs and related stablecoins to carry out other permissible payment activities. A bank must conduct these activities consistent with applicable law and safe and sound banking practices.

As noted in a recent statement of the President's Working Group on Financial Markets, stablecoin arrangements "should have the capability to obtain and verify the identity of all transacting parties, including for those using unhosted wallets."[14] "The stablecoin arrangement should have appropriate systems, controls, and practices in place to manage these risks, including to safeguard reserve assets. Strong reserve management practices include ensuring a 1:1 reserve ratio and adequate financial resources to absorb losses and meet liquidity needs."[15]

II. Discussion

The OCC has recognized that bank-permissible activities may be conducted with new and evolving technologies. Banks may use electronic means or facilities to perform any function, or provide any product or service, as part of an authorized activity.[16] Consistent with this precedent, banks may serve as a node on an INVN and use INVNs and related stablecoins to conduct permissible banking activities, including authorized payment activities.

National banks may engage in payment-related activities as activities within the business of banking.[17] The OCC has found that "[p]ayment system activities (e.g., electronic payments message transmission, electronic payments processing, and payments settlement among members) are clearly within the business of banking and are functionally consistent with the primary role of banks as financial intermediaries."[18] Similarly, FSAs may engage in payment-

---

[13] See, e.g., Zack Voell, Stablecoin Supply Breaks $10B as Traders Demand Dollars Over Bitcoin, Coindesk.com (May 12, 2020) available at https://www.coindesk.com/stablecoin-supply-breaks-10b-as-traders-demand-dollars-over-bitcoin; USD Coin, Coinmarketcap.com (last accessed Jan. 4, 2021), available at https://coinmarketcap.com/currencies/usd-coin.

[14] *President's Working Grp. on Fin. Markets Releases Statement on Key Regulatory & Supervisory Issues Relevant to Certain Stablecoins*, Treas. SM-1223 (Dec. 23, 2020).

[15] Id.

[16] See 12 C.F.R. § 7.5000 et seq.; 12 C.F.R. § 155.200.

[17] See, e.g., IL 1157; IL 1140; OCC Interpretive Letter 1014 (Jan. 10, 2005); OCC Interpretive Letter 929 (Feb. 11, 2002); OCC Interpretive Letter 993 (May 16, 1997) (IL 993); IL 737; OCC Conditional Approval Letter 220.

[18] IL 1140, at 3 n. 12.

related activities and may transfer customer funds "by any mechanism or device," including through electronic means.[19]

The OCC has repeatedly recognized that banks may conduct permissible payment activities using new and evolving technologies. As discussed above, banks may use electronic means or facilities to perform any function, or provide any product or service, as part of an authorized activity.[20] Moreover, the OCC has explicitly permitted national banks to adopt new technologies as a means of executing payment services, consistent with safe and sound banking practices and applicable law. For example, the OCC has concluded that national banks may engage in activities related to electronic funds transfer systems,[21] real-time settlement systems,[22] and stored value systems as part of their permissible payments-related activities.[23] Courts have similarly recognized that banks' authority to engage in payment activities encompasses new and evolving payment technologies.[24] These precedents are consistent with the fundamental principle that national bank powers "must be construed so as to permit new ways of conducting the very old business of banking."[25]

Using INVNs to facilitate payments transactions represents a new means of performing banks' permissible payments functions. At their core, payment activities involve transmitting instructions to transfer a specified sum from one account on a ledger to another account on the same or a different ledger (either at the same bank or at different banks). Established payment systems typically use a trusted, centralized entity to validate payments. Serving as nodes on INVNs is a new means of transmitting payment instructions and validating payments.[26] Rather

---

[19] See 12 C.F.R. § 145.17. As discussed above, FSAs are also permitted to use, or participate with others to use, electronic means or facilities to perform any function, or provide any product or service, as part of an authorized activity. See 12 C.F.R. § 155.200. For example, the Office of Thrift Supervision explicitly permitted FSAs to invest in electronic funds transfer networks. See OTS Op. Ch. Couns. (Dec. 22, 1995); OTS Op. Ch. Couns. (Sept. 15, 1995).

[20] See 12 C.F.R. § 7.5000 et seq; 12 C.F.R. § 155.200.

[21] See, e.g., IL 890; IL 854.

[22] See, e.g., IL 1157; IL 1140.

[23] See, e.g., OCC Conditional Approval Letter 220; OCC Conditional Approval Letter 568; IL 737.

[24] State of Illinois v. Continental Illinois National Bank, 536 F.2d 176, 178 (7th Cir. 1976) ("Any order to pay which is properly executed by a customer, whether it be check, card or electronic device, must be recognized as a routine banking function. . ."); Independent Bankers Association of America v. Smith, 534 F.2d 921, 944 (D.C. Cir. 1976) ("We conclude that Congress envisioned all account withdrawals when it used the shorthand phrase 'checks paid' in section 36(f). If future technological innovations render paper checks totally obsolete, section 36(f) will still include within its broad standard those facilities that permit bank customers to perform the traditional banking function of withdrawing funds from their accounts.").

[25] M & M Leasing Corp. v. Seattle First Nat. Bank, 563 F.2d 1377, 1382 (9th Cir. 1977) cert. denied, 436 U.S. 956 (1978).

[26] While the technology is new, the concept of using distributed ledgers to validate ownership and title is not. See e.g., Oliver Smith, Forbes, Blockchain's Secret 1,000 Year History (Mar 23, 2018), available at https://www.forbes.com/sites/oliversmith/2018/03/23/blockchains-secret-1000-year-history/#4484e42818d2; Kristin Sommer, Phys.org, Team puts an ancient spin on a new digital currency (June 11, 2019), available at https://phys.org/news/2019-06-team-ancient-digital-currency.htmlhttps://phys.org/news/2019-06-team-ancient-

than utilizing a centralized entity, nodes on the shared network validate the transfers. However, the basic functions are the same: transmitting payment instructions and validating payments. Accordingly, the same legal analysis applies, and a bank therefore may serve as a node on an INVN to facilitate payments transactions.

Likewise, a bank may use stablecoins to facilitate payment transactions for customers on an INVN, including by issuing a stablecoin,[27] and by exchanging that stablecoin for fiat currency.[28] In this context, stablecoins function as a mechanism of payment, in the same way that debit cards, checks, and electronically stored value (ESV) systems convey payment instructions. Banks have long used cashiers' checks, travelers' checks, and other bearer instruments as a means of facilitating cashless payments.[29]

Twelve C.F.R. 7.5002(a)(3) expressly provides that a national bank may offer ESV systems. In an ESV system, cash is exchanged for ESV. That ESV is stored on a computer chip within a card. The cardholder makes payments by transferring that ESV to another party who may then redeem the ESV for cash. When codifying the authority of a national bank to offer ESV systems, the OCC noted that the "creation, sale, and redemption of [ESV] in exchange for dollars is part of the business of banking because it is the electronic equivalent of issuing circulating notes or other paper-based payment devices like travelers checks."[30] As the OCC had previously explained in Conditional Approval Letter No. 220, banks may engage in activities related to developing and operating an ESV system because ESV systems are an element of the payment system, and the issuance and redemption of ESV is a new way of conducting one aspect

---

digital-currency.html; Sam Auch, rsmus.com, Blockchain and the Island of Yap, available at https://rsmus.com/what-we-do/services/blockchain-consulting/featured-topics/blockchain-basics/blockchain-and-the-island-of-yap.html.

[27] Certain stablecoins may be securities. A bank's issuance of a stablecoin must comply with all applicable securities laws and regulations. Staff of the Securities and Exchange Commission (SEC) has issued a statement encouraging issuers of stablecoins of the type described in IL 1172 to contact the staff with any questions they may have to help ensure that such stablecoins are structured, marketed, and operated in compliance with the federal securities laws. The statement notes that the staff stands ready to engage with market participants, and, depending on the particular facts and circumstances, to assist them and consider providing, if appropriate, a "no-action" position regarding whether activities with respect to a specific stablecoin may invoke the application of the federal securities laws. See SEC FinHub Staff Statement on OCC Interpretation (Sept. 21, 2020), available at https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation.

[28] The OCC previously addressed the permissibility of a national bank holding reserves for stablecoins that are backed by fiat currency on at least a 1:1 basis. See IL 1172. In addition, the OCC has previously determined that a national bank may facilitate a customer's cryptocurrency and fiat currency exchange transactions. See IL 1170 n. 39.

[29] See, e.g., Arnold Tours, Inc. v. Camp, 472 F.2d 427, 438 (1st Cir. 1972). National banks may cash and process checks; issue, collect, and process cashiers' checks and money orders; and sell travelers' checks and certified checks. 12 U.S.C. 24(Seventh); 12 U.S.C. 4001 et seq; Conditional Approval No. 307 (April 1999). Banks may cash checks for non-customers. See OCC Interpretive Letter No. 1094 (Feb. 27, 2008); Interpretive Letter No. 932 (May 2002).

[30] Electronic Activities, 67 FR 34,992, 34,966 (May 17, 2002).

of payments: issuing and circulating notes.[31] The OCC further noted that ESV-related clearing and settlement activities are similar to those already being performed by banks in connection with the large volume of transactions using checks, drafts, travelers' checks, credit cards, debit cards, and electronic transfers of funds within and through the payments system.[32]

Like ESV, stablecoins can serve as electronic representations of those U.S. dollars. Instead of value being stored on an ESV card, the value is represented on the stablecoin. This distinction is technological in nature and does not affect the permissibility of the underlying activity. Banks may use new technologies that afford a new means of carrying out permissible banking functions, such as providing payments services and facilitating payments.[33] Using INVNs and related stablecoins to facilitate payments is merely a new means of performing that function.

Just as banks may buy and sell ESV as a means of converting the ESV into dollars (and vice versa) to complete customer payment transactions, banks may buy, sell, and issue stablecoin to facilitate payments.[34] For example, one entity (payer) may wish to remit a payment of U.S. dollars to a second entity (payee). Rather than using a centralized payment system, the payer converts the U.S. dollars to stablecoin and transfers the stablecoin to the payee via the INVN. The payee then converts the stablecoin back into U.S. dollars. In one common version of this fact pattern, the payment is a cross-border remittance. In certain circumstances, using INVNs and related stablecoins to facilitate the remittance may provide a cheaper, faster, and more efficient means of effecting the payment. The bank may serve several potential roles in

---

[31] See OCC Conditional Approval Letter No. 220. Specifically, the OCC permitted banks to invest, via operating subsidiaries, in a company (Mondex LLC) that created, sold, and redeemed ESV. The OCC also permitted banks to serve as members in the ESV system. As described in the letter, members would issue ESV cards to individuals in exchange for dollars. These cards were intended to become a new element of the payment system substituting ESV for cash and small checks in consumer transactions. Mondex LLC would create and sell ESV to members in exchange for dollars. Mondex LLC would invest the dollars in government securities, cash, and cash equivalents. If a member tendered ESV to Mondex LLC, Mondex LLC would redeem the ESV at par. Members would sell ESV to individuals and participating retailers in exchange for dollars. ESV would be loaded onto the individual's card or retailer or retailer's "purse carrier device." Members would also purchase ESV from retailers and individuals.

[32] See id.

[33] See, e.g., State of Ill. ex rel. Lignoul v. Cont'l Nat. Bank & Tr. Co. of Chicago, 536 F.2d 176, 178 (7th Cir. 1976) (concluding that debit cards constituted checks under the National Bank Act, despite technological differences between the two because "[t]he check is merely the means used by the bank to attain the desired objective, i.e., the payment of the money to its customer. The card serves the same purpose as the check. It is an order on the bank. Any order to pay which is properly executed by a customer, whether it be check, card or electronic device, must be recognized as a routine banking function when used as here. The relationship between the bank and its customer is the same."); Smith, 534 F.2d at 944 ("We conclude that Congress envisioned all account withdrawals when it used the shorthand phrase "checks paid" in section 36(f) [of the National Bank Act]. If future technological innovations render paper checks totally obsolete, section 36(f) will still include within its broad standard those facilities that permit bank customers to perform the traditional banking function of withdrawing funds from their accounts.").

[34] Moreover, buying, selling, and issuing stablecoins to facilitate payments responds to customer demand and benefits customers by offering faster and more resilient payment mechanisms. In addition, providing payment services using INVNs and related stablecoins may allow banks to offer services to a more diverse customer base. Finally, the risks associated with buying, selling, and issuing stablecoins are similar to those that banks assume in other permissible payment activities, including the provision of ESV systems.

this type of transaction: supporting the INVN by validating transactions as a node on the INVN, facilitating the conversion from U.S. dollars to stablecoin (and vice versa), and issuing the stablecoin.

III. Benefits and Risks

While the OCC neither encourages nor discourages banks from participating in and supporting INVNs and stablecoins, the recent adoption of INVNs and stablecoins by a major payment system operator,[35] coupled with the rapid market adoption of INVNs and stablecoins,[36] indicates that banks should evaluate the appropriateness of INVNs and stablecoin participation in order to ensure banks' continuing ability to provide payment services to their customers in a manner that reflects changing demand.

INVNs and stablecoins present both benefits and risks. Among the potential benefits is the fact that INVNs may enhance the efficiency, effectiveness, and stability of the provision of payments. For example, they may be more resilient than other payment networks because of the decentralized nature of INVNs. Rather than relying on a single entity (or a small number of parties) to verify payments, INVNs allow a comparatively large number of nodes to verify transactions in a trusted manner. Simply put, these networks may be more resilient because they have no single point of failure and can continue to operate even if a number of nodes cease to function for some reason and may be more trusted because of their consensus mechanisms requiring more nodes to validate the underlying transactions. In addition, an INVN also acts to prevent tampering or adding inaccurate information to the database. Information is only added to the network after consensus is reached among the nodes confirming that the information is valid.

The use of stablecoins to facilitate payments allows banks to capture the advantages that INVNs may present in a manner that retains the stability of fiat currency.[37] INVNs can transfer multiple different cryptocurrencies including but not limited to stablecoins. Stablecoins serve as a means of representing fiat currency on an INVN. In this way, the stablecoin provides a means for fiat currency to have access to the payment rails of an INVN.

Although the use of INVNs may provide certain advantages over other technologies, it may also present new risks. Banks that seek to use these networks should ensure that they understand these risks, as well as the risks generally associated with the underlying activity.[38] In addition, banks seeking to use these networks must conduct the activities in a safe and sound manner. These banks should also conduct a legal analysis to ensure the activities will be

---

[35] See supra n. 11.

[36] See supra n. 12.

[37] See, e.g., Advancing Our Approach to Digital Currency: Visa's Outlook on New Digital Currency Payment Flows (July 22, 2020).

[38] See, e.g., Comptroller's Handbook on Payment Systems and Fund Transfer Activities (March 1990); New, Modified, or Expanded Bank Products and Services: Risk Management Principles, OCC Bulletin 2017-43.

conducted consistent with all applicable laws, including applicable anti-money laundering laws and regulations and consumer protection laws and regulations.

Payment activities involving cryptocurrencies could increase operational risks, including fraud risk. Depending on the nature of the payment activity, activities involving stablecoins could entail significant liquidity risks for banks.[39] Moreover, new technologies require sufficient technological expertise to ensure a bank can manage them in a safe and sound manner and otherwise conduct the activities in compliance with applicable law, including applicable consumer protection laws and regulations. Banks have experience developing such expertise in analogous areas. These risks are similar (though potentially greater in degree) to those of other electronic activities expressly permitted for banks, including providing electronic custody services,[40] acting as a digital certification authority[41] and providing data processing services.[42] Risk management should be commensurate with the complexity of the products and services offered. New activities should be developed and implemented consistently with sound risk management practices and should align with banks' overall business plans and strategies.[43]

Cryptocurrency payment activities could also raise heightened compliance risks. In particular, cryptocurrencies can present risks under anti-money laundering (AML) and countering the financing of terrorism requirements set forth in applicable laws, including the Bank Secrecy Act (BSA), because cryptocurrencies may be used by bad actors for the purposes of avoiding the financial system or engaging in other illicit activities. However, banks have significant experience with developing BSA/AML compliance programs to assure compliance with the reporting and recordkeeping requirements of the BSA and to prevent such usage of their systems by bad actors.[44] The OCC similarly would expect banks engaged in providing cryptocurrency services to customers to adapt and expand their BSA/AML compliance programs to assure compliance with the reporting and recordkeeping requirements of the BSA and to address the particular risks of cryptocurrency transactions.

A bank may validate, store, and record payments transactions by serving as a node on an INVN and use INVNs and related stablecoins to carry out other bank-permissible payment activities, consistent with applicable law and safe and sound banking practices. A bank should consult with OCC supervisors, as appropriate, prior to engaging in these payment activities. The OCC will review these activities as part of its ordinary supervisory processes.

Sincerely,

---

[39] See IL 1172.

[40] See Comptroller's Handbook on Custody Services at 70 (Jan. 2002).

[41] 12 C.F.R. § 7.5005.

[42] Id.

[43] See OC Bulletin-2017-43.

[44] See, e.g., 12 U.S.C. § 1818(s); 12 C.F.R. § 21.21; 31 C.F.R. § 1020.210; see also FFIEC, FFIEC BSA/AML Examination Manual, available at https://bsaaml.ffiec.gov/manual (database of BSA/AML policies and procedures).

/s/

Jonathan V. Gould
Senior Deputy Comptroller & Chief Counsel

Office of the Comptroller of the Currency

Washington, DC 20219

Interpretive Letter #1172

October 2020

OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves

September 21, 2020

I. Introduction and Summary Conclusion

This letter addresses the authority of a national bank to hold deposits that serve as reserves for certain "stablecoins." Generally, a stablecoin is a type of cryptocurrency designed to have a stable value as compared with other types of cryptocurrency, which frequently experience significant volatility. One type of stablecoin is backed by an asset such as a fiat currency. Reports suggest stablecoins have various applications, including the potential to enhance payments on a broad scale,[1] and are increasingly in demand.[2] As described further below, stablecoin issuers may desire to place assets in a reserve account with a national bank to provide assurance that the issuer has sufficient assets backing the stablecoin in situations where there is a hosted wallet.[3] For the reasons discussed below, we conclude that a national bank may hold such stablecoin "reserves" as a service to bank customers.[4] We are not presently addressing the authority to support stablecoin transactions involving un-hosted wallets. In addition, this letter only addresses the use of stablecoin backed on a 1:1 basis by a single fiat currency where the

---

[1] See, e.g., Marc Di Maggio and Nicholas Platias, Is Stablecoin the Next Big Thing in E-Commerce?, Harv. Bus. Rev. (May 21, 2020), available at https://hbr.org/2020/05/is-stablecoin-the-next-big-thing-in-e-commerce.

[2] See, e.g., Antonio Madeira, On Solid Ground: Stablecoins Thriving Amid Financial Uncertainty, Cointelegraph.com (Aug. 2, 2020), available at https://cointelegraph.com/news/on-solid-ground-stablecoins-thriving-amid-financial-uncertainty.

[3] "Cryptocurrencies are generally held in 'wallets,' which are programs that store the cryptographic keys associated with a particular unit of digital currency." OCC Interpretive Letter No. 1170, at 5 (July 22, 2020), available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (IL 1170). A hosted wallet is an account-based software program for storing cryptographic keys controlled by an identifiable third party. These parties receive, store, and transmit cryptocurrency transactions on behalf of their accountholders; the accountholder generally does not have access to the cryptographic keys themselves. In contrast, an un-hosted or personal wallet is one where an individual owner of a cryptocurrency maintains control of the cryptographic keys for accessing the underlying cryptocurrency.

[4] These conclusions apply only to the deposit activities of national banks and Federal savings associations (FSAs). This letter expresses no conclusion on the application of any other laws to the stablecoin activities discussed in this letter or on the permissibility of these activities for any institutions other than those supervised by the OCC.

bank verifies at least daily that reserve account balances are always equal to or greater than the number of the issuer's outstanding stablecoins.[5]

A bank providing services in support of a stablecoin project must comply with all applicable laws and regulations and ensure that it has instituted appropriate controls and conducted sufficient due diligence commensurate with the risks associated with maintaining a relationship with a stablecoin issuer. The due diligence process should facilitate an understanding of the risks of cryptocurrency and include a review for compliance with applicable laws and regulations, including those related to the Bank Secrecy Act (BSA) and anti-money laundering. In this regard, the review should include, but not be limited to, customer due diligence requirements under the BSA[6] and the customer identification requirements under section 326 of the USA PATRIOT Act.[7] A national bank or FSA must also identify and verify the beneficial owners of legal entity customers opening accounts.[8] A national bank or FSA must also comply with applicable federal securities laws.[9]

II. Stablecoin Reserves

Cryptocurrencies—also known as "digital currencies" or "virtual currencies"—are often designed to work as a medium of exchange and are created and stored electronically.[10] As we previously described, cryptocurrencies are enabled by two technologies: cryptography and distributed ledger technology.[11] Cryptography and distributed ledger technology are both rapidly evolving technologies. As described above, "stablecoin" often refers to a particular type of digital coin that is backed by another asset, such as a fiat currency.

Like cryptocurrencies more broadly, stablecoins are an evolving technology. Different types of stablecoins may share certain characteristics, but there are variations in the way various

---

[5] The current stablecoin activities discussed in this letter would not contribute to the global and systemic risks noted by the Financial Stability Board in its recent consultation. See Fin. Stability Board, Addressing the Regulatory, Supervisory and Oversight Challenges Raised by "Global Stablecoin" Arrangements (Apr. 14, 2020), available at https://www.fsb.org/wp-content/uploads/P140420-1.pdf.

[6] 31 C.F.R. § 1020.210(b)(5).

[7] 12 C.F.R. § 21.21(c)(2); 31 C.F.R. § 1020.220. See also OCC Bulletin 2016-10, Prepaid Cards: Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016), available at https://occ.gov/news-issuances/bulletins/2016/bulletin-2016-10.html.

[8] 31 C.F.R. § 1010.230.

[9] We note that staff of the Securities and Exchange Commission (SEC) has issued a statement encouraging issuers of stablecoins of the type described herein to contact the staff with any questions they may have to help ensure that such stablecoins are structured, marketed, and operated in compliance with the federal securities laws. The statement notes that the staff stands ready to engage with market participants, and, depending on the particular facts and circumstances, to assist them and consider providing, if appropriate, a "no-action" position regarding whether activities with respect to a specific stablecoin may invoke the application of the federal securities laws. See SEC FinHub Staff Statement on OCC Interpretation (Sept. 21, 2020).

[10] The OCC recently described many features of cryptocurrency. See IL 1170.

[11] IL 1170, at 2.

cryptocurrencies described as "stablecoins" work. Cryptocurrencies referred to as "stablecoins" may be backed by a fiat currency, a commodity, or another cryptocurrency. Fiat-backed stablecoins are typically redeemable for the underlying fiat currency, where one unit of the stablecoin can be exchanged for one unit of the underlying fiat currency. Other types of cryptocurrencies described as "stablecoins" may be more complex, backed by commodities, cryptocurrencies, or other assets but with values that are pegged to a fiat currency or managed by algorithm. For purposes of this letter, we consider a "stablecoin" to be a unit of cryptocurrency associated with hosted wallets that is backed by a single fiat currency and redeemable by the holder of the stablecoin on a 1:1 basis for the underlying fiat currency upon submission of a redemption request to the issuer. We are only opining on those facts and circumstances at this time.

Companies that issue stablecoins often desire to place the funds backing the stablecoin, or reserve funds, with a U.S. bank. Public independent auditors' statements of several stablecoin issuers indicate reserve funds are placed as deposits with U.S. banks. Several of these issuers promote these reserves—and the fact that they are held by banks—to support the trustworthiness of their stablecoin. In light of the public interest in these reserve accounts, this letter addresses the legal authority of national banks to hold stablecoin reserves on behalf of customers.

III. Discussion

We understand that some stablecoin issuers may desire to place the cash reserves backing their issued stablecoin with a national bank. In the most basic example, a stablecoin issuer may seek to place its reserve funds in a deposit account with a national bank. National banks are expressly authorized to receive deposits.[12] Receiving deposits is recognized as a core banking activity.[13] As the OCC recently reaffirmed, national banks may provide permissible banking services to any lawful business they choose, including cryptocurrency businesses, so long as they effectively manage the risks and comply with applicable law, including those relating to the BSA and anti-money laundering.[14] Accordingly, national banks may receive deposits from stablecoin issuers, including deposits that constitute reserves for a stablecoin associated with hosted wallets. In connection with these activities, a national bank may also engage in any activity incidental to

[12] 12 U.S.C. 24(Seventh).

[13] See, e.g., 12 C.F.R. § 5.20(e).

[14] See IL 1170, at 1. In IL 1170, the OCC reaffirmed its view that banks determine the levels and types of risks that they will assume. Banks that operate in compliance with applicable law, properly manage customer relationships and effectively mitigate risks by implementing controls commensurate with those risks are neither prohibited nor discouraged from providing banking services. As the federal banking agencies have previously stated, banks are encouraged to manage customer relationships and mitigate risks based on customer relationships rather than declining to provide banking services to entire categories of customers. See Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision, at 2 (July 22, 2019), available at https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf.

receiving deposits from stablecoin issuers.[15] Likewise, an FSA is authorized to take deposits,[16] including from an issuer of stablecoin associated with hosted wallets.

As with any deposit product, a national bank or FSA that accepts reserve accounts should be aware of the laws and regulations relating to deposit insurance coverage, including deposit insurance limits,[17] and the requirements for deposit insurance to "pass through" to an underlying depositor, if applicable.[18] Stablecoin reserve accounts could be structured as either deposits of the stablecoin issuer or as deposits of the individual stablecoin holder if the requirements for pass through insurance are met.[19] Accordingly, a national bank or FSA should provide accurate and appropriate disclosures regarding deposit insurance coverage. A national bank or FSA must ensure that its deposit activities comply with applicable laws and regulations, including those relating to the BSA and anti-money laundering. Specifically, a national bank or FSA must ensure that it establishes and maintains procedures reasonably designed to assure and monitor its compliance with the BSA and its implementing regulations, including but not limited to customer due diligence requirements under the BSA[20] and the customer identification requirements under section 326 of the USA PATRIOT Act.[21] A national bank or FSA must also identify and verify the beneficial owners of legal entity customers opening accounts.[22] A national bank or FSA must also comply with applicable federal securities laws.

---

[15] 12 C.F.R. § 7.4007 (permitting "any activity incidental to receiving deposits, including issuing evidence of accounts, subject to such terms, conditions, and limitations prescribed by the Comptroller of the Currency and any other applicable Federal law").

[16] See 12 U.S.C. 1464(b).

[17] See generally 12 U.S.C. 1821; 12 C.F.R. Part 330.

[18] 12 C.F.R. Part 330; FDIC General Counsel's Op. No. 8 (Nov. 13, 2008), available at https://www.govinfo.gov/content/pkg/FR-2008-11-13/pdf/E8-26867.pdf. For example, in the context of prepaid cards, OCC guidance has explained that, according to FDIC General Counsel's Opinion No. 8, "stored value (electronic cash) issued by banks will be insured if the funds underlying the electronic cash remain in a customer's account until it is transferred to a merchant or other third party, who in turn collects the funds from the customer's bank. However, bank-issued electronic cash does not result in an insured deposit when the underlying funds are placed in a reserve or general liability account held by the issuing bank to pay merchants and other payees as they make claims for payments." OCC Bulletin 1996-48 (Sept. 3, 1996), https://www.occ.gov/news-issuances/bulletins/1996/bulletin-1996-48.html.

[19] 12 C.F.R. Part 330; FDIC General Counsel's Op. No. 8 (Nov. 13, 2008). The general requirements for pass-through deposit insurance coverage are: (1) the account records at the bank must disclose the existence of the third-party custodial relationship; (2) the bank's records or records maintained by the custodian or other party must disclose the identities of the actual owners of the funds and the amount owned by each such owner; and (3) the deposits actually must be owned (under the agreements among the parties) by the named owners.

[20] 31 C.F.R. § 1020.210(b)(5).

[21] 12 C.F.R. § 21.21(c)(2); 31 C.F.R. § 1020.220. See also OCC Bulletin 2016-10, Prepaid Cards: Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016).

[22] 31 C.F.R. § 1010.230.

New bank activities should be developed and implemented consistently with sound risk management principles and should align with banks' overall business plans and strategies.[23] Bank management should establish appropriate risk management processes for new activity development and effectively identify, measure, monitor, and control the risks associated with new activities. In particular, reserves associated with stablecoins could entail significant liquidity risks. The OCC expects all banks to manage liquidity risk with sophistication equal to the risks undertaken and complexity of exposures.[24] A bank may also enter into appropriate contractual agreements with a stablecoin issuer governing the terms and conditions of the services that the bank provides to the issuer.[25] Such agreements may include contractual restrictions or requirements with respect to the assets held in the reserve account. The agreement may also specify the respective responsibilities of the parties, such as the steps the parties will take to ensure the appropriate party will be deemed the issuer or obligor of the stablecoin. For example, the bank should have appropriate agreements in place with an issuer to verify and ensure that the deposit balances held by the bank for the issuer are always equal to or greater than the number of outstanding stablecoins issued by the issuer. Such agreements should include mechanisms to allow the bank to verify the number of outstanding stablecoins on a regular basis.[26] In the analogous context of prepaid cards distributed and sold by third-party program managers, interagency guidance specifically contemplates that banks would enter into contracts with third-party program managers permitting banks to audit the third-party program managers.[27]

---

[23] See OCC Bulletin 2017-43, New, Modified, or Expanded Bank Products and Services: Risk Management Principles, available at https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-43.html.

[24] See Comptroller's Handbook on Liquidity (June 2012), at 4, available at https://occ.gov/publications-and-resources/publications/comptrollers-handbook/files/liquidity/pub-ch-liquidity.pdf. For example, a critical component of an institution's ability to effectively respond to potential liquidity stress is the availability of a cushion of unencumbered highly liquid assets without legal, regulatory, or operational impediments that can be sold or pledged to obtain funds in a range of stress scenarios. Id. at 30.

[25] OCC guidance has previously recognized the importance of contracts in establishing responsibilities and liability in the context of prepaid cards. In describing the responsibilities of national banks participating in then-emergent prepaid card systems, the OCC said: "A bank should be clear as to who bears the responsibility at each stage of an electronic cash transaction. Thus far, transactional rules for some electronic cash systems are not well established by current law. Accordingly, in many important respects, the transactional rules for such systems must be established by contract." OCC Bulletin 1996-48 (Sept. 3, 1996). See also OCC Bulletin 2016-10, Prepaid Cards: Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016). Similarly, a bank that receives deposits from a stablecoin issuer should enter into appropriate contracts to define the responsibilities of the parties.

[26] Banks are subject to capital and reserve requirements intended to ensure that banks have sufficient liquidity and are able to meet the needs of customers, including by satisfying withdrawals and cashing checks. See generally, 12 C.F.R. Part 204 (reserve requirements); 12 C.F.R. Part 3 (capital requirements). See also Comptroller's Handbook on Cash Accounts (Mar. 1998), available at https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/cash-accounts/pub-ch-cash-accounts.pdf; Comptroller's Handbook on Depository Services (Aug. 2010), available at https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/depository-services/pub-ch-depository-services.pdf.

[27] See OCC Bulletin 2016-10, Prepaid Cards: Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (Mar. 21, 2016).

A bank should consider all relevant risk factors, including liquidity risk and compliance risk, before entering any agreement or relationship with a stablecoin issuer.

/s/

Jonathan V. Gould
Senior Deputy Comptroller and Chief Counsel

FEDERAL DEPOSIT INSURANCE CORPORATION

RIN 3064-ZA25

Request for Information and Comment on Digital Assets

AGENCY: Federal Deposit Insurance Corporation.

ACTION: Request for information and comment.

SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is gathering information and soliciting comments from interested parties regarding insured depository institutions' (IDIs') current and potential activities related to digital assets. The FDIC is interested in receiving input on current and potential digital asset use cases involving IDIs and their affiliates.

DATES: Comments must be received by July 16, 2021.

ADDRESSES: Commenters are encouraged to use the title "*Request for Information and Comment on Digital Assets (RIN 3064-ZA25)*" and to identify the number of the specific question(s) for comment to which they are responding. Please send comments by one method only directed to:

- *Agency Website:* https://www.fdic.gov/regulations/laws/federal/. Follow the instructions for submitting comments on the agency's website.
- *Email:* Comments@fdic.gov. Include RIN 3064-ZA25 in the subject line of the message.
- *Mail:* James P. Sheesley, Assistant Executive Secretary, Attention: Comments-RIN 3064-ZA25, Federal Deposit Insurance Corporation, 550 17th Street N.W., Washington, D.C. 20429.

- *Hand Delivery/Courier:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street N.W. building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m., ET.

Public Inspection: All comments received will be posted without change to *https://www.fdic.gov/regulations/laws/federal/*—including any personal information provided—for public inspection. Paper copies of public comments may be ordered from the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226 or by telephone at (877) 275-3342 or (703) 562-2200.

FOR FURTHER INFORMATION CONTACT:

Rae-Ann Miller, Senior Deputy Director, Supervisory Examinations and Policy, Division of Risk Management Supervision, (202) 898–3898, rmiller@fdic.gov; Jonathan Miller, Deputy Director, Division of Depositor and Consumer Protection, 202-898-3587, jonmiller@fdic.gov; or C. Chris Ledoux, Corporate Expert, Financial Innovation and Technology Group, Legal Division, 202-898-3535, cledoux@fdic.gov.

SUPPLEMENTARY INFORMATION

Background Information

FDIC Overview

The FDIC is an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system. The FDIC works to maintain the strength of the U.S. financial sector through effective supervision of regulated financial institutions, consumer

protection, the resolution of failed financial institutions, and the provision of deposit insurance.[1] In its capacity as a federal banking regulator and deposit insurer, among other functions, the FDIC examines and supervises institutions' safe and sound operations and compliance with laws and regulations, evaluates resolution plans of large financial institutions, maintains the Deposit Insurance Fund (DIF), and resolves failed IDIs.[2] Collectively, the FDIC's activities support a safe-and-sound banking sector and contribute to the stability of and public confidence in the U.S. financial system as a whole.

In addition to its individual responsibilities, the FDIC works cooperatively with its fellow state and federal banking regulators to strengthen the banking sector and the U.S. financial system, including through a number of interagency formal structures, joint rule making and examinations.

Current and Potential Digital Assets Use Cases

One area of new technology and innovation surrounds the use of digital assets in financial markets and intermediation, as well as with settlement and payment systems. Banks are increasingly exploring several roles in the emerging digital asset ecosystem, such as being custodians, reserve holders, issuers, and exchange or redemption agents; performing node functions; and holding digital asset issuers' money deposits.

Digital asset use cases and related activities may fall into one or more broad categories:

[1] As of December 31, 2020, the FDIC insured 5,001 insured commercial banks and savings institutions. The FDIC is the primary federal regulator of state-chartered banks and savings associations that are not members of the Federal Reserve System. As of December 31, 2020, the FDIC supervised approximately 3,221 banks and savings associations. The FDIC also has a back-up supervision and examination role with respect to insured depository institutions for which the Office of the Comptroller of the Currency and the Board of Governors of the Federal Reserve System are the primary federal regulators. *See* https://www.fdic.gov/analysis/quarterly-banking-profile/qbp/2020dec/.

[2] "Insured depository institution" means any bank or savings association the deposits of which are insured by the FDIC pursuant to the Federal Deposit Insurance Act (FDI Act). *See* 12 U.S.C. 1813(c).

- Technology solutions, such as those involving closed and open payment systems, other token-based systems for banking activities other than payments (e.g., lending), and acting as nodes in networks (*e.g.*, distributed ledgers).
- Asset-based activities, such as investments, collateral, margin lending and liquidity facilities.
- Liability-based activities, such as deposit services and where deposits serve as digital asset reserves.
- Custodial activities, such as providing digital asset safekeeping and related services, such as secondary lending, as well as acting as a qualified custodian on behalf of investment advisors.
- Other activity that does not align with the others above. Examples could include market-making and decentralized financing.

Request for Comment

The FDIC recognizes that there are novel and unique considerations related to digital assets, and this RFI is intended to help inform the FDIC's understanding in this area. The FDIC is seeking input on current and potential use cases involving IDIs and their affiliates and risk and compliance management in conducting such activities.

Questions Regarding Current and Potential Use Cases

1. In addition to the broad categories of digital assets and related activities described above, are there any additional or alternative categories or subcategories that IDIs are engaged in or exploring?

2. What, if any, activities or use cases related to digital assets are IDIs currently engaging in or considering? Please explain, including the nature and scope of the activity. More specifically:
    a. What, if any, types of specific products or services related to digital assets are IDIs currently offering or considering offering to consumers?
    b. To what extent are IDIs engaging in or considering engaging in activities or providing services related to digital assets that are custodial in nature, and what are the scope of those activities? To what extent are such IDIs engaging in or considering secondary lending?
    c. To what extent are IDIs engaging in or considering activities or providing services related to digital assets that have direct balance sheet impacts?
    d. To what extent are IDIs engaging in or considering activities related to digital assets for other purposes, such as to facilitate internal operations?
3. In terms of the marketplace, where do IDIs see the greatest demand for digital asset-related services, and who are the largest drivers for such services?

Questions Regarding Risk and Compliance Management

4. To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?

5. What unique or particular risks are challenging to measure, monitor, and control for the various digital asset use cases? What unique controls or processes are or could be implemented to address such risks?
6. What unique benefits to operations do IDIs consider as they analyze various digital asset use cases?
7. How are IDIs integrating, or how would IDIs integrate, operations related to digital assets with legacy banking systems?
8. Please identify any potential benefits, and any unique risks, of particular digital asset product offerings or services to IDI customers.
9. How are IDIs integrating these new technologies into their existing cybersecurity functions?

Questions Regarding Supervision and Activities

10. Are there any unique aspects of digital asset activities that the FDIC should take into account from a supervisory perspective?
11. Are there any areas in which the FDIC should clarify or expand existing supervisory guidance to address digital asset activities?
12. In what ways, if any, does custody of digital assets differ from custody of traditional assets?
13. FDIC's Part 362 application procedures may apply to certain digital asset activities or investments.[3] Is additional clarity needed? Would any changes to FDIC's regulations or the related application filing procedures be helpful in addressing

[3] *See* 12 C.F.R. Part 362, subpart A.

uncertainty surrounding the permissibility of particular types of digital asset-related activity, in order to support IDIs considering or engaging in such activities?

Questions Regarding Deposit Insurance and Resolution

14. Are there any steps the FDIC should consider to ensure customers can distinguish between uninsured digital asset products on the one hand, and insured deposits on the other?
15. Are there distinctions or similarities between fiat-backed stablecoins and stored value products where the underlying funds are held at IDIs and for which pass-through deposit insurance may be available?
16. If the FDIC were to encounter any of the digital assets use cases in the resolution process or in a receivership capacity, what complexities might be encountered in valuing, marketing, transferring, operating, or resolving the digital asset activity? What actions should be considered to overcome the complexities?

Additional Considerations

17. Comments are invited to address any other digital asset-related information stakeholders seek to bring to the FDIC's attention. Comments are also welcome about the digital asset-related activities of uninsured banks and nonbanks.

Federal Deposit Insurance Corporation.

Dated at Washington, D.C., on or about May 17, 2021

James P. Sheesley,

Assistant Executive Secretary.

BILLING CODE 6714-01-P

FEDERAL RESERVE SYSTEM

Docket No. OP-1747

Proposed Guidelines for Evaluating Account and Services Requests

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Notice; request for comment

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is requesting comment on proposed guidelines (Account Access Guidelines) to evaluate requests for accounts and services at Federal Reserve Banks (Reserve Banks).

DATES: Comments on the proposed changes must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by Docket No. OP-1747, by any of the following methods:

- Agency website: http://www.federalreserve.gov. Follow the instructions for submitting comments at http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.
- Email: regs.comments@federalreserve.gov. Include docket number in the subject line of the message.
- Fax: (202) 452-3819 or (202) 452-3102.
- Mail: Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, N.W., Washington, DC 20551.

All public comments are available from the Board's web site at www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm as submitted, unless modified for technical reasons or to remove personally identifiable information at the

commenter's request. Accordingly, comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper in Room 146, 1709 New York Avenue NW, Washington, DC 20006, between 9:00 a.m. and 5:00 p.m. on weekdays.

FOR FURTHER INFORMATION CONTACT:

Jason Hinkle, Assistant Director (202-912-7805), Division of Reserve Bank Operations and Payment Systems, or Sophia Allison, Senior Special Counsel (202-452-3565) or Gavin Smith, Senior Counsel (202-872-7578), Legal Division, Board of Governors of the Federal Reserve System. For users of Telecommunications Device for the Deaf (TDD) only, please contact 202-263-4869.

SUPPLEMENTARY INFORMATION:

I. Background

The Board of Governors of the Federal Reserve System (Board) is considering adopting guidelines (Account Access Guidelines) to be used by Federal Reserve Banks (Reserve Banks) in evaluating requests for master accounts and/or access to Federal Reserve Bank financial services (accounts and services). The Board's approach to this proposal reflects its analysis of the Board's policy goals of (1) ensuring the safety and soundness of the banking system, (2) effectively implementing monetary policy, (3) promoting financial stability, (4) protecting consumers, and (5) promoting a safe, efficient, inclusive, and innovative payment system. The Board's proposed guidelines are also intended to ensure that Reserve Banks evaluate a transparent and consistent set of factors when reviewing requests for accounts and services (access requests).

The payments landscape is evolving rapidly as technological progress and other factors are leading to both the introduction of new financial products and services and to different ways of providing traditional banking services (i.e., payments, deposit-taking, and lending). Relatedly, there has been a recent uptick in novel charter types being authorized or considered across the country and, as a result, the Reserve Banks are receiving an increasing number of inquiries and requests for access to accounts and services from novel institutions.

Although the Reserve Banks have received such inquiries on an exceptional basis in the past, the Board now believes, given the increase in the number and novelty of such inquiries, that a more transparent and consistent approach to such requests should be adopted by the Reserve Banks. Given that access decisions made by individual Reserve Banks can have implications for a wide array of Federal Reserve System (Federal Reserve) policies and objectives, a structured, transparent, and detailed framework for evaluating access requests would benefit the financial system broadly. Such a framework would also help foster consistent evaluation of access requests, from both risk and policy perspectives, across all twelve Reserve Banks.

To help achieve the goal of applying a transparent and consistent process for all access requests, the Board is proposing guidelines for the Reserve Banks to evaluate such requests. The proposed account access guidelines contain six principles that would support consistency in approach and decision-making across Reserve Banks while maintaining Reserve Bank discretionary authority to grant or deny requests. Accordingly, the proposed guidelines would reduce the potential for forum shopping

across Reserve Banks and mitigate the risk that individual decisions by Reserve Banks could create de facto System policy for a particular business model or risk profile. These risk-focused guidelines would also promote more consistent implementation for eligible institutions with similar risk profiles.

The proposed account access guidelines are centered on a foundation of risk management and mitigation. In developing the proposed guidelines, the Board considered the risks that may arise when an institution gains access to accounts and services. These risks include, among others, risks to the Reserve Banks, to the payment system, to the financial system, and to the effective implementation of monetary policy.

The introduction to the proposed guidelines discusses the Federal Reserve's broad policy goals when providing accounts and services as well as the reasons for proposing to issue the account access guidelines. In addition, the introduction provides that while the guidelines are designed primarily for new access requests, Reserve Banks should also apply the guidelines to existing account and services relationships when a Reserve Bank becomes aware of a significant change in the risks that the account holder presents due to changes in the nature of its principal business activities, condition, etc.

The proposed account access guidelines identify potential risks and prompt the Reserve Bank to identify risk mitigation strategies adopted by the institution (including capital, risk frameworks, compliance with regulations, and supervision) and by the Reserve Bank (including account agreement provisions, restrictions on financial services accessed, account risk controls, and denial of access requests). The first principle specifies that only institutions that are legally eligible for accounts and services are in

scope, and the remaining five principles are designed to address specific risks ranging from narrow risks (such as risk to an individual Reserve Bank) to broader risks (such as risk to the U.S. financial system).[1] The Board is considering whether it may in the future be useful to clarify the interpretation of legal eligibility under the Federal Reserve Act for a Federal Reserve account and services.

For each of these principles, the proposed guidelines identify factors that Reserve Banks should consider when evaluating an institution against the specific risk targeted by the pringciple (several factors are pertinent to more than one principle). The identified factors are commonly used in the regulation and supervision of federally-insured institutions. When applying the account access guidelines the Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile. Given that the proposed guidelines utilize factors broadly applied to federally-insured institutions, the Board anticipates the application of the guidelines to access requests by federally-insured institutions would be fairly straightforward in most cases. Reserve Bank assessments of access requests from non-federally-insured institutions , however, may require more extensive due diligence.

Currently, Reserve Bank risk management practices include monitoring the condition of institutions with accounts and services on an ongoing basis using

[1] The proposed guidelines are designed as a risk management framework and, as such, the principles focus on risks an institution's access could pose. The Board notes, however, that an institution's access could have net benefits to the financial system that are not a focus of the risk management framework.

supervisory ratings, capitalization data, and other supplementary information. Reserve Banks use this process to determine whether risk controls or other restrictions should be placed on an institution's account. For example, the process is used to determine if an institution continues to remain eligible for primary credit. The Board anticipates that, if the proposed guidelines are adopted, Reserve Banks would use the guidelines to re-evaluate the risks posed by an institution in cases where these condition-monitoring activities indicate potential changes in the institution's risk profile.

II. II. Proposed Guidelines

Guidelines Covering Access to Accounts and Services at Federal Reserve Banks (Account Access Guidelines)

The Board of Governors of the Federal Reserve System (Board) has adopted account access guidelines comprised of six principles to be used by Federal Reserve Banks (Reserve Banks) in evaluating requests for master accounts and access to Federal Reserve Bank financial services (access requests).[2,3] The account access guidelines apply

[2] As discussed in the Federal Reserve's Operating Circular No. 1, an institution has the option to settle its Federal Reserve financial services transactions in its master account with a Reserve Bank or in the master account of another institution that has agreed to act as its correspondent. These principles apply to requests for either arrangement.

[3] Reserve Bank financial services mean all services subject to Federal Reserve Act, section 11A ("priced services") and Reserve Bank cash services. Financial services do not include transactions conducted as part of the Federal Reserve's open market operations or administration of the Reserve Banks' Discount Window.

to requests from all institutions that are legally eligible to receive an account or services, as discussed in more detail in the first principle.[4]

The Federal Reserve System's (Federal Reserve) approach to providing institutions with accounts and services depends on, among other things, whether the institution is legally eligible to obtain an account and on the Federal Reserve's policy goals of ensuring the safety and soundness of the banking system, effectively implementing monetary policy, promoting financial stability, protecting consumers, and promoting a safe, effective, efficient, accessible and innovative payment system. The Board believes it is important to make clear that legal eligibility does not bestow a right to obtain an account and services. While decisions regarding individual access requests remain at the discretion of the individual Reserve Banks, the Board believes it is important that the Reserve Banks apply a consistent set of guidelines when reviewing such access requests to promote consistent outcomes across Reserve Banks and to facilitate equitable treatment across institutions.

These account access guidelines also serve to inform requestors of the factors that a Reserve Bank will review in any access request and thereby allow requestors to make any enhancements to its risk management, documentation, or other practices, as the case may be, to attempt to demonstrate how it meets each of these factors for review.

[4] These principles would not apply to accounts provided under fiscal agency authority or to accounts authorized pursuant to the Board's Regulation N (12 CFR 214), joint account requests, or account requests from designated financial market utilities, since existing rules or policies already set out the considerations involved in granting these types of accounts.

These guidelines broadly outline considerations for evaluating access requests but are not intended to provide assurance that any specific institution will be granted an account and services. The individual Reserve Bank will evaluate each access request on a case-by-case basis. When applying these account access guidelines, the Reserve Bank should incorporate to the extent possible the assessments of an institution by state and/or federal supervisors into its independent analysis of the institution's risk profile. The evaluation of an institution's access request should also consider whether the request has the potential to set a precedent that could affect the Federal Reserve's ability to achieve its policy goals now or in the future.

If the Reserve Bank decides to grant an access request, it may impose (at the time of account opening, granting access to service, or any time thereafter) obligations relating to, or conditions or limitations on, use of the account or services as necessary to limit operational, credit, legal, or other risks posed to the Reserve Banks, the payment system, financial stability or the implementation of monetary policy or to address other considerations.[5] The account-holding Reserve Bank may, at its discretion, decide to place additional risk management controls on the account and services, such as real-time monitoring of account balances, as it may deem necessary to mitigate risks. If the obligations, limitations, or controls are ineffective in mitigating the risks identified or if the obligations, limitations, or controls are breached, the account-holding Reserve Bank

[5] The conditions imposed could include, but are not limited to, paying a different rate of interest on balances held in the account, limiting the amount of balances on which interest is paid, or establishing a cap on the amount of balances held in the account.

may further restrict the institution's use of accounts and services or may close the account. Establishment of an account and provision of services by a Reserve Bank under these guidelines is not an endorsement or approval by the Federal Reserve of the institution. Nothing in the Board's guidelines relieves any institution from compliance with obligations imposed by the institution's supervisors and regulators.

Accordingly, Reserve Banks should evaluate how each institution requesting an account and services will meet the following principles.[6] Each principle identifies factors that Reserve Banks should consider when evaluating an institution against the specific risk targeted by the principle (several factors are pertinent to more than one principle). The identified factors are commonly used in the regulation and supervision of federally-insured institutions. As a result, the Board anticipates the application of the account access guidelines to access requests by federally-insured institutions will be fairly straightforward in most cases. However, Reserve Bank assessments of access requests from non-federally insured institutions may require more extensive due diligence.

Reserve Banks monitor and analyze the condition of institutions with accounts and services on an ongoing basis. Reserve Banks should use the guidelines to re-evaluate the risks posed by an institution in cases where its condition monitoring and analysis indicate

[6] The principles are designed to address risks posed by an institution having access to an account and services, ranging from narrow risks (e.g., to an individual Reserve Bank) to broader risks (e.g., to the overall economy). Review activities performed by the Reserve Bank may address several principles at once.

potential changes in the risk profile of an institution, including a significant change to the institution's business model.

1. Each institution requesting an account or services must be eligible under the Federal Reserve Act or other federal statute to maintain an account at a Federal Reserve Bank (Reserve Bank) and receive Federal Reserve services and should have a well-founded, clear, transparent, and enforceable legal basis for its operations.[7]

a. Unless otherwise specified by federal statute, only those entities that are member banks or meet the definition of a depository institution under section 19(b) of the Federal Reserve Act are legally eligible to obtain Federal Reserve accounts and financial services.[8]

b. The Reserve Bank should assess the consistency of the institution's activities and services with applicable laws and regulations, such as Article 4A of the Uniform Commercial Code and the Electronic Fund Transfer Act. The Reserve Bank should also consider whether the design of the institution's services would impede compliance by the institution's customers with U.S. sanction programs, Bank Secrecy Act (BSA) and

[7] These principles do not apply to accounts provided by a Reserve Bank as depository and fiscal agent for the Treasury and for certain government-sponsored entities (12 U.S.C. 391, 393-95, 1823, 1435) as well as to accounts provided to certain international organizations (22 U.S.C. sections 285d, 286d, 290o-3, 290i-5, 290l-3), to designated financial market utilities (12 U.S.C. 5465), pursuant to the Board's Regulation N (12 CFR 214), or to the Board's Guidelines for Evaluating Joint Account Requests.

[8] These principles apply to account requests from member banks or other entities that meet the definition of a depository institution under section 19(b), as well as Edge and Agreement corporations (12 U.S.C. 601-604a, 611-631), and branches and agencies of foreign banks (12 U.S.C. 347d).

anti-money-laundering (AML) requirements or regulations, or consumer protection laws and regulations.

2. Provision of an account and services to an institution should not present or create undue credit, operational, settlement, cyber or other risks to the Reserve Bank.

a. The Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile.

b. The Reserve Bank should confirm that the institution has an effective risk management framework and governance arrangements to ensure that the institution operates in a safe and sound manner, during both normal conditions and periods of idiosyncratic and market stress.

i. For these purposes, effective risk management includes having a robust framework, including policies, procedures, systems, and qualified staff, to manage applicable risks. The framework should at a minimum identify, measure, and control the particular risks posed by the institution's business lines, products and services. The effectiveness of the framework should be further supported by internal testing and internal audit reviews.

ii. The framework should be subject to oversight by a board of directors (or similar body) as well as oversight by state and/or federal banking supervisor(s).

iii. The framework should clearly identify all risks that may arise related to the institution's business (e.g., legal, credit, liquidity, operational, custody, investment) as well as objectives regarding the risk tolerances for the management of such risks.

c. The Reserve Bank should confirm that the institution is in substantial compliance with its supervisory agency's regulatory and supervisory requirements.

d. The institution must, in the Reserve Bank's judgment:

i. Demonstrate an ability to comply, were it to obtain a master account, with Board orders and policies, Reserve Bank agreements and operating circulars, and other applicable Federal Reserve requirements.

ii. Be in sound financial condition, including maintaining adequate capital to continue as a going concern and to meet its current and projected operating expenses under a range of scenarios.

iii. Demonstrate the ability, on an ongoing basis (including during periods of idiosyncratic or market stress), to meet all of its obligations in order to remain a going concern and comply with its agreement for a Reserve Bank account and services, including by maintaining:

A. Sufficient liquid resources to meet its obligations to the Reserve Bank under applicable agreements, operating circulars, and Board policies;

B. The operational capacity to ensure that such liquid resources are available to satisfy all such obligations to the Reserve Bank on a timely basis; and

C. Settlement processes designed to appropriately monitor balances in its Reserve Bank account on an intraday basis, to process transactions through its account in an orderly manner and maintain/achieve a positive account balance before the end of the business day.

iv. Have in place an operational risk framework designed to ensure operational resiliency against events associated with processes, people, and systems that may impair the institution's use and settlement of Reserve Bank services. This framework should consider internal and external factors, including operational risks inherent in the institution's business model, risks that might arise in connection with its use of any Reserve Bank account and services, and cyber-related risks. At a minimum, the operational risk framework should:

A. Identify the range of operational risks presented by the institution's business model (e.g., cyber vulnerability, operational failure, resiliency of service providers), and establish sound operational risk management objectives to address such risks;

B. Establish sound governance arrangements, rules, and procedures to oversee and implement the operational risk management framework;

C. Establish clear and appropriate rules and procedures to carry out the risk management objectives;

D. Employ the resources necessary to achieve its risk management objectives and implement effectively its rules and procedures, including, but not limited to, sound processes for physical and information security, internal controls, compliance, program management, incident management, business continuity, audit, and well-qualified personnel; and

E. Support compliance with the electronic access requirements, including security measures, outlined in the Reserve Banks' Operating Circular 5 and its supporting documentation.

3. Provision of an account and services to an institution should not present or create undue credit, liquidity, operational, settlement, cyber or other risks to the overall payment system.

a. The Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile.

b. The Reserve Bank should confirm that the institution has an effective risk management framework and governance arrangements to limit the impact that idiosyncratic stress, disruptions, outages, cyber incidents or other incidents at the institution might have on other institutions and the payment system broadly. The framework should include:

i. Clearly defined operational reliability objectives and policies and procedures in place to achieve those objectives.

ii. A business continuity plan that addresses events that have the potential to disrupt operations and a resiliency objective to ensure the institution can resume services in a reasonable timeframe.

iii. Policies and procedures for identifying risks that external parties may pose to sound operations, including interdependencies with affiliates, service providers, and others.

c. The Reserve Bank should identify actual and potential interactions between the institution's use of a Reserve Bank account and services and (other parts of) the payment system.

i. The extent to which the institution's use of a Reserve Bank account and services might restrict funds from being available to support the liquidity needs of other institutions should also be considered.

d. The institution must, in the Reserve Bank's judgment:

i. Be in sound financial condition, including maintaining adequate capital to continue as a going concern and to meet its current and projected operating expenses under a range of scenarios.

ii. Demonstrate the ability, on an ongoing basis (including during periods of idiosyncratic or market stress), to meet all of its obligations in order to remain a going concern and comply with its agreement for a Reserve Bank account and services, including by maintaining:

A. Sufficient liquid resources to meet its obligations to the Reserve Bank under applicable agreements, Operating Circulars, and Board policies;

B. The operational capacity to ensure that such liquid resources are available to satisfy all such obligations to the Reserve Bank on a timely basis; and

C. Settlement processes designed to appropriately monitor balances in its Reserve Bank account on an intraday basis, to process transactions through its account in an orderly manner and maintain/achieve a positive account balance before the end of the business day.

iii. Have in place an operational risk framework designed to ensure operational resiliency against events associated with processes, people, and systems that may impair the institution's payment system activities. This framework should consider internal and

external factors, including operational risk inherent in the institution's business model, risk that might arise in connection with its use of the payment system, and cyber-related risks. At a minimum, the framework should:

A. Identify the range of operational risks presented by the institution's business model (e.g., cyber vulnerability, operational failure, resiliency of service providers), and establish sound operational risk-management objectives;

B. Establish sound governance arrangements, rules, and procedures to oversee the operational risk management framework;

C. Establish clear and appropriate rules and procedures to carry out the risk management objectives;

D. Employ the resources necessary to achieve its risk management objectives and implement effectively its rules and procedures, including, but not limited to, sound processes for physical and information security, internal controls, compliance, program management, incident management, business continuity, audit, and well-qualified personnel.

4. Provision of an account and services to an institution should not create undue risk to the stability of the U.S. financial system.

a. The Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile.

b. The Reserve Bank should determine, in coordination with the other Reserve Banks and Board, whether the access to an account and services by an institution itself or a

group of like institutions could introduce financial stability risk to the U.S. financial system.

c. The Reserve Bank should confirm that the institution has an effective risk management framework and governance arrangements for managing liquidity, credit, and other risks that may arise in times of financial or economic stress.

d. The Reserve Bank should consider the extent to which, especially in times of financial or economic stress, liquidity or other strains at the institution may be transmitted to other segments of the financial system.

e. The Reserve Bank should consider the extent to which, especially during times of financial or economic stress, access to an account and services by an institution itself (or a group of like institutions) could affect deposit balances across U.S. financial institutions more broadly and whether any resulting movements in deposit balances could have a deleterious effect on U.S. financial stability.

i. Balances held in Reserve Bank accounts are high-quality liquid assets, making them very attractive in times of financial or economic stress. For example, in times of stress, investors that would otherwise provide short-term funding to nonfinancial firms, financial firms, and state and local governments could rapidly withdraw that funding and instead deposit their funds with an institution holding mostly central bank balances. If the institution is not subject to capital requirements similar to a federally-insured institution, the potential for sudden and significant deposit inflows into that institution is particularly large, which could disintermediate other parts of the financial system, greatly amplifying stress.

5. Provision of an account and services to an institution should not create undue risk to the overall economy by facilitating activities such as money laundering, terrorism financing, fraud, cybercrimes, or other illicit activity.

a. The Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile.

b. The Reserve Bank should confirm that the institution has an anti-money-laundering program consistent with the requirements in 31 CFR 1020.210(b) and complies with the Office of Foreign Asset Control (OFAC) regulations at 31 CFR Chapter V.

i. For these purposes, the Reserve Bank should confirm that these compliance programs contain the following elements:

A. A system of internal controls, including policies and procedures, to ensure ongoing BSA/AML and OFAC compliance, including regular written risk assessments to identify, analyze and address the risks the institution faces, policies, procedures, and an effective transaction-monitoring system;

B. Independent audit and testing of BSA/AML and OFAC compliance;

C. Senior management commitment to BSA/AML and OFAC compliance, including, at a minimum: (a) the designation of a specific person or persons responsible for managing BSA/AML and OFAC compliance, including the employment of an experienced BSA/AML and OFAC compliance officer; (b) senior management review and approval of the institution's BSA/AML and OFAC compliance programs; (c) the institution's compliance staff has sufficient authority and autonomy to deploy policies

and procedures in a manner that effectively controls the institution's BSA/AML and OFAC risk; and (d) senior management taking, and demonstrating that it will continue to take, steps to ensure that the institution's compliance unit receives adequate resources;

D. Ongoing training for appropriate personnel with a scope that is appropriate for the products and services the institution offers; and

E. Processes that allow for a risk-based classification of its customer base, including risk-based procedures for conducting ongoing customer due diligence.

6. Provision of an account and services to an institution should not adversely affect the Federal Reserve's ability to implement monetary policy.

a. The Reserve Bank should incorporate, to the extent possible, the assessments of an institution by state and/or federal supervisors into its independent assessment of the institution's risk profile.

b. The Reserve Bank should determine, in coordination with the other Reserve Banks and the Board, whether access to an account and services by an institution itself or a group of like institutions could have an effect on the implementation of monetary policy.

c. The Reserve Bank should consider, among other things, whether access to a Reserve Bank account and services by the institution could affect the level and variability of the demand for and supply of reserves, the level and volatility of key policy interest rates, the structure of key short-term funding markets, and on the overall size of the consolidated balance sheet of the Reserve Banks. The Reserve Bank should consider the implications of providing an account to the institution in normal times as well as in times

of stress. This consideration should occur regardless of the current monetary policy implementation framework in place.

III. Request for Comment

The Board requests comment on all aspects of the proposed account access guidelines, including: (1) whether the scope and application of the proposed guidance are sufficiently clear and appropriate to achieve their intended purpose; and (2) suggesting/identifying other criteria or information that commenters believe may be relevant to evaluate accounts and services requests under the proposed guidance. The Board further seeks comment specifically on the following aspects of the proposed guidance:

1. Do the proposed account access guidelines address all the risks that would be relevant to the Federal Reserve's policy goals?
2. Does the level of specificity in each principle provide sufficient clarity and transparency about how the Reserve Banks will evaluate requests?
3. Do the proposed account access guidelines support responsible financial innovation?

Finally, the Board also seeks comment on whether the Board or the Reserve Banks should consider other steps or actions to facilitate the review of requests for accounts and services in a consistent and equitable manner.

By order of the Board of Governors of the Federal Reserve System.

Ann Misback,
Secretary of the Board

11:00 a.m. – 12:00 p.m.

Legal Issues with Non-Fungible Tokens

Moderator:

James H. S. Levine, Esquire

Troutman Pepper Hamilton Sanders LLP

Panelists:

Olta Andoni, Esquire

Chief Legal Officer, Nifty's

Deborah Julie Marfurt, Chief Financial Officer

Horizon Blockchain Games Inc.

Greg Strong, Esquire

DLx Law LLP