This document is scheduled to be published in the Federal Register on 12/23/2020 and available online at **federalregister.gov/d/2020-28437**, and on **govinfo.gov**

Billing Code

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

31 CFR Parts 1010, 1020, and 1022

RIN 1506-AB47

Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

AGENCY: Financial Crimes Enforcement Network ("FinCEN"), Treasury.

ACTION: Notice of proposed rulemaking.

SUMMARY: FinCEN is issuing this notice of proposed rulemaking to seek public comments on a proposal to require banks and money service businesses ("MSBs") to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA") held in unhosted wallets (as defined below), or held in wallets hosted in a jurisdiction identified by FinCEN. FinCEN is proposing to adopt these requirements pursuant to the Bank Secrecy Act ("BSA"). To effectuate certain of these proposed requirements, FinCEN proposes to prescribe by regulation that CVC and LTDA are "monetary instruments" for purposes of the BSA. However, FinCEN is not proposing to modify the regulatory definition of "monetary instruments" or otherwise alter existing BSA regulatory requirements applicable to "monetary instruments" in FinCEN's regulations, including the existing currency transaction reporting ("CTR") requirement and the existing transportation of currency or monetary instruments reporting requirement.

DATES: Written comments on this proposed rule may be submitted on or before January 4, 2021.

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

- Federal E-rulemaking Portal: http://www.regulations.gov. Follow the instructions for

submitting comments. Refer to Docket Number FINCEN-2020-0020 and the specific RIN number 1506-AB47 the comment applies to.

- Mail: Policy Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, VA 22183. Refer to Docket Number FINCEN-2020-0020 and the specific RIN number.

FOR FURTHER INFORMATION CONTACT: The FinCEN Regulatory Support Section at 1-800-767-2825 or electronically at frc@fincen.gov.

SUPPLEMENTARY INFORMATION:

I. Executive Summary

Through this proposed rule, FinCEN is seeking to address the illicit finance threat created by one segment of the CVC market and the anticipated growth in LTDAs based on similar technological principles. FinCEN proposes to address this threat by establishing a new reporting requirement with respect to certain transactions in CVC or LTDA, that is similar to the existing currency transaction reporting requirement, and by establishing a new recordkeeping requirement for certain CVC/LTDA transactions, that is similar to the recordkeeping and travel rule regulations pertaining to funds transfers and transmittals of funds.

FinCEN is providing a 15-day period for public comments with respect to this proposed rule. FinCEN has determined that such a comment period is appropriate for several reasons.[1]

First, FinCEN assesses that there are significant national security imperatives that necessitate an efficient process for proposal and implementation of this rule. As explained further below, U.S. authorities have found that malign actors are increasingly using CVC to facilitate international terrorist financing, weapons proliferation, sanctions evasion, and transnational money laundering, as well as to buy and sell controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other

[1] Although the formal comment period concludes 15 days after filing at the Federal Register, FinCEN will endeavor to consider any material comments received after the deadline as well.

computer hacking tools, firearms, and toxic chemicals.[2] In addition, ransomware attacks and associated demands for payment, which are almost exclusively denominated in CVC, are increasing in severity,[3] and the G7 has specifically noted concern regarding ransomware attacks "in light of malicious actors targeting critical sectors amid the COVID-19 pandemic."[4]

Second, the new requirements FinCEN is proposing to adopt represent a targeted expansion of BSA reporting and recordkeeping obligations, and FinCEN has engaged with the cryptocurrency industry on multiple occasions on the AML risks presented in the cryptocurrency space and carefully considered information and feedback received from industry participants.

---

[2] *See, e.g.*, *United States. v. Cazes*, No. 1:17CR-00144, Indictment ¶ 2 (E.D. Ca. filed June 1, 2017) (alleging that "AlphaBay [was] a dark-web marketplace designed to enable users to buy and sell illegal goods, including controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals . . . AlphaBay required its users to transact in digital currencies, including Bitcoin, Monero, and Ethereum."); Dep't of the Treasury Press Release—Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence (May 13, 2019), *https://home.treasury.gov/news/press-releases/sm687*; Press Release, Dep't of Justice, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack" at pp. 1 (Mar. 2, 2020) ("North Korea continues to attack the growing worldwide ecosystem of virtual currency as a means to bypass the sanctions imposed on it by the United States and the United Nations Security Council."), *https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack*. For vulnerabilities of digital assets to securities fraud, see SEC—Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13), *https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf* (accessed June 23, 2020); CFTC—Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html (accessed Aug. 28, 2020); U.S. Dep't of Justice, "Report of the Attorney General's Cyber-Digital Task Force, Cryptocurrency: An Enforcement Framework," (Oct. 8, 2020), *https://www.justice.gov/ag/page/file/1326061/download*.

[3] In 2019, ransomware demands reached $25 billion globally, and FinCEN observed an increase in the average amount involved in ransomware incidents of $280,000 from 2018 to 2019. *See* Emsisoft, "Report: The Cost of Ransomware in 2020. A Country-by-Country Analysis" (Feb. 2020), *https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/* (accessed Dec. 1, 2020); FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (Oct. 2020), *https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf*. *See also* G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments, Ransomware Annex to G7 Statement (Oct. 13, 2020) ("[Ransomware] [a]ttacks have intensified in the last two years[.]"), *https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf*.

[4] G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments (Oct. 13, 2020), *https://home.treasury.gov/news/press-releases/sm1152*. In ransomware attacks, victims are often compelled to obtain and send CVC to an account or address designated by the perpetrator of the attack. This activity can occur through regulated financial institutions. For example, across 2017 and 2018, FinCEN observed at least seventeen separate transactions over $10,000 conducted between U.S. financial institutions and unhosted wallets affiliated with the Lazarus Group, a malign actor engaged in efforts to steal and extort CVC as a means of generating and laundering large amounts of revenue for the North Korean regime. Generally, FinCEN has observed that, following initial receipt of the funds, the perpetrator may then engage in multiple transactions between unhosted wallets before exchanging the CVC for fiat currency. *See also* Joe Tidy, "How hackers extorted $1.14m from University of California, San Francisco," (June 29, 2020), *https://www.bbc.com/news/technology-53214783* (detailing ransomware attack against COVID-19 researchers); Dep't of the Treasury Press Release—Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence (May 13, 2019), *https://home.treasury.gov/news/press-releases/sm687*.

These engagements have included a FinCEN Exchange event in May 2019, visits to cryptocurrency businesses in California in February 2020, an industry roundtable with the Secretary of the Treasury in March 2020, and a FinCEN Exchange event on cryptocurrency and ransomware in November 2020. FinCEN also has received outreach on unhosted wallets in response to anticipated FinCEN regulatory action, including letters from CoinCenter, the Blockchain Association, Blockchain.com, Global Digital Asset & Cryptocurrency Association, Circle, and the Association for Digital Asset Markets.

Third, although FinCEN is publishing this proposal in the Federal Record and invites public comment, FinCEN has noted that notice-and-comment rulemaking requirements are inapplicable because this proposal involves a foreign affairs function of the United States and because "notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest."[5] The proposal seeks to establish appropriate controls to protect United States national security from a variety of threats from foreign nations and foreign actors, including state-sponsored ransomware and cybersecurity attacks, sanctions evasion, and financing of global terrorism, among others. Furthermore, undue delay in the implementation of the proposed rule would encourage movement of unreported or unrecorded assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets, such as by moving CVC to exchanges that do not comply with AML/CFT requirements.

This section provides an overview of the relevant technology and the requirements of the proposed rule.

A. Technology Overview

CVC is a medium of exchange, such as a cryptocurrency, that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status.[6] Blockchain-

---

[5] 5 U.S.C. § 533.

[6] CVC is therefore a type of "value that substitutes for currency." *See* 31 CFR 1010.100(ff)(5)(i)(A). This definition is consistent with the recent joint notice of proposed rulemaking issued by FinCEN and the Board of Governors of the Federal Reserve in relation to the collection, recordkeeping, and transmission requirements applicable to funds transfers and transmittals of funds. *See* "Threshold for the Requirement To Collect, Retain, and

based types of CVC (*e.g.*, Bitcoin) are peer-to-peer systems that allow any two parties to transfer value directly with each other without the need for a centralized intermediary (e.g., a bank or MSB). As a technical matter, blockchain-based CVC generally consist of computers operating the network software (nodes) that enable, validate, and store transaction records on a distributed digital ledger (a blockchain). To transfer an asset on a blockchain, a person enters an alphanumeric code known only to the transferor (a private key) into a cryptographic hash function enabled by the network software, which allows the transferor to request that the network software validate a new entry on the ledger showing that control of an asset has been assigned to the recipient.[7] Once the network software has validated this transfer, the ledger is altered and the recipient may transfer the asset to another recipient using their own private key.[8] Ledger entries are cryptographically secured, and accounts are identified on a blockchain by alphanumeric "public keys"—not by the owner's name.

Some persons use the services of a financial institution to acquire or transact in CVC. For example, certain financial institutions provide custody services for their customers' CVC in so-called "hosted wallets." In such arrangements, a financial institution may execute transactions on a blockchain on behalf of a customer using a private key controlled by the financial institution. Other persons do not use the services of a financial institution, in which case they use the private key controlling the CVC to transact directly on a blockchain. Such persons may store the private key in a software program or written record, often referred to as an "unhosted wallet." Importantly, as described below, financial institutions are subject to certain BSA regulatory obligations when providing CVC-related services, including services involving

---

Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status," 85 FR 68005, 68011 (Oct. 27, 2020) ("Funds Transfer / Travel Rule NPRM").

[7] *See* Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), *https://bitcoin.org/bitcoin.pdf*; Chamber of Digital Commerce, "Legislator's Toolkit for Blockchain Technology" (Dec. 2018), *https://digitalchamber.s3.amazonaws.com/State-Working-Group-Toolkit_Final_12.4.1.pdf*.

[8] *Id.*

hosted wallets.[9] A person conducting a transaction through an unhosted wallet to purchase goods or services on their own behalf is not a money transmitter.[10]

Blockchain-based CVC networks present opportunities as well as risks. The G7 Finance Ministers and Central Bank Governors recently noted that "[t]he widespread adoption of digital payments [such as CVC] has the potential to address frictions in existing payment systems by improving access to financial services, reducing inefficiencies, and lowering costs."[11] At the same time, however, CVCs are used in illicit financial activity that presents substantial national security concerns. Depending on the features of the particular CVC and its network, a CVC's global reach can enable the rapid transfer of significant value with only anonymized or pseudonymized information about the transaction recorded, making it easier for malign actors to engage in illicit financial activity without detection or traceability.[12] Specifically, illicit finance risks involving CVC are enhanced by the capacity of users to engage with the CVC through unhosted wallets or wallets hosted by a foreign financial institution not subject to effective anti-money laundering regulation (an "otherwise covered wallet"). In such cases, there may be gaps in the recordkeeping and reporting regime with respect to financial transactions, which malign actors may seek to exploit.

Determining the true amount of illicit activity that is conducted in cryptocurrency is challenging. One industry estimate is that approximately 1% of overall market transaction volume, or $10 billion, in CVC activity conducted globally in 2019 was illicit.[13] This figure, however, may underestimate such illicit activity. Despite significant underreporting due to compliance challenges in parts of the CVC sector, in 2019, FinCEN received approximately

---

[9] Financial institutions that use unhosted wallets but that still conduct money transmission activities on behalf of third parties, such as peer-to-peer exchangers, are money transmitters. FinCEN Guidance – Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies at pp. 14-15 (May 9, 2019) ("FinCEN 2019 CVC Guidance").
[10] *Id.* at 16.
[11] G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments (Oct. 13, 2020).
[12] U.S. Dep't of Justice, "Report of the Attorney General's Cyber-Digital Task Force, Cryptocurrency: An Enforcement Framework," (Oct. 8, 2020), *https://www.justice.gov/ag/page/file/1326061/download*.
[13] *See* Chainalysis, "2020 Crypto Crime Report," (Jan. 2020), *https://go.chainalysis.com/2020-Crypto-Crime-Report.html*.

$119 billion in suspicious activity reporting associated with CVC activity taking place wholly or in substantial part in the United States.[14] By industry measures, this would equate to approximately 11.9% of total CVC market activity being relevant to a possible violation of law or regulation .[15] U.S. authorities have found that malign actors have used CVC to facilitate international terrorist financing, weapons proliferation, sanctions evasion, and transnational money laundering, as well as to buy and sell controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals.[16] In addition, ransomware attacks and associated demands for payment, which are almost exclusively denominated in CVC, have increased in severity,[17] and the G7 has specifically noted concern regarding ransomware attacks "in light of malicious actors targeting critical sectors amid the COVID-19 pandemic."[18]

---

[14] A significant majority of this $119 billion related to suspicious activity that took place before 2019 based on subsequent lookbacks. FinCEN anticipates that in the future it will receive additional suspicious activity reporting for activity that took place in 2019 but that has not yet been recognized as suspicious.

[15] FinCEN emphasizes that suspicious activity is not a clear indication of a crime but is activity that is potentially illicit. *See* 31 CFR 1020.320, 1022.320 (laying out the standards for suspicious activity).

[16] *See, e.g.*, *United States. v. Cazes*, No. 1:17CR-00144, Indictment ¶ 2 (E.D. Ca. filed June 1, 2017) (alleging that "AlphaBay [was] a dark-web marketplace designed to enable users to buy and sell illegal goods, including controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals . . . AlphaBay required its users to transact in digital currencies, including Bitcoin, Monero, and Ethereum."); Dep't of the Treasury Press Release—Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence (May 13, 2019), *https://home.treasury.gov/news/press-releases/sm687*; Press Release, Dep't of Justice, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack" at pp. 1 (Mar. 2, 2020) ("North Korea continues to attack the growing worldwide ecosystem of virtual currency as a means to bypass the sanctions imposed on it by the United States and the United Nations Security Council."), *https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack*. For vulnerabilities of digital assets to securities fraud, see SEC—Investor Alert: Ponzi Schemes Using Virtual Currencies, SEC Pub. No. 153 (7/13), *https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf* (accessed June 23, 2020); CFTC—Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html (accessed Aug. 28, 2020).

[17] In 2019, ransomware demands reached $25 billion globally, and FinCEN observed an increase in the average amount involved in ransomware incidents of $280,000 from 2018 to 2019. *See* Emsisoft, "Report: The Cost of Ransomware in 2020. A Country-by-Country Analysis" (Feb. 2020), *https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/* (accessed Dec. 1, 2020); FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (Oct. 2020), *https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf*. *See also* G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments, Ransomware Annex to G7 Statement (Oct. 13, 2020) ("[Ransomware] [a]ttacks have intensified in the last two years[.]"), *https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf*.

[18] G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments (Oct. 13, 2020), *https://home.treasury.gov/news/press-releases/sm1152*. In ransomware attacks, victims are often compelled to obtain and send CVC to an account or address designated by the perpetrator of the attack. This activity can occur through regulated financial institutions. For example, across 2017 and 2018, FinCEN observed at least seventeen

Some types of CVC pose particularly severe illicit finance challenges. Anonymity-enhanced cryptocurrency ("AEC") protocols have the effect of limiting the ability of investigators or other parties to follow transaction flows on their distributed public ledgers, unlike other types of CVC that allow a bank or MSB to identify the full transaction history of the CVC or LTDA value involved in the transaction (*i.e.* the entire transaction history of the value from the transaction block it was mined). Though relatively small in comparison to more established CVC networks, AECs have a well-documented connection to illicit activity. For example, AECs were used to launder Bitcoins paid to the wallet used in the Wannacry ransomware attack. AECs are accepted on various darknet marketplaces and the largest cryptocurrency mining malware networks continue to mine Monero, a type of AEC. Other innovations in distributed ledger technology designed to address transaction scalability, such as so-called Layer 2 solutions, together with AEC protocols represent an overall trend towards less transparency. These technology features are readily transferable to existing systems through protocol upgrades or system forks, *i.e.* the development of a new blockchain from an existing blockchain.[19]

B. Rule Overview

This proposed rule would adopt recordkeeping, verification, and reporting requirements for certain deposits, withdrawals, exchanges, or other payments or transfers of CVC or LTDA

---

separate transactions over $10,000 conducted between U.S. financial institutions and unhosted wallets affiliated with the Lazarus Group, a malign actor engaged in efforts to steal and extort CVC as a means of generating and laundering large amounts of revenue for the North Korean regime. Generally, FinCEN has observed that, following initial receipt of the funds, the perpetrator may then engage in multiple transactions between unhosted wallets before exchanging the CVC for fiat currency. *See also* Joe Tidy, "How hackers extorted $1.14m from University of California, San Francisco," (June 29, 2020), *https://www.bbc.com/news/technology-53214783* (detailing ransomware attack against COVID-19 researchers); Dep't of the Treasury Press Release—Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence (May 13, 2019), *https://home.treasury.gov/news/press-releases/sm687.*;

[19] *Cf.* Financial Action Task Force, "12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 2020) ("The ML/TF [Money Laundering/Terror Finance] risks of virtual assets are more difficult to address and mitigate once the products are launched. Their cross-border nature can present difficulties for enforcement if AML/CFT is not considered from the start. Hence, it is very important for jurisdictions to analyse and address risk in a forward-looking manner and ensure that they have all the necessary tools and authorities in place before they are needed."), *http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.*

by, through, or to a bank or MSB[20] that involve an unhosted or otherwise covered wallet. FinCEN is proposing to define otherwise covered wallets as those wallets that are held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN on a List of Foreign Jurisdictions Subject to 31 CFR § 1010.316 Reporting and 31 CFR § 1010.410(g) Recordkeeping (the "Foreign Jurisdictions List"). Initially, FinCEN is proposing that the Foreign Jurisdictions List be comprised of jurisdictions designated by FinCEN as jurisdictions of primary money laundering concern (*i.e.* Burma, Iran, and North Korea).

First, this proposed rule would require banks and MSBs to file a report with FinCEN containing certain information related to a customer's CVC or LTDA transaction and counterparty (including name and physical address), and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000 (or the transaction is one of multiple CVC transactions involving such counterparty wallets and the customer flowing through the bank or MSB within a 24-hour period that aggregate to value in or value out of greater than $10,000). Second, this proposed rule would require banks and MSBs to keep records of a customer's CVC or LTDA transaction and counterparty, including verifying the identity of their customer, if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000.

II. Background

A. Risks of Unhosted and Otherwise Covered Wallets Versus Hosted Wallets

CVC wallets are interfaces for storing and transferring CVC.[21] There are two wallet types: "hosted wallets" and "unhosted wallets." The ability to transact in CVC using unhosted or otherwise covered wallets, and the possibility that there will be a similar ability to transact in LTDA using unhosted or otherwise wallets, increases risks related to AML and combatting the

[20] FinCEN requests comment on whether to expand the requirements of the proposed rule to other types of financial institutions, such as broker-dealers.
[21] FinCEN 2019 CVC Guidance at pp. 15-16.

financing of terrorism ("CFT").

Hosted wallets are provided by account-based money transmitters that receive, store, and transmit CVC on behalf of their accountholders. Such entities generally interact with their customers through websites or mobile applications. In this business model, the money transmitter (*i.e.*, the hosted wallet provider) is the host, the account is the wallet, and the accountholder is the wallet owner. Banks can also be hosted wallet providers.[22] Money transmitters doing business in whole or substantial part in the United States, as well as banks within the United States, that are hosted wallet providers are subject to the BSA and must comply with AML/CFT program requirements, including by conducting customer due diligence with respect to accountholders and reporting suspicious activity.

By contrast, the term unhosted wallet describes when a financial institution is not required to conduct transactions from the wallet (for example, when an owner has the private key controlling the cryptocurrency wallet and uses it to execute transactions involving the wallet on the owner's own behalf). Users of unhosted wallets interact with a virtual currency system directly and have independent control over the transmission of the value. When such a person conducts a transaction to purchase goods or services on the person's own behalf, they are not a money transmitter and are not subject to BSA requirements applicable to financial institutions.[23] Additionally, because such transactions do not necessarily involve a regulated financial

---

[22] Since the FinCEN 2019 CVC Guidance, certain BSA-regulated banks have obtained authorization to custody CVC through hosted wallets. For example, on July 22, 2020, the Office of the Comptroller of the Currency ("OCC") concluded that a national bank or federal savings association may provide cryptocurrency custody services on behalf of customers (the "OCC Custody Guidance"). Office of the Comptroller of the Currency, Interpretive Letter #1170 at pp. 1, 9 (July 22, 2020), *https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf*. The OCC Custody Guidance notes that demand for cryptocurrency custody services has grown for several reasons, including that (i) access to cryptocurrency value is lost when an owner loses its cryptographic private key; (ii) banks may offer more secure storage than other existing options; and (iii) some investors may wish to manage cryptocurrency on behalf of customers and use national banks as custodians for the managed assets. *Id.* at pp. 4-5. The OCC Custody Guidance notes that as part of the custody services they provide, national banks and federal savings associations 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. *Id.* at pp. 8 n.39, 9. Similarly, some state-chartered banks are also authorized to custody CVC in hosted wallets. For example, in 2019 Wyoming created a new class of financial institutions, Special Purpose Depository Institutions, or SPDIs. *See* H.B. 74, 65th Wyo. Leg., 1st Sess. (as amended) (2019). The SPDI bank charter permits an SPDI to engage in a range of services, including custodial services and trade execution related to digital assets.

[23] FinCEN 2019 CVC Guidance at pp. 16.

intermediary on at least one side of the transaction, they may never be scrutinized pursuant to any AML/CFT program.

The Treasury Department has previously noted that "[a]nonymity in transactions and funds transfers is the main risk that facilitates money laundering."[24] The Financial Action Task Force ("FATF")[25] has similarly observed that the extent to which anonymous peer-to-peer permit transactions via unhosted wallets, without involvement of a virtual asset service provider or a financial institution, is a key potential AML/CFT risk in some CVC systems.[26] FATF members have specifically observed that unregulated peer-to-peer transactions "could present a leak in tracing illicit flows of virtual assets," particularly if one or more blockchain-based CVC networks were to reach global scale.[27] Importantly, as explained below, while data contained on some blockchains are open to public inspection and can be used by authorities to attempt to trace illicit activity, FinCEN believes that this data does not sufficiently mitigate the risks of unhosted and otherwise covered wallets.[28]

---

[24] Dep't of the Treasury, National Money Laundering Risk Assessment at pp. 4 (2018), *https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf*.

[25] The FATF is an international, inter-governmental task force whose purpose is the development and promotion of international standards and the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, the financing of proliferation, and other related threats to the integrity of the international financial system.

[26] FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins at pp. 15 (June 2020), *https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf*.

[27] 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers at pp. 15 (June 2020), *https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf*. The FATF has also encouraged government authorities to address potential risks posed by disintermediated (*i.e.*, peer-to-peer) transactions in a proactive manner, as they deem appropriate. *Id*. at pp. 7. The FATF noted that jurisdictions have a range of national-level tools to mitigate, to some extent, the risks posed by anonymous peer-to-peer transactions if national authorities consider the ML/TF risk to be unacceptably high. This includes banning or denying licensing of platforms if they allow unhosted wallet transfers, introducing transactional or volume limits on peer-to-peer transactions, or mandating that transactions occur with the use of a VASP or financial institutions. *Id.* at pp. 15.

[28] The risk profile of wallets hosted by foreign financial institutions located in certain jurisdictions that do not have an effective AML regime resembles the risk profile of unhosted wallets. The reason transactions involving hosted wallets present lower illicit finance risk in jurisdictions with an effective AML regime is because of the role that intermediaries in such jurisdictions play in preventing money laundering by applying a variety of controls, such as due diligence, transaction monitoring, and suspicious activity reporting. Financial institutions subject to effective regulation are also obligated to cooperate with lawful investigations. In jurisdictions in which financial institutions are allowed to turn a blind eye to, or even purposefully facilitate, money laundering, there is no basis to conclude that intermediation reduces illicit finance risk. The reporting, recordkeeping, and verification requirements of this proposed rule would apply to transactions with wallets hosted in jurisdictions listed on the Foreign Jurisdictions List.

B. Limitations of Current Tools to Mitigate the AML/CFT Risks of CVC

In certain circumstances, investigators may be able to analyze blockchain data to identify illicit activity.[29] While such analytic techniques can be used to combat illicit finance, they are not a panacea. Blockchain analysis can be rendered less effective by a number of factors, including the scale of a blockchain network, the extent of peer-to-peer activity (*i.e.*, transactions between unhosted wallets), the use of anonymizing technologies to obscure transaction information, and a lack of information concerning the identity of transferors and recipients in particular transactions. Additionally, several types of AEC (*e.g.*, Monero, Zcash, Dash, Komodo, and Beam) are increasing in popularity and employ various technologies that inhibit investigators' ability both to identify transaction activity using blockchain data and to attribute this activity to illicit activity conducted by natural persons.[30]

Regulations under the BSA already require filing CTRs for transactions involving or aggregating to more than $10,000 in currency or monetary instruments as defined in 31 CFR 1010.100(dd). Such CTRs provide valuable information that helps investigators identify bulk cash smuggling, structuring, and other large-scale money laundering efforts, among other activity, even when the customer is not complicit in the overall money laundering scheme.[31] This proposed rule would similarly provide greater insight into transacting parties with a nexus to one or more potentially illicit transactions:

- First, the proposed rule would require that banks and MSBs identify and verify hosted wallet customers who engage in transactions with unhosted or otherwise covered wallet counterparties when those customers conduct transactions above the equivalent of $3,000 in CVC or LTDA with an unhosted or otherwise covered wallet counterparty (with

[29] D. Y. Huang et al., "Tracking Ransomware End-to-end," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 618-631, doi: 10.1109/SP.2018.00047.
[30] *See* "What is Monero (XMR)?" *https://web.getmonero.org/get-started/what-is-monero/* (accessed Dec. 1, 2020).
[31] Other types of reports required under the BSA, including suspicious activity reports, are also critical to law enforcement. The reporting requirements of this proposed rule are a virtual currency analogue to the CTR reporting requirement.

reporting required for transactions over $10,000), and that banks and MSBs collect certain information (*i.e.* name and physical address) concerning the customer's counterparties.[32]

- Second, the proposed rule would cause banks and MSBs to generate reports containing the transaction hash and identity of persons holding wallets engaging with unhosted or otherwise covered wallets engaging in transactions across multiple financial institutions.
- Third, the proposed rule would create a new prohibition on structuring—*i.e.*, engaging in transactions in a manner to avoid reporting requirement—applicable to virtual currency transactions. Structuring is a method used by some malign actors to avoid detection by law enforcement of their illicit activities.

In this notice, FinCEN is seeking comment on the potential effects of this proposed rule on activity through financial intermediaries that are subject to the BSA or to AML/CFT regulations in a foreign jurisdiction.

C. Legal Framework

1. The Bank Secrecy Act

The Currency and Foreign Transactions Reporting Act of 1970, as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") (Public Law 107-56) and other legislation, is the legislative framework commonly referred to as the BSA. The Secretary of the Treasury ("Secretary") has delegated to the Director of FinCEN ("Director") the authority to implement, administer, and enforce compliance with the BSA and associated regulations.[33]

Pursuant to this authority, FinCEN may require financial institutions to keep records and

---

[32] FinCEN recognizes that persons engaged in illicit finance will likely attempt to use falsified credentials and other types of schemes to evade the requirement to report their true identities. However, banks and MSBs develop solutions to try to ferret out such abuse, not only for AML purposes but also to avoid being defrauded by illicit actors themselves. Furthermore, such efforts can generate valuable leads through suspicious activity reports.
[33] Treasury Order 180-01 (Jan. 14, 2020)

file reports that the Director determines have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in intelligence or counterintelligence matters to protect against international terrorism.[34] Regulations implementing Title II of the BSA appear at 31 CFR chapter X.[35]

Specifically, under 12 U.S.C. 1829b(b)(1), where the Secretary determines that the maintenance of appropriate types of records and other evidence by insured depository institutions has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, the Secretary has the authority to prescribe regulations to carry out the purposes of this section. Similarly, under 12 U.S.C. 1953, the Secretary is authorized to promulgate recordkeeping requirements for uninsured banks and uninsured financial institutions, to include MSBs.

Under 31 U.S.C. 5313, the Secretary is authorized to require financial institutions to report currency transactions, or transactions involving other monetary instruments as the Secretary prescribes. These reports may be required on transactions in an amount, denomination, or amount and denomination, or under circumstances the Secretary prescribes by regulation. Reports must be filed at the time and in the way the Secretary prescribes. The BSA defines the term "monetary instruments" to include, among other things, "United States coins and currency . . . [and] as the Secretary may prescribe by regulation, coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which title is passed on delivery, and similar material . . . ."[36] The term "monetary instruments" is also defined for the purposes of FinCEN's regulations in 31 CFR chapter X at 31 CFR 1010.100(dd).[37]

Under 31 U.S.C. 5318(a)(2), the general powers of the Secretary pursuant to the BSA

---

[34] 31 U.S.C. 5311.
[35] Treasury Order 180-01 (Jan. 14, 2020)
[36] 31 U.S.C. 5312(a)(3).
[37] This proposed rule would not modify the regulatory definition of "monetary instruments" at 31 CFR 1010.100(dd), although it would prescribe that CVC and LTDA are "monetary instruments" pursuant to 31 U.S.C. 5313 for the purposes of the issuance of the proposed reporting requirement added at 31 CFR 1010.316.

include the ability to require a class of domestic financial institutions to "maintain appropriate procedures to ensure compliance with [subchapter 53 of title 31 of the U.S. Code] and regulations prescribed under [such] subchapter or to guard against money laundering."[38]

2. Implementation of the BSA with Respect to Persons Dealing in CVC

Under FinCEN's regulations found at 31 CFR chapter X, banks and MSBs are subject to a number of requirements under the BSA, including requirements to maintain an AML/CFT program and to report suspicious activity to FinCEN.[39] Specifically, banks and MSBs are required to have an AML/CFT program that includes, at a minimum, (1) internal controls to assure ongoing compliance; (2) independent testing for compliance to be conducted by internal personnel or by an outside party; (3) designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) training and education for appropriate personnel.[40] Banks are also required to maintain appropriate risk-based procedures for conducting customer due diligence and a customer identification program ("CIP") as part of their AML/CFT program.[41] The BSA and its implementing regulations also require banks and MSBs to file CTRs and suspicious activity reports ("SARs"). Financial institutions are required to file SARs to report any transaction that the financial institution "knows, suspects, or has reason to suspect" is suspicious, if the transaction is conducted or attempted by, at, or through the institution, and the transaction involves or aggregates to at least $5,000 in funds or other assets in the case of banks, and at least $2,000 in funds or other assets in the case of MSBs.[42]

Many of the BSA requirements that apply to banks and MSBs are applicable to their transactions in CVC or LTDA.[43] For instance, financial institutions are required to address the

---

[38] The proposed rule relies on authority under 31 U.S.C. 5313 and 5318(a)(2) to extend several existing requirements that apply to the current requirement to file currency transaction reports to the new requirement to file transaction reports related to transactions in CVC or LTDA. It also relies on the authority of 31 U.S.C. 5318(a)(2) for the promulgation of the recordkeeping requirements on wallets held by foreign financial institutions in jurisdictions identified by FinCEN.
[39] *See, e.g.*, 31 CFR 1020.210, 1020.320, 1022.210, 1022.320.
[40] 31 CFR 1020.210, 1022.210.
[41] 31 CFR 1020.210(b)(5), 1020.220, 1022.210(d)(1).
[42] 31 CFR 1020.320, 1022.320.
[43] FinCEN guidance makes clear that CVC is a type of "value that substitutes for currency." *See, e.g.*, FinCEN

risks of such transactions as part of their AML/CFT programs, file CTRs where appropriate (such as where a person uses a reportable amount of currency to purchase CVC or LTDA), and report suspicious activity related to such transactions to FinCEN.

FinCEN's guidance also states that financial institutions are subject to the collection, recordkeeping, and transmittal requirements applicable to transmittals of funds with respect to transactions in CVC or LTDA.[44] A notice of proposed rulemaking recently published by FinCEN and the Board of Governors of the Federal Reserve System proposes regulatory amendments to these same rules to clarify that they apply to transactions in CVC or LTDA, and also to lower the monetary threshold triggering the rules for certain transactions (the "Funds Transfer / Funds Travel Rule NPRM").[45] Under the collection and recordkeeping aspect of these rules, banks and nonbank financial institutions are required to collect and retain information related to transmittals of funds in amounts of $3,000 or more.[46] Furthermore, the transmittal aspect of these rules requires financial institutions to transmit certain information required to be collected by the funds recordkeeping rule to other banks or nonbank financial institutions participating in the transmittal.[47]

3. CTR Reporting Obligations

The existing regulations that implement the CTR reporting requirement are found at several sections of 31 CFR chapter X. The basic reporting requirement is found at 31 CFR 1010.311, and applies generally to all financial institutions as defined by FinCEN's regulations. Individual regulatory parts also refer back to 31 CFR 1010.311, such as in the regulatory parts

---

Guidance – Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies at pp. 3-5 (Mar. 18, 2013) ("FinCEN 2013 CVC Guidance"); FinCEN 2019 CVC Guidance at pp. 7. While LTDA does, by definition, have legal tender status, it does not meet the definition of currency in 31 CFR 1010.100 as it is not coin or paper money. Thus, like CVC, LTDA is also value that substitutes for currency.

[44] *See* FinCEN 2019 CVC Guidance at pp. 11-12.

[45] Funds Transfer / Travel Rule NPRM at pp. 68005-06.

[46] *See* 31 CFR 1010.410(e) (non-bank financial institutions); 31 CFR 1020.410(a) (banks). Among the information that must be collected and retained is (a) name and address of the transmittor; (b) the amount of the transmittal order; (c) the execution date of the transmittal order; (d) any payment instructions received from the transmittor with the transmittal order; and (e) the identity of recipient's financial institution.

[47] *See* 31 CFR 1010.410(f).

that apply to banks and MSBs.[48] Timing, procedural, and recordkeeping requirements related to the CTR reporting requirement are found at 31 CFR 1010.306(a)(1)-(3) and (d)-(e). Identification verification and recordkeeping requirements applicable to transactions requiring a CTR are found at 31 CFR 1010.312 and are referenced in other regulatory parts.[49] Aggregation requirements that require financial institutions to aggregate across multiple branches and transactions for the purposes of determining whether the CTR reporting requirement's monetary threshold is satisfied are found at 31 CFR 1010.313 and are referenced in other regulatory parts.[50] Anti-structuring rules that apply to transactions in currency reporting requirements are found at 31 CFR 1010.314 and are referenced in other regulatory parts.[51] An exemption that applies to non-bank financial institutions obligations under the CTR reporting requirement is found at 31 CFR 1010.315 and is also referenced in other regulatory parts.[52] Finally, banks are subject to specific statutory exemptions from the CTR reporting requirement as incorporated into FinCEN's regulations at 31 CFR 1020.315; the mandatory and discretionary statutory exemptions these regulations implement are found at 31 U.S.C. 5313(d) and (e), respectively.

III. Proposed Reporting Requirement for Transactions Involving CVC or LTDA

A. Expansion of the BSA Definition of "Monetary Instruments"

This proposed rule would add a determination at 31 CFR 1010.316(a), a new section this proposed rule would add, that CVC and LTDA are "monetary instruments" for the purposes of 31 U.S.C. 5313. Section 5313 authorizes the Secretary to issue reporting requirements in relation to "transactions for the payment, receipt, or transfer of United States coins or currency (*or other monetary instruments the Secretary of the Treasury prescribes*)" (emphasis added). The BSA defines "monetary instruments" to include, among other things, "United States coins and currency" and "as the Secretary may prescribe by regulation, coins and currency of a foreign

---

[48] *See, e.g.*, 31 CFR 1020.311, 1022.311.
[49] *See, e.g.*, 31 CFR 1020.312, 1022.312.
[50] *See, e.g.*, 31 CFR 1020.313, 1022.313.
[51] *See, e.g.*, 31 CFR 1020.314, 1022.314.
[52] *See, e.g.*, 31 CFR 1022.315.

country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which title is passed on delivery, and similar material[.]"[53]

CVC and LTDA are "similar material" to "coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, [and] stock on which title is passed on delivery . . . . "[54] The six specific instruments included in 31 U.S.C. 5312(a)(3)(B) each represent material that can serve as a substitute for U.S. coins and currency, or in other words, function as money. Like currency itself, negotiable instruments and instruments in bearer form are commodified so that they can serve monetary functions, such as by acting as a medium of exchange, a store of value, or a unit of account. CVC similarly functions as a commodified unit of exchange and a substitute for coins and currency.

For purposes of the BSA, a salient characteristic shared by the six specific instruments included in 31 U.S.C. 5312(a)(3)(B) is not the right to an underlying asset, but rather that title to the asset passes upon delivery, that is, whoever possess the instrument is considered its owner.[55] With respect to CVC and LTDA, the holder of the private key related to any such CVC or LTDA has control over that CVC or LTDA. That private key grants the holder the ability and blockchain-based authority to transfer the CVC or LTDA.[56] In essence, ownership of CVC and LTDA passes upon delivery similar to the instruments described in 31 U.S.C. 5312(a)(3)(B).

As the note to the proposed determination at 31 CFR 1010.316(a) makes clear, however, that proposed determination is *not* intended to affect the regulatory definition of "monetary instruments" at 31 CFR 1010.100(dd), or the use of that regulatory definition elsewhere in FinCEN's regulations, including in relation to the CTR reporting requirement at 31 CFR 1010.311 and the transportation of currency or monetary instruments reporting requirement

---

[53] 31 U.S.C. 5312(a)(3).
[54] 31 U.S.C. 5312(a)(3)(B).
[55] Some CVCs, such as stablecoins, may be redeemable for an underlying asset.
[56] *See, e.g.*, Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, *available at* https://bitcoin.org/bitcoin.pdf ("Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.") (accessed December 5, 2020).

at 31 CFR 1010.340.[57]

B. Scope of the Reporting Requirement

The proposed reporting requirement would apply to transactions involving CVC or LTDA between a bank's or MSB's hosted wallet customer and an unhosted or otherwise covered wallet. This proposed rule would apply an aggregation requirement, similar to the CTR aggregation requirement, to the proposed reporting requirement for transactions involving CVC or LTDA. However, only CVC or LTDA transactions would need to be aggregated together for the purposes of the proposed reporting requirement; a report would not be required when the total value of a person's CVC or LTDA transactions plus the person's currency transactions in a 24-hour period is greater than $10,000 in value, as determined by the financial institution based on the value at the time of each transaction, but the total value of the person's CVC or LTDA transactions alone is not greater than $10,000 in value, as determined by the financial institution based on the value at the time of each transaction.[58]

FinCEN is proposing an exemption to the reporting requirement that would make this requirement inapplicable to transactions between hosted wallets held at financial institutions subject to the BSA. FinCEN is also proposing to extend this exemption to CVC or LTDA transactions where the counterparty wallet is hosted by a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the Foreign Jurisdictions List, which FinCEN is proposing to establish. Initially, the Foreign Jurisdictions List would be comprised of jurisdictions designated by FinCEN as jurisdictions of primary money laundering concern (*i.e.* Burma, Iran, and North Korea), but could in the future be expanded to include jurisdictions that

---

[57] Nor is this proposed regulatory determination intended to have any impact on the definition of "currency" in 31 CFR 1010.100(m). Furthermore, nothing in this proposal is intended to constitute a determination that any CVC or LTDA that is within the regulatory definition of "monetary instruments" at 31 U.S.C. 5312(a)(3) is currency for the purposes of the federal securities laws, 15 U.S.C. 78c(47), or the federal derivatives laws, 7 U.S.C. 1-26, and the regulations promulgated thereunder.

[58] As noted previously, the changes this proposed rule would make are not intended to modify the CTR reporting requirement. Consistent with this intention, the proposed rule would make no change to the CTR aggregation requirements; the value of a person's CVC or LTDA transactions is not relevant to the determination of whether the person's currency transactions in aggregate require the filing of a CTR.

are identified to have significant deficiencies in their regulation of CVC or LTDA such that the application of this proposed rule's recordkeeping and reporting requirements would be appropriate.

C. Comparison to the CTR Reporting Requirements and Consideration of Extension of Current CTR Exemptions to the Proposed CVC/LTDA Transaction Reporting Requirement

Similar to the CTR reporting requirement, this proposed rule would require reporting of transactions in CVC or LTDA that aggregate to greater than $10,000 in one day. Substantive exemptions to the CTR reporting requirement can be found at 31 CFR 1010.315 and 1020.315. The exemption at 31 CFR 1010.315 exempts a non-bank financial institution (including an MSB) from the obligation to file a report otherwise required by 31 CFR 1010.311 with respect to a transaction in currency between the institution and a commercial bank. This proposed rule would not extend this exemption to the reporting requirement proposed to be added at 31 CFR 1010.316(b) related to CVC/LTDA transactions between a bank's or MSB's hosted wallet customer and an unhosted or otherwise covered wallet. FinCEN is not proposing extending this exemption because unhosted and otherwise covered wallets would generally not involve a U.S. commercial bank. FinCEN has requested comment, however, on whether these exemptions should be extended with respect to the proposed CVC/LTDA transaction reporting requirement.

The current exemptions to the CTR reporting requirement for banks at 31 CFR 1020.315 are based in the mandatory and discretionary statutory exemptions to reporting requirements imposed on banks pursuant to 31 U.S.C. 5313(d) and (e), respectively. The two sections below consider those exemptions in turn.

1. Application of Mandatory Exemptions to 31 U.S.C. 5313 Reporting Requirements to the Proposed CVC/LTDA Transaction Reporting Requirement

31 U.S.C. 5313(d) mandates that the Secretary exempt "depository institutions"—which include the banks on which the proposed CVC/LTDA transaction reporting requirement would

be imposed—from reporting requirements imposed pursuant to 31 U.S.C. 5313(a) with respect to transactions between the depository institution and: (a) another depository institution; (b) a department or agency of the United States, any State, or any political subdivision of any State; (c) any entity established under the laws of the United States, any State, or any political subdivision of any State, or under an interstate compact between two or more States, which exercises governmental authority on behalf of the United States or any such State or political subdivision; or (d) any business or category of business the reports on which have little or no value for law enforcement purposes.

FinCEN believes these mandatory statutory exemptions are likely to be of limited practical relevance with respect to the proposed reporting requirement because of the limited likelihood that the types of institutions covered by these mandatory statutory exemptions would maintain unhosted or otherwise covered wallets. Nevertheless, FinCEN is proposing to apply the mandatory statutory exemptions to the proposed CVC/LTDA transaction reporting requirement. At this time, however, FinCEN is not proposing to determine that there is any business or category of business for which the reports on CVC or LTDA would have little or no value for law enforcement purposes.[59]

2. Consideration of Applying the Discretionary Exemptions to 31 U.S.C. 5313 Reporting Requirements to the Proposed CVC/LTDA Transaction Reporting Requirement

31 U.S.C. 5313(e) states that the Secretary may exempt a depository institution from the reporting requirements of subsection (a) with respect to transactions between the depository institution and a qualified business customer of the institution on the basis of information submitted to the Secretary by the institution in accordance with procedures which the Secretary

[59] FinCEN is therefore not extending the exemptions at 31 CFR 1020.315(b)(4)-(5) to the proposed CVC/LTDA transaction reporting requirement. 31 CFR 1020.315(b)(4)-(5) were promulgated to implement the mandatory reporting exemptions of 31 U.S.C. 5313(d) with respect to transactions in currency. "Amendment to the Bank Secrecy Act Regulations—Exemptions From the Requirement To Report Transactions in Currency" 62 FR 47141, 47142 (Sept. 8, 1997).

shall establish. FinCEN's regulations incorporate this provision by including as "exempt persons" two categories of entities that are not within the mandatory exemptions of 31 U.S.C. 5313(d),[60] and then requiring that banks file a notice to FinCEN with respect to such persons prior to applying the exemption to discontinue the filing of CTRs.[61]

The discretionary exemptions that FinCEN has adopted relate to U.S. businesses with transaction accounts that frequently engage in transactions greater than $10,000, and certain payroll account customers.[62] Neither of these discretionary categories appear likely to be counterparties to transactions between banks' hosted wallet customers and unhosted or otherwise covered wallets. Therefore, FinCEN is not proposing to extend these provisions to the proposed CVC/LTDA transaction reporting requirement. FinCEN has requested comment on the exemptions it should apply.

IV. Proposed Recordkeeping, Verification, and Other Procedural Requirements on Transactions Involving CVC or LTDA

A. Recordkeeping, Verification, and Other Procedural Requirements Related to the Proposed CVC/LTDA Transaction Reporting Requirement

As noted above in Section II.C.3, the basic CTR reporting requirement at 31 CFR 1010.311 is complemented by identification verification, recordkeeping, and procedural requirements, and other provisions found in other sections of 31 CFR chapter X. In particular, with respect to transactions for which a CTR must be filed, financial institutions must comply with the following related requirements:

- Pursuant to 31 CFR 1010.312, financial institutions must verify and record the identity of the individual presenting the transaction, as well as record the identity, account number, and the social security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected. The regulation also lays out

[60] *See* 31 CFR 1020.315(b)(6)-(7).
[61] *See* 31 CFR 1020.315(c)(1).
[62] *See* 31 CFR 1020.315(b)(6)-(7).

specific requirements for verification.

- Pursuant to 31 CFR 1010.306(a)(1), a CTR must be filed within 15 days following the date of the reportable transaction.
- Pursuant to 31 CFR 1010.306(a)(2), a CTR must be retained for five years from the date of the report.
- Pursuant to 31 CFR 1010.306(a)(3), a CTR must be filed with FinCEN, unless otherwise specified.
- Pursuant to 31 CFR 1010.306(d), a CTR must be filed on a form prescribed by the Secretary. Pursuant to 31 CFR 1010.306(e), the CTR form may be obtained from the BSA E-Filing System.
- Pursuant to 31 CFR 1010.314, structuring transactions to evade the CTR reporting requirement is prohibited.

This proposed rule would amend these requirements. Specifically, the procedural and anti-structuring rules are proposed to be amended in a straightforward manner by adding to their scope the proposed reporting requirement at 31 CFR 1010.316. The identity verification and recordkeeping requirements are proposed to be amended to apply a new verification requirement to a financial institution's hosted wallet customer, and to require the collection of the name and physical address of the customer's counterparty, when engaging in a transaction reportable pursuant to the proposed CVC/LTDA transaction reporting requirement.

B. Recordkeeping and Verification Requirements Distinct From the Proposed CVC/LTDA Transaction Reporting Requirement

This proposed rule would add a new recordkeeping requirement at 31 CFR 1010.410(g) requiring banks and MSBs to keep records and verify the identity of their hosted wallet customers, when those customers engage in transactions with unhosted or otherwise covered wallets with a value of more than $3,000. With respect to the verification requirement for recordkeeping, the proposed rule would allow for methods analogous to those permitted for

verification of hosted wallet customers in relation to transactions subject to the proposed CVC/LTDA transaction reporting requirement. The proposed recordkeeping requirement would not apply to transactions between hosted wallets (except for otherwise covered wallets).

FinCEN is proposing to establish this recordkeeping and verification requirement pursuant to 12 U.S.C. 1829b(b)(1) and 12 U.S.C. 1953, which authorize the Secretary to adopt recordkeeping requirements for banks and MSBs that have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, as well as 31 U.S.C. 5318(a), which authorizes the Secretary to require domestic banks and MSBs to maintain appropriate procedures to ensure compliance with subchapter 53 of title 31 of the U.S. Code and regulations prescribed thereunder or to guard against money laundering. As a result, the statutory exemptions of 31 U.S.C. 5313 covering transactions between depository institutions and certain other entities do not apply to these proposed requirements.

V. Section-by-Section Analysis

A. Expansion of the Definition of "Monetary Instruments"

As described in Section III.B, the proposed rule would add a new provision at 31 CFR 1010.316(a) that includes a determination that CVC and LTDA are "monetary instruments" for the purposes of 31 U.S.C. 5313. This determination provides a basis for the proposed CVC/LTDA transaction reporting requirement proposed to be added at 31 CFR 1010.316(b).[63]

This proposed determination is *not* intended to impact the regulatory definition of "monetary instruments" at 31 CFR 1010.100(dd), nor that regulatory definition's use elsewhere in FinCEN's regulations, including in relation to the currency transaction reporting requirement at 31 CFR 1010.311, and the transportation of currency or monetary instruments reporting requirement at 31 CFR 1010.340.

---

[63] 31 CFR 1010.316(c) provides definitions for CVC and LTDA. As noted previously, CVC is defined consistently with the proposed definition in FinCEN and the Board of Governors of the Federal Reserve Board's recent Funds Transfer / Travel Rule NPRM. *See* 85 FR 68005, 68011 (Oct. 27, 2020). LTDA is defined for the first time to be any type of digital asset issued by the United States or any other country that is designated as legal tender by the issuing country and accepted as a medium of exchange in the country of issuance.

B. Reporting Requirements on CVC and LTDA Transactions with Unhosted or Otherwise Covered Wallets

This notice proposes a new reporting requirement at 31 CFR 1010.316(b). This would require banks and MSBs to file a report similar to the CTR for transactions between their customers' CVC or LTDA hosted wallets and unhosted or otherwise covered wallets, either as senders or recipients. This reporting requirement would apply even if the user of the unhosted or otherwise covered wallet is the customer for which the financial institution holds a hosted wallet.

To maintain consistency with the CTR form, this proposed rule would require CVC and LTDA transaction reporting at a threshold of $10,000 in value, as determined by the financial institution based on the prevailing exchange rate at the time of the transaction.[64] FinCEN plans to issue a reporting form similar to but distinct from the CTR reporting form that will require the reporting of information on the filer, transaction, hosted wallet customer, and each counterparty.

The proposed rule would add aggregation requirements similar to those that apply to the requirement to file CTRs. Specifically, the proposed aggregation provision at 31 CFR 1010.313(c) would require that banks and MSBs, in calculating whether the $10,000 threshold has been met, treat multiple CVC and LTDA transactions as a single transaction if the bank or MSB has knowledge that they are by or on behalf of any person and result in value in or value out of CVC or LTDA above the threshold of $10,000 during a 24-hour period. This 24-hour period begins from the first unreported transaction.[65] The aggregation provisions would not require that CVC/LTDA transactions be aggregated with currency

---

[64] The term "prevailing exchange rate" means a rate reasonably reflective of a fair market rate of exchange available to the public for the CVC/LTDA at the time of the transaction. Financial institutions would be required to document their method for determining the prevailing exchange rate.

[65] For example, if three $6,000 transactions with unhosted wallets are initiated by a MSB's hosted wallet customer at 7:00 a.m. on Tuesday, 7:00 p.m. on Tuesday, and 8:00 a.m. on Wednesday, then the first two transactions would be reported, consistent with the aggregation requirement, but not the third transaction. However, the third transaction would be subsequently reported, consistent with the aggregation requirement, if there were additional transactions with unhosted or otherwise covered wallets before 8:00 a.m. on Thursday totaling more than $4,000 in value.

transactions for the purposes of either the CTR reporting requirement threshold or the CVC/LTDA transaction reporting requirement threshold.

Because a bank or MSB may provide CVC or LTDA hosting through distinct corporate structures and from different physical locations than it provides traditional financial services, proposed 31 CFR 1010.313(c) makes clear that, for purposes of aggregation with respect to the CVC/LTDA transaction reporting requirement, a bank or MSB must include all of its offices and records, wherever they may be located. Additionally, under this proposed rule, foreign-located MSBs must comply with the proposed CVC/LTDA transaction reporting requirement, and this related aggregation requirement, with respect to their activities in the United States.[66]

With respect to counterparty information that would be required to be reported pursuant to 31 CFR 1010.316(b), the proposed rule would require the reporting of certain identifying information including, at a minimum, the name and physical address of each counterparty. Consistent with their AML/CFT programs, under the proposed rule, banks and MSBs would continue to follow risk-based procedures to determine whether to obtain additional information about their customer's counterparties or take steps to confirm the accuracy of counterparty information.

The proposed 31 CFR 1010.316 would exempt from required reporting those transactions that are between a filer's hosted wallet customer and a counterparty hosted wallet at a financial institution that is either regulated under the BSA or located in a foreign jurisdiction that is not on the Foreign Jurisdictions List. As proposed, prior to applying the exemption at 31 CFR 1010.316(d), banks and MSBs would need to have a reasonable basis to determine that a counterparty wallet is a hosted wallet at either a BSA-regulated financial institution or a foreign financial institution in a jurisdiction that is not on the Foreign

---

[66] *Cf.* FinCEN Advisory, FIN-2012-A001, "Foreign-Located Money Services Businesses" (Feb. 2012), *https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A001.pdf.*

Jurisdictions List. For example, in analyzing whether a counterparty's wallet is hosted by a BSA-regulated MSB, financial institutions would need to ensure that the MSB is registered with FinCEN. In making a determination of the applicability of the exemption to a wallet hosted by a foreign financial institution, banks and MSBs would need to confirm that the foreign financial institution is not located in a jurisdiction on the Foreign Jurisdictions List, and would need to apply reasonable, risk-based, documented procedures to confirm that the foreign financial institution is complying with registration or similar requirements that apply to financial institutions in the foreign jurisdiction.

As discussed in Section III.D, FinCEN also proposes amending 31 CFR 1020.315 to apply the mandatory statutory exemptions to the reporting requirements imposed pursuant to 31 U.S.C. 5313(a) to the proposed CVC/LTDA transaction reporting requirement to be added at 31 CFR 1010.316(b). However, as discussed in Section III.D, FinCEN is not proposing to conclude that there is any business or category of business the reports on which have little or no value for law enforcement purposes under the proposed CVC/LTDA transaction reporting requirement. Therefore, FinCEN is not proposing to extend the regulatory exceptions related to public companies and their subsidiaries that have been applied to such entities with respect to currency transactions pursuant to 31 CFR 1020.315(b)(4)-(5). Further, FinCEN is not proposing applying the discretionary statutory exemptions to further limit the scope of the proposed CVC/LTDA transaction reporting requirement. FinCEN is continuing to consider these issues and has sought comments on whether it should apply these exemptions differently.

Because FinCEN has only proposed extending the exemption under 31 CFR 1020.315 to entities subject to the mandatory statutory exemption listed in 31 CFR 1020.315(b)(1)-(3), FinCEN is not proposing to require a bank to file FinCEN Form 110 or a similar form in relation to such exempt persons in order to take advantage of the exemption. This is consistent with the existing special rule at 31 CFR 1020.315(c)(2)(B) for transactions

in currency.

In some instances, CVC/LTDA transactions may involve multiple senders and recipients. As reflected in the proposed exemption language at 31 CFR 1010.316(d), a transaction where any one participating wallet is unhosted or otherwise covered would be subject to the proposed CVC/LTDA transaction reporting requirement. Therefore, banks and MSBs would be required to report, keep records, and engage in verification with respect to such transactions, if the aggregate amount of CVC/LTDA transactions involving unhosted or otherwise covered wallets, either sent or received from their customer's account, exceeds $10,000 in value within a 24-hour period.

C. Recordkeeping and Verification Requirements Related to the Transaction Reporting Requirement for CVC and LTDA Transactions with Unhosted or Otherwise Covered Wallets

As described in Section IV, the proposed rule would also extend to the new CVC/LTDA transaction reporting requirement provisions analogous to the identity verification, recordkeeping, and procedural requirements, and the anti-structuring rule, that apply to the CTR reporting requirement.

1. Identity Verification and Recordkeeping Requirements

The identity verification and recordkeeping requirements applicable to transactions that require the filing of a CTR are found at 31 CFR 1010.312. The proposed rule would amend this provision by adding a requirement at 31 CFR 1010.312(b) that banks and MSBs verify and keep records of their hosted wallet customers who engage in a transaction with unhosted or otherwise covered wallet counterparties. Specifically, banks and MSBs would be required to verify and record the identity of their customer engaged in a reportable transaction.[67] Under the proposed rule, in the case of a transaction in which the bank's or

[67] Pursuant to the note to 31 CFR 1010.312(b), this includes verifying the identity of the person accessing the customer's account, which may be someone conducting a transaction on the customer's behalf.

MSB's customer is the sender and the bank or MSB is aware at the time of the transaction that reporting is required pursuant to 31 CFR 1010.316 or 1010.313(c) (where the reporting requirement applies based on aggregation), the bank or MSB should not complete the transmission of funds until such recordkeeping and verification is complete. Similarly, in the case of a transaction in which the bank's or MSB's customer is the recipient, the bank or MSB would need to obtain the required recordkeeping and verification information as soon as practicable. In addition, under the proposed rule, banks and MSBs would be expected to incorporate policies tailored to their respective business models should the bank or MSB be unable to obtain the required information, such as by terminating its customer's account in appropriate circumstances.

FinCEN recognizes that verification of identity in the CTR context generally involves transactions in currency that are physically presented, in contrast to the CVC and LTDA transactions that are subject to the proposed CVC/LTDA transaction reporting requirement, for which this is often not the case. Accordingly, under the proposed rule, consistent with the bank's or MSB's AML/CFT program, the bank or MSB would need to establish risk-based procedures for verifying their hosted wallet customer's identity that are sufficient to enable the bank or MSB to form a reasonable belief that it knows the true identity of its customer. These procedures would be based on the bank's or MSB's assessment of the relevant risks, including those presented by the nature of their relationship with their hosted wallet customer, the transaction activity, and other activity associated with each counterparty and the CVC or LTDA assets. In the case of a bank, which is subject to very similar requirements pursuant to its obligations to obtain CIP information and engage in ongoing customer due diligence ("CDD"), the bank may be able to leverage information it has previously collected and is already obligated to collect.[68] The same may be true for MSBs which must maintain internal controls as part of an effective money laundering

[68] *See* 31 CFR 1020.210(b)(5); 31 CFR 1020.220(a).

program that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.[69]

2. Procedural Requirements and the Anti-Structuring Rule

a. Procedural Requirements

The proposed rule would amend several procedural requirements that apply to the CTR reporting requirement to ensure their application to the proposed CVC/LTDA transaction reporting requirement as well. These include the requirements of 31 CFR 1010.306(a)(1), which applies a 15-day deadline from the date of a reportable transaction for the filing of the new report; (a)(2), which requires the retention of a copy of each filed report for five years from the date of the report; (a)(3), which requires reports to be filed with FinCEN unless otherwise specified); (d), which requires reports to be filed on form prescribed by the Secretary; and (e), which states that forms used to make reports may be obtained on FinCEN's BSA E-Filing System.

The proposed rule would also make several clerical edits. It would amend 31 CFR 1010.310, which previously provided an overview of the CTR requirement, so that it describes both the CTR requirement and the proposed CVC/LTDA transaction reporting requirement. The proposed rule would also conform the relevant cross-references in Parts 1020 and 1022 to the new requirements,[70] and would add cross-references to the new reporting requirement at 31 CFR 1020.316 and 31 CFR 1022.316.

b. Anti-Structuring Rule

The proposed rule would amend the definition of structuring at 31 CFR 1010.100(xx) to refer to the new reporting requirement at 31 CFR 1010.316 and would also modify the prohibition on structuring at 31 CFR 1010.314 to refer to the proposed reporting requirement. In order to make the proposed reporting requirement effective, it is necessary to ensure that parties

---

[69] *See* 31 CFR 1022.210(a).

[70] Specifically, the proposed rule would make relevant conforming changes to 31 CFR 1020.310, 1020.312, 1020.313, 1022.310, 1022.312, and 1022.313.

engaged in structuring to avoid the new reporting requirement are subject to penalties. Because the proposed reporting requirement at 31 CFR 1010.316 would be imposed pursuant to 31 U.S.C. 5313(a), the proposed amended structuring prohibition at 31 CFR 1010.314 is consistent with 31 U.S.C. 5324.

D. Recordkeeping and Verification Requirements for Transactions Greater than $3,000

Under the proposed recordkeeping provision, to be added at 31 CFR 1010.410(g), banks and MSBs would be required to keep records and verify the identity of their customers engaging in transactions involving the withdrawal, exchange or other payment or transfer, by, through, or to such financial institution of CVC or LTDA, as those terms are defined in § 1010.316(c), with a value of more than $3,000, as determined by the bank or MSB based on the prevailing exchange rate at the time of the transaction.

With respect to counterparty information for which banks and MSBs would be required to collect records pursuant to 31 CFR 1010.410(g), the proposed rule would require that banks and MSBs collect, at a minimum, the name and physical address of each counterparty, and other information the Secretary may prescribe on the reporting form implementing the proposed CVC/LTDA transaction reporting requirement. Banks and MSBs would, under the proposed rule, continue to follow risk-based procedures, consistent with their AML/CFT program, to determine whether to obtain additional information about their customer's counterparties or take steps to confirm the accuracy of counterparty information.

Transactions with a value of greater than $10,000 would be subject to both the reporting requirement of 31 CFR 1010.316(b) and the recordkeeping and verification requirements of 31 CFR 1010.410(g). However, FinCEN expects that banks and MSBs would be able to employ a single set of information collection and verification procedures to

satisfy both requirements, and has made the verification requirements consistent.[71] Furthermore, FinCEN has proposed to apply to these recordkeeping and verification requirements the exemption for transactions between hosted wallets (except for otherwise covered wallets).[72] The same considerations, discussed in Section V.B, that govern the application of the exemption to the proposed CVC/LTDA transaction reporting requirement, such as the need for banks or MSBs to have a documented basis for applying an exemption, would also govern the application of this exemption. In addition, no aggregation would be required for the purpose of the recordkeeping requirement at 31 CFR 1010.410(g).

Furthermore, banks and MSBs would be subject to similar programmatic requirements under the recordkeeping requirement at 31 CFR 1010.410(g) as they would be under the verification requirement for the proposed CVC/LTDA transaction reporting requirement. Specifically, in the case of a transaction in which the bank's or MSB's customer is the sender and recordkeeping and verification is required pursuant to 31 CFR 1010.410(g), the bank or MSB should not complete the transmission of funds until such recordkeeping and verification is complete. Similarly, in the case of a transaction in which the bank's or MSB's customer is the recipient, the bank or MSB should obtain the required recordkeeping and verification information as soon as practicable. In addition, banks and MSBs would be expected to incorporate policies tailored to their respective business models should the bank or MSB be unable to obtain the required information, such as by terminating its customer's account in appropriate circumstances.

For transactions subject to the proposed recordkeeping requirement at 31 CFR 1010.410(g), a bank or MSB would be required to obtain and retain an electronic record of information about its customer, the amount and execution date of the transaction, and the counterparty. Unlike other recordkeeping requirements, such as 31 CFR 1010.410(e) and

---

[71] *Cf., e.g.*, 31 CFR 1010.410(g)(2), *with* 31 CFR 1010.312(b) (verification is only required under either provision for hosted wallet customers transacting through unhosted or otherwise covered wallets).
[72] *Cf.* 31 CFR 1010.410(g)(4), *with* 31 CFR 1010.316(d).

1020.410(a), the recordkeeping requirement in the proposed rule would require the electronic retention of information. FinCEN is proposing to require electronic recordkeeping based on the fact that such recordkeeping is the practical way in which businesses engaged in CVC or LTDA transactions are likely to track their data and the most efficient form in which data can be provided to law enforcement and national security authorities.

Furthermore, under 31 CFR 1010.410(g)(3) as proposed, the information that a financial institution would be required to retain under paragraphs (g)(1) and (g)(2) of that section must be retrievable by the bank or MSB by reference to the name or account number of its customer, or the name of its customer's counterparty. This information would not need not be retained in any particular manner, so long as the bank or MSB is able to retrieve the information. FinCEN is proposing these requirements to ensure that the information retained by banks and MSBs is efficiently searchable in response to lawful information requests.

VI. Request for Comment

FinCEN welcomes comment on all aspects of this proposed rule. FinCEN encourages all interested parties to provide their views.

With respect to the effect of expanding the scope on the definition of "monetary instruments" in the BSA, FinCEN in particular requests comment on the following question from financial institutions and members of the public:

(1) Has FinCEN been sufficiently clear that the impact of the definitional change to "monetary instruments" would be limited to the reporting, recordkeeping, verification, and other requirements of this proposed rule, and not to preexisting regulatory obligations such as the CTR reporting requirement at 31 CFR 1010.311?

With respect to the reporting requirements in proposed 31 CFR 1010.316, FinCEN in particular requests comment on the following questions from law enforcement, financial institutions, and members of the public:

(2) Describe the costs from complying with the proposed reporting requirement.

(3) Describe the benefits to law enforcement from the data obtained from the proposed reporting requirement.

(4) Has FinCEN struck a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity? If not, what would be a more appropriate way to balance these objectives?

(5) Describe how the costs of complying with the proposed reporting requirement, or the benefits to law enforcement from the data obtained from the proposed reporting requirement, would vary were FinCEN to adopt a higher or lower threshold than $10,000.

(6) Describe how the costs of complying with the proposed reporting requirement, or the benefits to law enforcement from the data obtained from the proposed reporting requirement, would vary were FinCEN to apply the reporting requirement to all CVC/LTDA transactions by hosted wallets, including those with hosted wallet counterparties.

(7) Should FinCEN add additional jurisdictions to the Foreign Jurisdictions List or remove jurisdictions currently on that list? Are there any particular considerations FinCEN should take into account when adding or removing jurisdictions?

(8) Has FinCEN provided sufficient clarity to financial institutions on the scope of the aggregation requirements that apply to the proposed CVC/LTDA transaction reporting requirement?

(9) Discuss the costs and benefits of modifying the aggregation requirement to require aggregation for the purposes of the proposed CVC/LTDA transaction reporting requirement across both fiat and CVC/LTDA transactions.

(10) Has FinCEN properly considered the extension of the mandatory and discretionary statutory exemptions at 31 U.S.C. 5313(d)-(e) that are currently applicable to the CTR reporting requirement to the proposed CVC/LTDA transaction reporting requirement? Has FinCEN extended exemptions either too broadly or too narrowly? Was FinCEN correct to not extend the exemption from the CTR reporting requirement at 31 CFR 1010.315 related to transactions

between a non-bank financial institution and a commercial bank to the proposed CVC/LTDA transaction reporting requirement?

(11) Should FinCEN extend the obligation to file reports under the proposed CVC/LTDA transaction reporting requirement to financial institutions other than banks and MSBs (*e.g.*, brokers-dealers, futures commission merchants, mutual funds, etc.)? What would be the cost and benefits of extending the proposed CVC/LTDA transaction reporting requirements to other financial institutions?

With respect to the proposed recordkeeping, verification, and other requirements in connection with CVC/LTDA transactions, FinCEN in particular requests comment on the following questions from law enforcement, financial institutions, and members of the public:

(12) Describe the costs from complying with the proposed recordkeeping and verification requirements.

(13) Describe the benefits to law enforcement from being able to access data verified and obtained based on the proposed recordkeeping and verification requirements.

(14) Could the verification requirements be adjusted to enhance the benefits to law enforcement without a significant change to the costs to banks and MSBs, or to reduce the costs to banks and MSBs without a significant change in the benefit to law enforcement?

(15) Describe the potential changes to the costs and benefits that would be available to law enforcement were FinCEN to maintain the reporting requirement of 31 CFR 1010.316 but also require that banks and MSBs verify the identity of the counterparties of their hosted wallet customers.

(16) Is it necessary for the anti-structuring prohibition to be extended to the proposed CVC/LTDA transaction reporting requirement?

With respect to the proposed recordkeeping requirements in 31 CFR 1010.410(g), FinCEN in particular requests comment on the following questions from law enforcement, financial institutions, and members of the public:

(17) Would it be appropriate for FinCEN to require additional data be retained pursuant to 31 CFR 1010.410(g)?

(18) Describe the costs from complying with the proposed recordkeeping and verification requirements.

(19) Describe the benefits to law enforcement from being able to access data verified and obtained based on the proposed recordkeeping and verification requirements.

(20) Could the verification requirements be adjusted to enhance the benefits to law enforcement without a significant change to the costs to banks and MSBs, or to reduce the costs to banks and MSBs without a significant change in the benefit to law enforcement?

(21) Describe the potential changes to the costs and benefits that would be available to law enforcement were FinCEN to maintain the recordkeeping requirement of 31 CFR 1010.410(g) but also require that banks and MSBs verify the identity of the counterparties of their hosted wallet customers.

(22) Is it reasonable to require that records be retained in electronic form? Are the retrievability criteria reasonable?

(23) Should FinCEN extend the obligation to keep records under the proposed CVC/LTDA transaction reporting requirement to financial institutions other than banks and MSBs (*e.g.*, broker-dealers, futures commission merchants, mutual funds, etc.)?

(24) Describe technical challenges to implementation to could impact reasonable ability to implement these requirements.

VII. Administrative Procedure Act

The Administrative Procedure Act (APA) generally requires an agency to provide notice of proposed rulemaking in the Federal Register and an opportunity for interested persons to participate in the rulemaking by submitting comments on the proposal.[73] No minimum period for comment is prescribed, although agencies must provide the public with a "meaningful

[73] *See generally* 5 U.S.C. 553.

opportunity" to comment on a proposal.[74] The APA also requires publication of the final version of a rule at least thirty days before the rule's effective date.

These requirements do not apply, however, to rules involving a "foreign affairs function" or where "good cause" is shown for rules with respect to which "notice and public procedure" is "impracticable, unnecessary, or contrary to the public interest."[75] As described below, the proposed rule is not subject to notice-and-comment requirements because it falls within each of these exceptions. Nevertheless, FinCEN is publishing its proposed rule in the Federal Register and inviting comments, and will consider any comments received.

FinCEN has determined that a longer period of public comment is not necessary and would frustrate the objectives of the rule by unduly delaying implementation of measures to curb illicit finance and threats to United States national interests. FinCEN notes that in addition to the comment period being provided, the agency has directly engaged with the cryptocurrency industry on multiple occasions and in a variety of formats over the past year on the AML risks arising in connection with cryptocurrency and carefully considered information and feedback received from industry participants. These engagements have included a FinCEN Exchange event in May 2019 on virtual currency with representatives from virtual currency money transmitters, third-party service providers, federal government agencies, a federal task force, and depository institutions that included discussion of methods to identify vulnerabilities, disrupt terrorist and proliferation financing, and guard against other financial crimes;[76] visits to cryptocurrency businesses in California in February 2020; a working session in March 2020 with cryptocurrency industry leaders, compliance experts, and senior Treasury Department and FinCEN officials that included discussion of supervisory and regulatory challenges facing digital

---

[74] *See* N. Carolina Growers' Ass'n, Inc. v. United Farm Workers, 702 F.3d 755, 770 (4th Cir. 2012); Rural Cellular Ass'n v. FCC, 588 F.3d 1095, 1101 (D.C. Cir. 2009).
[75] *See* 5 U.S.C. 553(a)(1), (b)(3)(B), (d)(3).
[76] *See* Press Release, FinCEN, May 3, 2019, *available at* https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange (last accessed Dec. 18, 2020).

assets, including cryptocurrency;[77] and a FinCEN Exchange event on cryptocurrency and ransomware in November 2020 that included discussion of emerging trends and typologies, and recovery of victims' funds.[78] Recently, FinCEN also has received outreach from industry specifically addressing potential regulatory requirements for unhosted wallets, including letters from CoinCenter, the Blockchain Association, Blockchain.com, the Global Digital Asset & Cryptocurrency Association, Circle, and the Association for Digital Asset Markets.

The proposed rule is a vital part of FinCEN's efforts to curb illicit finance, and, subject to feedback received during the comment period, FinCEN believes rapid implementation is critical to the successful accomplishment of the proposed rule's objectives. Undue delay in implementing this rule would encourage movement of unreported or unrecorded assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets, such as by moving CVC to exchanges that do not comply with AML/CFT requirements. Such delay presents an opportunity to illicit actors who have substantial proceeds in regulated financial institutions and who want to be able to move those funds without detection into the darker, unregulated corners of the CVC ecosystems: withdraw the funds quickly with no required reporting to federal authorities, or withdraw the funds after the rule takes effect with detailed mandatory reporting to federal authorities. Conversely, participants with funds at regulated financial institutions who wish to transact with illicit actors operating outside that regulated environment are similarly enabled to proceed with those transactions immediately without detailed mandatory reporting to federal authorities, but face significant reporting obligations if they wait until after a period of delayed implementation. FinCEN has concluded that the incentives that would be created by an undue implementation delay could seriously undermine the interests the rule is designed to advance. In addition, the substantial concerns

---

[77] *See* Press Release, U.S. Dep't of the Treasury, Mar. 2, 2019, *available at* https://home.treasury.gov/news/press-releases/sm926 (last accessed Dec. 18, 2020).
[78] *See* Press Release, FinCEN, Nov. 12, 2020, *available at* https://www.fincen.gov/news/news-releases/fincen-holds-virtual-fincen-exchange-ransomware (last accessed Dec. 18, 2020).

about national security, terrorism, ransomware, money laundering, and other illicit financial activities discussed above, and the need for an effective response in a rapidly changing area of major national concern, support making the amendments in the proposed rule effective as quickly as is feasible.

The considerations are reinforced by the inapplicability of the APA's notice-and-comment requirements to the proposed rule. As noted, the APA provides an exemption from notice-and-comment requirements where "there is involved . . . a foreign affairs function of the United States," and while this exemption is not to be "interpreted loosely" to reach any function having an impact beyond U.S. borders,[79] it is applicable wherever a foreign affairs function is "involved." This exemption is distinct from the APA's good cause exception,[80] and reaches matters affecting relations with other governments to a substantial extent, such as where adherence to the APA's requirements would "provoke definitely undesirable international consequences."[81]

The proposed rule advances foreign policy and national security interests of the United States, using a statute that was designed in part for that purpose. As the Supreme Court has explained, one of Congress's core aims in enacting the Bank Secrecy Act was to respond to threats associated with international financial transactions.[82] Those concerns are plainly implicated where a foreign financial institution is not subject to adequate AML/CFT regulation, or where individuals outside the United States transact without using a financial institution at all. With the increasingly geographically dispersed operating models of CVC systems and financial institutions, both in their organizational and operational structures as well as in their services to customers in many jurisdictions, most CVC and LTDA activity involves cross-border value transfer or cross-border operations. For example, the Bitcoin network operates across nodes

---

[79] *See Mast Indus., Inc. v. Regan*, 596 F. Supp. 1567, 1581 (Ct. Int'l Trade 1984) (quoting H.R.Rep. No. 79–1980, at 23 (1946), H.R.Rep. No. 79–1980, at pp. 23 (1946)).
[80] *See Mast*, 596 F. Supp. at pp. 1581.
[81] *Id.*
[82] *See California Bankers Assn. v. Shultz*, 416 U.S. 21, 27-28 (1974).

around the world. Only approximately 17% of the nodes on the Bitcoin network operate in the United States.[83]

The requirements of the proposed rule directly involve one or more foreign affairs functions of the United States. The illicit financing targeted by these requirements involves substantial international dimensions. Among the objectives of these requirements is the application of appropriate controls to curb malign actions of hostile foreign states facilitated by means of CVC/LTDA, to prevent evasion of United States sanctions regimes, to combat the financing of global terrorism, and to address other threats originating in whole or in substantial part outside the United States, including the proliferation of ransomware attacks, transnational money laundering, and international trafficking in controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. Unduly delaying the implementation of the proposed rule would hinder the efforts of the United States government to perform important national security and foreign affairs functions.[84] In addition, as explained in the discussion of the good cause exception, FinCEN expects that malign actors may exploit such a delay by moving assets to unhosted wallets and away from regulated financial institutions to escape financial transparency.[85]

Furthermore, and consistent with the policy interests underlying this rule, FinCEN notes that the requirements being imposed represent an important part of the leadership role of the United States in the development of international standards applicable to global financial networks, both in general and with respect to CVC/LTDA in particular.[86] In addition to the

---

[83] "Global Bitcoin Nodes Distribution," Bitnodes, https://bitnodes.io/ (accessed Dec. 2, 2020).
[84] *See Rajah v. Mukasey*, 544 F.3d 427, 438 (2d Cir. 2008) (reasoning that notice-and-comment process can be "slow and cumbersome," thereby impairing national interests).
[85] *See Am. Ass'n of Exporters & Importers-Textile & Apparel Grp. v. United States*, 751 F.2d 1239, 1249 (Fed. Cir. 1985) (noting incentive to engage in activities to manipulate trade levels that prior announcement of restricted quotas would create).
[86] *See City of New York v. Permanent Mission of India to United Nations*, 618 F.3d 172, 201–02 (2d Cir. 2010). As commentators have noted, the United States has played a leading role in the development of international AML/CFT measures, including through unilateral action establishing templates for global standards. *See* Laura K. Donohue, Anti-Terrorist Finance in the United Kingdom and United States, 27 Mich. J. Int'l L. 303, 381 (2006).

foreign affairs functions involved in efforts to combat illicit financing, the measures being adopted directly concern the movement of currency and its equivalents (*i.e.,* value that substitutes for currency) across national borders, which has long been viewed as a critical aspect of foreign policy, international relations, and global economic standing.[87]

In addition to the foreign affairs exemption, the APA permits an agency to forgo otherwise applicable notice-and-comment procedures where the agency "for good cause finds . . . that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest."[88] It has long been recognized that the APA's notice-and-comment requirements may run counter to the public interest "when the very announcement of a proposed rule itself can be expected to precipitate activity by affected parties that would harm the public welfare."[89] This is especially so in connection with financial regulation where the "announcement of a proposed rule would enable the sort of financial manipulation the rule sought to prevent."[90] In such circumstances "notice and comment could be dispensed with in order to prevent the amended rule from being evaded."[91] As noted above, FinCEN is concerned about the consequences of undue delay in the implementation of the proposed rule, and in particular that such delay could accelerate or cause the movement of assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets, such as by moving CVC to exchanges that do not comply with AML/CFT requirements. These concerns squarely implicate the APA's good cause exception. Good cause may also be supported where delay in implementation "could result in serious harm."[92] For example, agency good cause findings have

---

[87] *See Schultz*, 416 U.S. at pp. 27-28. Numerous provisions of the BSA single out transactions with foreign elements for special treatment. *See, e.g.,* 31 U.S.C. 5314 (reports on transactions with foreign financial agencies), 5316 (importation and exportation of monetary instruments); *see also* 31 U.S.C. 5315(a)(1), (3) (declaring congressional findings that, *inter alia*, "moving mobile capital can have a significant impact on the proper functioning of the international monetary system" and that authority should be provided to collect information on capital flows to beyond authorities under the Trading with the Enemy Act and the Bretton Woods Agreement Act).
[88] 5 U.S.C. 553(b)(3)(B).
[89] *Mobil Oil Corp. v. Dept of Energy*, 728 F.2d 1477, 1492 (Temp. Emer. Ct. App. 1983).
[90] *See* U.S. Dep't of Justice, Attorney General's Manual on the Administrative Procedure Act at pp. 31, quoted in *Utility Solid Waste Activities Group v. Environmental Protection Agency*, 236 F.3d 749, 755 (D.C. Cir. 2001).
[91] Mack Trucks, Inc. v. E.P.A., 682 F.3d 87, 95 (D.C. Cir. 2012) (citation and quotation marks omitted).
[92] *Jifry v. FAA*, 370 F.3d 1174, 1179 (D.C. Cir. 2004).

been sustained in connection with anti-terrorism measures, such as rules adopted to prevent airplane hijacking.[93] While serious harm most commonly involves threats to physical health and safety, agency good cause findings based on other concerns, such as the prevention of substantial financial fraud, have also survived challenge.[94] FinCEN has determined that the substantial concerns about national security, terrorism, ransomware, money laundering, and other illicit financial activities discussed above, and the need for an effective response in a rapidly changing area of major national concern, support making the amendments in the proposed rule effective as quickly as is feasible.

VIII. Regulatory Analysis

A. Executive Orders 13563, 12866, and 13771

Executive Orders 13563 and 12866 direct agencies to assess costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, and public health and safety effects; distributive impacts; and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. Although the review requirements of Executive Order 12866 do not apply to this proposed rule because it involves a foreign affairs function, in the interest of maximizing transparency, FinCEN has analyzed the economic effects of this proposed rule consistent with the principles of the Order.

FinCEN believes the primary cost of complying with the proposed rule is captured in its Paperwork Reduction Act (44 U.S.C. 3507(d)) ("PRA") burden estimates described in detail below, which amount to 1,284,349 hours. FinCEN estimated in its recent OMB control number renewal for SAR requirements that the average labor cost of storing SARs and

---

[93] *See id.*; *see also Airport Operators Council Intern. v. Shaffer*, 354 F. Supp. 79 (D.D.C. 1973).
[94] *See Disabled in Action of Metro. New York, Inc. v. Brezenoff*, 506 F. Supp. 244, 248 (S.D.N.Y. 1980); *see also Northern Arapahoe Tribe v. Hodel*, 808 F.2d 741, 751 (10th Cir. 1987) (finding good cause based on need to preserve wildlife in light of impending hunting season).

supporting documentation, weighed against the relevant labor required, was $24 per hour.[95] FinCEN assesses that this is a reasonable estimate for the labor cost of the requirements that would be imposed by this rule. Therefore a reasonable minimum estimate for the burden of administering this rule is approximately $30.8 million annually (1,284,349 hours multiplied by $24 per hour). However, the PRA burden does not include certain costs, such as information technology implementation costs solely resulting from the proposed rule. FinCEN specifically requests comment regarding the costs associated with implementing these requirements.

FinCEN notes that although institutions that provide CVC or LTDA wallet hosting services are, *ipso facto*, likely to be capable of handling the implementation of the proposed reporting requirement, the initial costs of implementation may be non-trivial. For instance, institutions may incur costs in the initial stages if they set up a process for fitting existing data they maintain into XML format.

The benefits from the proposed rule are expected to include enhanced law enforcement ability to investigate, prosecute and disrupt the financing of international terrorism and other priority transnational security threats, as well as other types of financial crime, by obtaining improved visibility into financial flows into unhosted wallets and improved attribution of CVC transactions involving unhosted and otherwise covered wallets.[96] FinCEN believes that the collection of CVC and LTDA indicators will significantly enhance law enforcement's and regulators' ability to leverage blockchain analytics to obtain attribution and move investigations forward in an expeditious manner.

The cost of terrorist attacks can be immense. For instance, one public report estimated the cost of terrorism globally at $33 billion in 2018, though this cost was primarily borne outside the United States.[97] The cost of a major terrorist attack, such as the September 11

---

[95] 85 FR 31598, 31604 and 31607 (May 26, 2020).
[96] At the moment, only a limited number of transactions occur involving LTDA, although many countries are developing LTDA.
[97] *See* Institute for Economics and Peace, Global Terrorism Index, 2019 (Nov. 2019), *https://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf*.

attacks, can reach tens of billions of dollars.[98] Of course, it is difficult to quantify the contribution of a particular rule to a reduction in the risk of a terrorist attack. However, even if the proposed rule produces very small reductions in the probability of a major terrorist attack, the benefits would exceed the costs.

The proposed rule would contribute to the ability of law enforcement to investigate a wide array of priority transnational threats and financial crimes, including terrorism, proliferation financing, sanctions evasion, money laundering, human trafficking, and child exploitation.

FinCEN considered several alternatives to the proposed rule. First, FinCEN considered imposing a reporting requirement on all CVC/LTDA transactions. However, FinCEN determined that existing AML requirements typically were sufficient to mitigate enough of the risks of illicit finance involving transactions between hosted wallets at BSA-regulated institutions that it did not appear justified to impose an additional transaction reporting requirement that all banks and MSBs report all such transactions. If FinCEN reevaluates this conclusion in light of comments to the proposed rule, FinCEN would likely extend the discretionary reporting requirement exemptions similar to the rules that apply to banks under 31 CFR 1020.315 such that filers could submit a FinCEN Form 110 or similar form to exempt certain customers that engage in consistent patterns of legal transactions.

Second, FinCEN considered only applying the exemption at 31 CFR 1010.316(d) to counterparty hosted wallets at BSA-regulated financial institutions and not extending it to hosted wallets at foreign financial institutions in jurisdictions not on the Foreign Jurisdictions List. However, FinCEN determined that given the inherently international nature of CVC and LTDA transactions, and the fact that certain other jurisdictions apply an AML regime to

---

[98] For example, the New York Comptroller estimated in 2002 that the direct physical and human cost of the September 11 attacks on New York was over $30.5 billion. *See* City of New York Comptroller, "One Year Later: The Fiscal Impact of 9/11 on New York City" (Sept. 4, 2002), *https://comptroller.nyc.gov/wp-content/uploads/documents/impact-9-11-year-later.pdf.*

financial institutions hosting CVC or LTDA wallets, it would be appropriate to initially not impose additional requirements with respect to wallets hosted by financial institutions in jurisdictions not on the Foreign Jurisdictions List. However, FinCEN will carefully analyze comments to determine whether additional jurisdictions should be added to the Foreign Jurisdictions List.

Third, FinCEN considered applying a lower threshold for the proposed CVC/LTDA transactions than the $10,000 threshold. While imposing a lower threshold for CVC/LTDA transactions would enhance the ability of law enforcement and national security authorities to obtain attribution on a larger number of wallets, FinCEN determined that it would be beneficial for the reporting requirement included in the proposed rule to have a threshold consistent with the CTR reporting requirement for fiat transactions. FinCEN will carefully consider comments as to whether a lower or higher reporting threshold would be appropriate for the proposed CVC/LTDA transaction reporting requirement.

Fourth, FinCEN considered extending the proposed CVC/LTDA transaction reporting requirement to different types of financial institutions besides banks and MSBs. Based on the current market structure, FinCEN determined that it would be appropriate to limit the proposed rule's application to banks and MSBs. FinCEN will carefully evaluate comments as to whether the CVC/LTDA custody market in its current form, or as a result of how it is expected to develop in the future, justifies extending the proposed CVC/LTDA transaction reporting requirement to other types of financial institutions such as those in the securities and commodities industries.

Fifth, FinCEN considered imposing the proposed CVC/LTDA transaction reporting requirement at 31 CFR 1010.316(b), as well as the proposed recordkeeping requirement at 31 CFR 1010.410(g), without associated verification requirements. However, FinCEN determined that it is reasonable to require verification at the time a hosted wallet customer engages in CVC/LTDA transactions that transfer significant value involving unhosted or

otherwise covered wallets. The proposed verification requirement would enhance the ability of financial institutions to provide accurate information in their CVC/LTDA transaction reporting, as well as to identify suspicious activity. FinCEN also considered proposing verification requirements that required gathering specific documentation consistent with the verification requirements applicable to CTR reporting, but determined that it would be more appropriate to allow banks and MSBs to rely on risk-based verification procedures.

Executive Order 13771 requires an agency to identify at least two existing regulations to be repealed whenever it publicly proposes for notice and comment or otherwise promulgates a new regulation. The reporting, recordkeeping, and verification requirements proposed in this notice involve a national security function. Therefore, Executive Order 13771 does not apply.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act ("RFA") (5 U.S.C. 601 et seq.) requires an agency either to provide an initial regulatory flexibility analysis with a proposed rule or certify that the proposed rule will not have a significant economic impact on a substantial number of small entities. This proposed regulation applies to all banks and MSBs and likely would affect a substantial number of small entities. FinCEN has therefore prepared an initial regulatory flexibility analysis pursuant to the RFA. FinCEN welcomes comments on all aspects of the initial regulatory flexibility analysis. A final regulatory flexibility analysis will be conducted after consideration of comments received during the comment period.

1. Statement of the Need for, and Objectives of, the Proposed Regulation

This proposed rule would adopt recordkeeping, verification, and reporting requirements for certain deposits, withdrawals, exchanges, or other payments or transfers of CVC or LTDA by, through, or to a bank or MSB that involve an unhosted or otherwise covered wallet. FinCEN is proposing to define otherwise covered wallets as those wallets that are held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN on a Foreign Jurisdictions List.

First, this proposed rule would require banks and MSBs to file a report with FinCEN containing certain information related to a customer's CVC or LTDA transaction and counterparty (including name and physical address), and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000 (or the transaction is one of multiple CVC transactions involving such counterparty wallets and the customer flowing through the bank or MSB within a 24-hour period that aggregate to value in or value out of greater than $10,000). Second, this proposed rule would require banks and MSBs to keep records of a customer's CVC or LTDA transaction and counterparty, including verifying the identity of their customer, if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000.

Although analytic techniques can be used to combat illicit finance through CVC or LTDA, they are not a panacea. Blockchain analysis can be rendered less effective by a number of factors, including the scale of a blockchain network, the extent of peer-to-peer activity (*i.e.*, transactions between unhosted wallets), the use of anonymizing technologies to obscure transaction information, and a lack of information concerning the identity of transferors and recipients in particular transactions. Additionally, several types of AEC are increasing in popularity and employ various technologies that inhibit investigators' ability both to identify transaction activity using blockchain data and to attribute this activity to illicit activity conducted by natural persons.

The requirements FinCEN is proposing would therefore provide greater insight into transacting parties with a nexus to one or more potentially illicit transactions in several respects. These include directly as a result of the information collected, maintained, and reported in relation to transactions above the recordkeeping or reporting thresholds and also through information identified in relation to structured transactions given the new structuring prohibition that would be imposed. This greater insight will contribute to the ability of law enforcement to investigate a wide array of priority transnational threats and financial crimes, including terrorism,

proliferation financing, sanctions evasion, money laundering, human trafficking, and child exploitation. The proposed rule's reporting requirements are similar to the reporting requirements applicable to cash transactions imposed by the CTR reporting requirement. Furthermore the recordkeeping requirements resemble the recordkeeping requirements applicable to transmittals of funds between financial institutions.

2. Small Entities Affected by the Proposed Regulation

This proposed regulation applies to all banks and MSBs and likely would affect a substantial number of small entities. As described in the PRA section that follows, based upon current data there are 5,306 banks, 5,236 credit unions, and 365 MSBs that would be impacted by the proposed rule changes. Based upon current data, for the purposes of the RFA, there are at least 3,817 small Federally-regulated banks and 4,681 small credit unions.[99] FinCEN believes that most money transmitters are small entities.[100] Because the proposed rule would apply to all of these small financial institutions, FinCEN concludes that this proposed rule would apply to a substantial number of small entities.

FinCEN anticipates that for most small banks and credit unions the impact of the proposed changes will be minor. While FinCEN is aware that such institutions, in light of developments such as the OCC Custody Guidance and the creation of the SPDI charter in Wyoming, are likely to engage in a growing amount of CVC transactions, that trend is still in the early stages. FinCEN anticipates the burden on banks will become more comparable to that on MSBs over time, as banks engage in more custody transactions involving CVC or LTDA. Likewise, FinCEN does not believe that any banks or MSBs currently facilitate a significant number of transactions involving sovereign digital currencies.

---

[99] The Small Business Administration ("SBA") defines a depository institution (including a credit union) as a small business if it has assets of $600 million or less. The information on small banks is published by the Federal Deposit Insurance Corporation ("FDIC") and was current as of March 31, 2020.

[100] The SBA defines an entity engaged in "Financial Transactions Processing, Reserve, and Clearinghouse Activities" to be small if it has assets of $41.5 million or less. FinCEN assesses that money transmitters most closely align with this SBA category of entities.

Based on the conclusions just mentioned, the primary impact of the proposed rules on small businesses will be on small businesses acting as money transmitters. FinCEN notes that although institutions that provide CVC or LTDA wallet hosting services are, *ipso facto*, likely to be capable of handling the implementation of the proposed reporting requirement, the initial costs of implementation may be non-trivial. For instance, institutions may incur costs in the initial stages if they set up a process for fitting existing data they maintain into XML format.

3. Compliance Requirements

Compliance costs for entities that would be affected by these regulations are generally, reporting, recordkeeping, and information technology implementation and maintenance costs. Data are not readily available to determine the costs specific to small entities and FinCEN invites comments about compliance costs, especially those affecting small entities.

This proposed rule would adopt recordkeeping, verification, and reporting requirements for certain deposits, withdrawals, exchanges, or other payments or transfers of CVC or LTDA by, through, or to a bank or MSB that involve an unhosted or otherwise covered wallet. First, this proposed rule would require banks and MSBs to file a report with FinCEN containing certain information related to a customer's CVC or LTDA transaction and counterparty (including name and physical address), and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000 (or the transaction is one of multiple CVC transactions involving such counterparty wallets and the customer flowing through the bank or MSB within a 24-hour period that aggregate to value in or value out of greater than $10,000). Second, this proposed rule would require banks and MSBs to keep records of a customer's CVC or LTDA transaction and counterparty, including verifying the identity of their customer, if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000.

4. Duplicative, Overlapping, or Conflicting Federal Rules

FinCEN is unware of any Federal rules that duplicate, overlap with, or conflict with the changes to the BSA regulation proposed herein. These rules are meant to be analogues to the recordkeeping requirements applicable to transmittals of funds between financial institutions and the CTR reporting requirements applicable to transactions in currency.

5. Significant Alternatives to the Proposed Regulations

FinCEN considered several alternatives to the proposed regulatory changes. First, FinCEN considered imposing a reporting requirement on all CVC/LTDA transactions. However, FinCEN determined that existing AML requirements typically were sufficient to mitigate enough of the risks of illicit finance involving transactions between hosted wallets at BSA-regulated institutions that it did not appear justified to impose an additional transaction reporting requirement that all banks and MSBs report all such transactions.

Second, FinCEN considered only applying the exemption at 31 CFR 1010.316(d) to counterparty hosted wallets at BSA-regulated financial institutions and not extending it to hosted wallets at foreign financial institutions in jurisdictions not on the Foreign Jurisdictions List. However, FinCEN determined that it would be appropriate to initially not impose additional requirements with respect to wallets hosted by financial institutions in jurisdictions not on the Foreign Jurisdictions List.

Third, FinCEN considered applying a lower threshold for the proposed CVC/LTDA transactions than the $10,000 threshold. FinCEN determined that it would be beneficial for the reporting requirement included in the proposed rule to have a threshold consistent with the CTR reporting requirement for fiat transactions.

Fourth, FinCEN considered extending the proposed CVC/LTDA transaction reporting requirement to different types of financial institutions besides banks and MSBs. Based on the current market structure, FinCEN determined that it would be appropriate to limit the proposed rule's application to banks and MSBs.

Fifth, FinCEN considered imposing the proposed CVC/LTDA transaction reporting requirement at 31 CFR 1010.316(b), as well as the proposed recordkeeping requirement at 31 CFR 1010.410(g), without associated verification requirements. However, FinCEN determined that it is reasonable to require verification at the time a hosted wallet customer engages in CVC/LTDA transactions that transfer significant value involving unhosted or otherwise covered wallets. FinCEN also considered proposing verification requirements that required gathering specific documentation consistent with the verification requirements applicable to CTR reporting, but determined that it would be more appropriate to allow banks and MSBs to rely on risk-based verification procedures.

FinCEN welcomes comment on the overall regulatory flexibility analysis, especially information about compliance costs and alternatives.

C. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995 (''Unfunded Mandates Act''), Public Law 104–4 (March 22, 1995), requires that an agency prepare a budgetary impact statement before promulgating a rule that may result in expenditure by the state, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 202 of the Unfunded Mandates Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule. See section VIII.A for a discussion of the economic impact of this proposed rule and regulatory alternatives.

D. Paperwork Reduction Act

The reporting and recordkeeping requirements contained in this proposed rule have been submitted by FinCEN to OMB for review in accordance with the PRA. Under the Paperwork Reduction Act, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by OMB. Written comments and recommendations for the information collection can be submitted by visiting

www.reginfo.gov/public/do/PRAMain. Find this particular notice by selecting "Currently under Review—Open for Public Comments" or by using the search function. Comments are welcome and must be received by **[INSERT DATE THAT IS 15 DAYS AFTER DATE OF FILING AT THE *FEDERAL REGISTER*]**. In accordance with requirements of the PRA and its implementing regulations, 5 CFR part 1320, the following information concerning the collections of information are presented to assist those persons wishing to comment on the information collections.

1. Change in the Definition of "Monetary Instruments"

The change proposed in this notice to the definition of monetary instruments would impose no direct burden on the public.

2. Reporting Requirement Related to CVC and LTDA: [31 CFR 1010.306(a)(1)-(3), (d)-(e), 1010.313, 1010.316, 1020.313, 1020.315, 1020.316, 1022.313, 1022.316]

The proposed rule would require banks and MSBs to report information related to CVC and LTDA transactions above $10,000 between their hosted wallet clients and unhosted or otherwise covered wallets. The proposed aggregation rules that would apply to CVC and LTDA transactions are broadly similar to those that apply to the CTR reporting requirement; aggregation is not required, however, between a person's CVC/LTDA and currency transactions. The mandatory exemptions of 31 U.S.C. 5313(d) apply to the proposed CVC/LTDA transaction reporting requirement, as incorporated in 31 CFR 1020.315.

Description of Recordkeepers: Banks and MSBs that conduct CVC or LTDA transactions on behalf of hosted wallet clients as senders or recipients in an amount above $10,000.

Estimated Number of Recordkeepers: 10,907 financial institutions. FinCEN estimates that there are approximately 5,306 federally regulated banks and 5,236 federally

regulated credit unions.[101] FinCEN, for purposes of these estimates, will assume that all of these banks and credit unions engage nominally in transactions involving CVC. FinCEN estimates that, as of November 2020, 365 MSBs engage in CVC transactions.[102] The FinCEN MSB registration form does not require that companies disclose whether they engage in CVC transactions. This estimate is therefore based on adding the number of MSBs that indicated they engage in CVC transactions in an optional field on the MSB registration form, and the number that did not so indicate but which, based on FinCEN's research, FinCEN believes engage in CVC transactions. (5,306 + 5,236 + 365= 10,907).

Estimated Average Annual Burden Hours Per Recordkeeper: FinCEN notes that in the recent Funds Transfer / Travel Rule NPRM, FinCEN estimated that the burden hours per bank was nominally one hour. FinCEN is retaining the same estimate for this rule. While FinCEN is aware that banks, in light of developments such as the OCC Custody Guidance and the creation of the SPDI charter in Wyoming, are likely to engage in a growing amount of CVC transactions, that trend is still in the early stages. FinCEN anticipates the burden on banks will become more comparable to that on MSBs over time, as banks engage in more custody transactions involving CVC or LTDA.

In the Funds Transfer / Travel Rule NPRM PRA analysis, FinCEN estimated that the burden per MSB to comply with the collection and recordkeeping requirement at the transactional threshold of $3,000 was 240 hours per institution, and that the burden per MSB to comply with the transmission requirement at the transactional threshold of $3,000 was 180 hours per institution. The burden analysis below assumes that the transmittal requirement burden in the Funds Transfer / Travel Rule NPRM context is analogous to the reporting

---

[101] According to the FDIC there were 5,103 FDIC-insured banks as of March 31, 2020. According to the Board of Governors of the Federal Reserve System, there were 203 other entities supervised by the Board or other Federal regulators, as of June 16, 2020, that fall within the definition of bank. (20 Edge Act institutions, 15 agreement corporations, and 168 foreign banking organizations). According to the National Credit Union Administration, there were 5,236 federally regulated credit unions as of December 31, 2019.

[102] In the Funds Transfer / Travel Rule NPRM, FinCEN estimated that there were 530 MSB filers. Certain of these, however, are filers that were previously registered with FinCEN and that subsequently allowed their expirations to lapse. As a result of their expirations lapsing, FinCEN has removed those filers from the burden calculation.

requirement burden under the proposed CVC/LTDA transaction reporting requirement.[103] However, the burden must be adjusted for four factors: (i) the fact that the $10,000 threshold under the CVC/LTDA transaction reporting requirement is greater than the $3,000 threshold in the Funds Transfer / Travel Rule NPRM; (ii) the fact that the burden analyzed in the Funds Transfer / Travel Rule NPRM relates to transactions between hosted wallets and not transactions from hosted to unhosted wallets, and there may be more or fewer hosted-to-unhosted transactions at any level; (iii) the fact that some transactions below the transaction reporting threshold may be subject to reporting due to aggregation requirements; and (iv) the fact that the reporting burden under the proposed CVC/LTDA transaction reporting requirement may be more complex than the transmission requirement under the Funds Transfer / Travel Rule NPRM.[104]

As FinCEN noted in the Funds Transfer / Travel Rule NPRM PRA analysis, the estimated average burden hours would vary depending on the number of transactions conducted by a financial institution's customers with unhosted or otherwise covered wallets. In a recent publication commenting on the recent Funds Transfer / Funds Travel NPRM, the blockchain analytics firm CipherTrace estimated that the proposed decrease in the applicable threshold for international transactions from $3,000 to $250 would increase the number of reportable transactions per month from approximately 27,300 to approximately 79,000.[105] Applying a constant elasticity model,[106] FinCEN estimates that approximately 60% as many

---

[103] As discussed in the next section, FinCEN assumes that the recordkeeping requirement burden in the Funds Transfer / Travel Rule NPRM context is analogous to the recordkeeping / verification burden related to CVC/LTDA transaction reporting.

[104] FinCEN anticipates that the number of transactions subject to reporting and recordkeeping related to otherwise covered wallets hosted by foreign financial institutions located in jurisdictions on the Foreign Jurisdictions List will be modest and does not calculate additional burden in relation to this aspect of the rule.

[105] CipherTrace, "FinCEN's Proposed Rule Change for Travel Rule Threshold Would More Than Double Compliance Events at US VASPs" (Nov. 13, 2020), *https://ciphertrace.com/fincens-proposed-rule-change-for-travel-rule-would-trigger-more-than-double-the-compliance-events-at-us-vasps/* (accessed Dec. 1, 2020).

[106] Specifically, FinCEN fit an equation of the model $Y = CX^{\alpha}$ to the data from CipherTrace, where Y equals the number of transactions above a given threshold, X equals the threshold, C is a constant, and α is the percent change in Y per one-percent change in X. FinCEN used the calibrated values of C and α to extrapolate to the number of transactions above the $10,000 threshold.

transactions would occur above the $10,000 threshold.

In order to estimate the ratio of unhosted-to-hosted transactions to hosted-to-hosted transactions, FinCEN analyzed blockchain data related to all identifiable transactions by each of two major exchanges in September 2020 using blockchain analytic tools. FinCEN found that the ratio of unhosted-to-hosted to hosted-to-hosted transactions were approximately 1.52 and 2.39 in the $3,000 to $10,000 transaction range for the two exchanges, respectively. In the greater than $10,000 range the ratios were 1.40 and 1.64, respectively. In the analysis below, FinCEN uses the larger ratios, 2.39 and 1.64. Thus FinCEN will assume that 164% as many transactions would be covered by the reporting requirements at the $10,000 threshold under the proposed rule than the transmission requirements at the same threshold in the Funds Transfer / Travel Rule NPRM. Similarly, in the $3,000 to $10,000 range, FinCEN will assume 239% as many transactions would be covered by the proposed rule's recordkeeping and verification requirements described in the next section in comparison to the recordkeeping requirements in the Funds Transfer / Travel Rule NPRM.

Thus, at the $10,000 threshold, we assume that only 60% as many transactions are occurring as at the $3,000 level, but that the number of such transactions which are unhosted-to-hosted are 164% of the amount of such transactions that are hosted-to-hosted, for a combined total scaling factor of 98.4%. To account for the fact that some transactions less than $10,000 will need to be aggregated due to aggregation requirements, we will assume that the total scaling factor is 148% (98.4% * 1.5).

In contrast to the PRA analysis used for the Funds Transfer / Travel Rule NPRM, the reporting burden will possibly be more complicated than the requirement to transmit information in the Funds Transfer / Travel Rule NPRM given the variety of information required by the reporting form. For purposes of calculations, FinCEN assumes that the

reporting burden will be twice as complex.[107] Therefore the total scaling factor applied to the Funds Transfer / Travel Rule NPRM PRA burden estimate for transmission burden is 2.96 (2.96 = 2 x 1.48). As a result, the estimated burden per MSB is 533 hours (180 hours (from Funds Transfer / Travel Rule NPRM PRA analysis) x 2.94).

Estimated Total Additional Annual Burden Hours: 10,542 hours (10,542 banks x 1 hour / bank) + 194,545 hours (365 MSBs x 533 hours / MSB) = 205,087 hours.

3. Recordkeeping and Verification Requirements Related to CVC and LTDA: [31 CFR 1010.312, 1010.410(g), 1022.312, 1022.312]

The proposed rule would require banks and MSBs to keep records of, and verify the identity of their hosted wallet customers who participate in, transactions subject to the CVC/LTDA transaction reporting requirements, *i.e.* CVC/LTDA transactions involving hosted wallet customers and unhosted or otherwise covered wallets related with a value aggregating to $10,000 or more. The proposed recordkeeping requirement at 31 CFR 1010.410(g) likewise would require banks and MSBs to keep records of, and verify the identity of their hosted wallet customers who engage in, transactions with a value of more than $3,000. Furthermore, under the proposed rule, for transactions that are greater than $3,000, or that aggregate to more than $10,000, the name and physical address of each counterparty must be collected and, in the case of reportable transactions, reported.

Description of Recordkeepers: Banks and MSBs that conduct CVC or LTDA transactions on behalf of hosted wallet clients as senders or recipients in an amount above $3,000, or that aggregate to an amount above $10,000.

Estimated Number of Recordkeepers: 10,907 financial institutions. FinCEN estimates that there are approximately 5,306 federally regulated banks and 5,236 federally regulated credit unions. FinCEN assesses that all of these banks and credit unions nominally

[107] The burden of collecting counterparty information that must be reported on the reporting form is considered in the next section.

engage in transactions involving CVC. FinCEN estimates that there are 365 MSBs that engage in CVC transactions.

Estimated Average Annual Burden Hours Per Recordkeeper: As noted in the previous section, FinCEN believes that the burden estimate for recordkeeping in the Funds Transfer / Travel Rule NPRM (240 hours per MSB) is analogous to the burden estimate for recordkeeping and verification requirements pursuant to the proposed CVC/LTDA transaction reporting requirement.

All transactions subject to reporting would also subject to recordkeeping and verification requirements. Therefore, the estimate that 148% as many transactions will be subject to the proposed reporting requirement as compared to the transactions subject to transmission requirements proposed by the Funds Transfer / Travel Rule NPRM, also applies to the recordkeeping and verification requirements of the proposed rule. However, this increase needs to be supplemented with the increase in transactions that would be subject to recordkeeping and verification under 31 CFR 1010.410(g), as proposed, which are between $3,000 and $10,000. Using the constant elasticity model described in the previous section, the number of hosted-to-hosted transactions between $3,000 and $10,000 is approximately 40% of the estimated number of transactions about $10,000. Applying the 239% scale factor used in the previous section to calculate the proportionate number of hosted-to-unhosted transactions, and making no adjustment for the fact that some transactions in this $3,000 to $10,000 range would contribute to aggregation for the purposes of the proposed CVC/LTDA transaction reporting requirement and already be subject to verification, the total number of transactions subject to verification and recordkeeping due to 31 CFR 1010.410(g) would increase by an additional 96% (0.4 * 2.39 = 0.956), for a total scaling factor of 244% (2.44 = 1.48 + 0.96).

However, FinCEN notes that the recordkeeping and verification requirement in the proposed rule is likely to be more burdensome than the collection and recordkeeping requirements of the Funds Transfer / Travel Rule NPRM. In particular, the requirements dealt

with in the Funds Transfer / Travel Rule NPRM do not require verification in most cases. In contrast, this proposed rule would require verifying the hosted wallet customer in each transaction subject to the reporting or recordkeeping requirements, as well as collecting each counterparty's name and physical address. As a result of this greater burden, FinCEN assumes, for the purpose of this burden estimate, that the recordkeeping and verification burden is five times greater per transaction, under the proposed rule, than the burden imposed under the recordkeeping requirements of the Funds Transfer / Travel Rule NPRM. Therefore the total scaling factor applied to the Funds Transfer / Travel Rule NPRM PRA burden estimate for transmission burden is 12.2 (12.2 = 5 x 2.44). As a result, the estimated burden per MSB is 2,928 hours (240 hours (from Funds Transfer / Travel Rule NPRM PRA analysis) x 12.2).

Estimated Total Additional Annual Burden Hours: 10,542 hours (10,542 banks x 1 hour / bank) + 1,068,720 hours (365 MSBs x 2,928 hours / MSB) = 1,079,262 hours.

4. Total Annual Burden Hours Estimate Under the Proposed Rule

205,087 (reporting requirements) + 1,079,262 hours (recordkeeping and verification requirements) = 1,284,349 hours.

5. Questions for Comment

In addition to the questions listed above, FinCEN specifically invites comment on: (a) the accuracy of the estimated burden associated with the collection of information; (b) how the quality, utility, and clarity of the information to be collected may be enhanced; and (c) how the burden of complying with the collection of information may be minimized, including through the application of automated collection techniques or other forms of information technology.

List of Subjects in 31 CFR Parts 1010 and 1020

Administrative practice and procedure, Banks, Banking, Currency, Foreign banking, Foreign currencies, Investigations, Penalties, Reporting and recordkeeping requirements, Terrorism.

Authority and Issuance

For the reasons set forth in the preamble, Parts 1010, 1020, and 1022 of chapter X of Title 31 of the Code of Federal Regulations are proposed to be amended as follows:

PART 1010 – GENERAL PROVISIONS

1. The authority citation for part 1010 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C. 5311-5314 and 5316-5332; title III, sec. 314, Pub. L. 107-56, 115 Stat. 307; sec. 701, Pub. L. 114-74, 129 Stat. 599.

2. Amend § 1010.100 by revising paragraph (xx) to read as follows:

§ 1010.100 General definitions.

* * * * *

(xx) *Structure (structuring)*. For purposes of § 1010.314, a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, or, as defined in § 1010.316(c), convertible virtual currency, and digital assets with legal tender status, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the reporting requirements under §§ 1010.311, 1010.313, 1020.315, 1010.316, 1021.311 and 1021.313 of this chapter. "In any manner" includes, but is not limited to, the breaking down of a single sum of currency exceeding $10,000 into smaller sums, including sums at or below $10,000, or the conduct of a transaction, or series of currency transactions at or below $10,000. The transaction or transactions need not exceed the $10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring within the meaning of this definition.

* * * * *

3. Amend § 1010.306, by revising the text of paragraphs (a), (d), and (e) to read as follows:

§ 1010.306 Filing of reports.

(a)(1) A report required by § 1010.311, § 1010.316, or § 1021.311 of this chapter, shall be filed by the financial institution within 15 days following the day on which the reportable transaction occurred.

(2) A copy of each report filed pursuant to §§ 1010.311, 1010.313, 1010.316, 1020.315, 1021.311 and 1021.313 of this chapter, shall be retained by the financial institution for a period of five years from the date of the report.

(3) All reports required to be filed by §§ 1010.311, 1010.313, 1010.316, 1020.315, 1021.311 and 1021.313 of this chapter, shall be filed with FinCEN, unless otherwise specified.

* * * * *

(d) Reports required by § 1010.311, 1010.313, 1010.316, 1010.340, § 1010.350, 1020.315, 1021.311 or 1021.313 of this chapter shall be filed on forms prescribed by the Secretary. All information called for in such forms shall be furnished.

(e) Forms to be used in making the reports required by § 1010.311, 1010.313, 1010.316, 1010.350, 1020.315, 1021.311 or 1021.313 of this chapter may be obtained from BSA E-Filing System. Forms to be used in making the reports required by § 1010.340 may be obtained from the U.S. Customs and Border Protection or FinCEN.

4. Revise § 1010.310 to read as follows:

§ 1010.310 Reports of transactions in currency.

Sections 1010.310 through 1010.314 and 1010.316 set forth the rules for the reporting by financial institutions of transactions in currency, convertible virtual currency, and digital assets with legal tender status. Unless otherwise indicated, the transactions in currency reporting requirements in §§ 1010.310 through 1010.314 apply to all financial institutions. The transactions in convertible virtual currency and digital assets with legal tender status requirements apply to banks and money services businesses. Each financial institution should refer to subpart C of its chapter X part for any additional transactions in currency reporting requirements.

5. Revise § 1010.312 to read as follows:

§ 1010.312 Identification required.

(a) Transactions in Currency: Before concluding any transaction with respect to which a report is required under § 1010.311, 1010.313(b), 1020.315, 1021.311, or 1021.313 of this chapter, a financial institution shall verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and the social security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States must be made by passport, alien identification card, or other official document evidencing nationality or residence (*e.g.*, a Provincial driver's license with indication of home address). Verification of identity in any other case shall be made by examination of a document, other than a bank signature card, that is normally acceptable within the banking community as a means of identification when cashing checks for nondepositors (*e.g.*, a driver's license or credit card). A bank signature card may be relied upon only if it was issued after documents establishing the identity of the individual were examined and notation of the specific information was made on the signature card. In each instance, the specific identifying information (*i.e.*, the account number of the credit card, the driver's license number, *etc.*) used in verifying the identity of the customer shall be recorded on the report, and the mere notation of "known customer" or "bank signature card on file" on the report is prohibited.

(b) Transactions in Convertible Virtual Currency or Digital Assets with Legal Tender Status: Before concluding any transaction with respect to which a report is required under § 1010.313(c) or § 1010.316 of this chapter, a bank or money services business shall verify and record the identity of its customer engaging in the transaction. Consistent with the bank's or money service business's anti-money laundering and countering the financing of terrorism program, the bank or money services business should establish risk-based procedures for

verifying the identity of its customer. The procedures must enable the bank or money services business to form a reasonable belief that it knows the true identity of its customer engaging in a transaction. These procedures must be based on the bank or money services business's assessment of the relevant risks, including those presented by the nature of their relationship with its customer, the transaction activity, and other activity associated with the convertible virtual currency or digital assets with legal tender status involved in the transaction.

Note to paragraph (b): If a bank or money services business has knowledge that a person has accessed the bank's or money services business's customer's wallet to conduct a reportable transaction who is not the bank's or money services business's customer, the bank or money services business should treat that person as a customer for the purposes of this paragraph, and verify both the person who accessed the account and the customer.

6. Revise § 1010.313 to read as follows:

§ 1010.313 Aggregation.

(a) *Multiple branches*. A financial institution includes all of its domestic branch offices, and any recordkeeping facility, wherever located, that contains records relating to the transactions of the institution's domestic offices, for purposes of the transactions in currency reporting requirements in this chapter.

(b) *Multiple transactions in currency*. In the case of financial institutions other than casinos, for purposes of the transactions in currency reporting requirements in this chapter, multiple currency transactions shall be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than $10,000 during any one business day (or in the case of the U.S. Postal Service, any one day). Deposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit.

(c) *Multiple transactions in convertible virtual currency or digital assets with legal*

tender status. In the case of banks and money services businesses, for purposes of the transactions in convertible virtual currency and digital assets with legal tender status reporting requirements in this chapter, multiple convertible virtual currency and digital assets with legal tender status transactions shall be treated as a single transaction if the bank or money services business has knowledge that they are by or on behalf of any person and result in value in or value out of convertible virtual currency or digital assets with legal tender status with a value of more than $10,000 during a 24-hour period. A bank or money services business includes all of its offices and records, wherever they may be located, for purposes of reporting requirements in this chapter for their transactions in convertible virtual currency or digital assets with legal tender status.

7. Amend § 1010.314 by revising the introductory text and paragraphs (a) and (b) to read as follows:

§ 1010.314 Structured transactions.

No person shall for the purpose of evading the transactions in currency or transactions in convertible virtual currency or digital assets with legal tender status reporting requirements of this chapter with respect to such transaction:

(a) Cause or attempt to cause a domestic financial institution to fail to file a report required under the transactions in currency or transactions in convertible virtual currency or digital assets with legal tender status reporting requirements of this chapter;

(b) Cause or attempt to cause a domestic financial institution to file a report required under the transactions in currency or transactions in convertible virtual currency or digital assets with legal tender status reporting requirements of this chapter that contains a material omission or misstatement of fact; or

* * * * *

8. Add § 1010.316 to read as follows:

§ 1010.316 - Filing obligations for reports of transactions in convertible virtual

currency and digital assets with legal tender status.

(a) For purposes of this section only, FinCEN has determined that "monetary instruments" as defined by 31 U.S.C. 5312(a)(3) includes convertible virtual currency and digital assets with legal tender status.

Note to paragraph (a): The determination in paragraph (a) authorizes the promulgation of reporting requirements for transactions in convertible virtual currency and digital assets with legal tender status pursuant to 31 U.S.C. 5313(a). However, the determination in paragraph (a) is intended to have no impact on the definition of the term "monetary instruments" at § 1010.100(dd) or as used elsewhere in this chapter, including in relation to the currency transaction reporting requirement at § 1010.311 and the transportation of currency or monetary instruments reporting requirement at § 1010.340. Therefore, other requirements in this chapter that depend on the definition of "monetary instruments" are not affected by the determination in paragraph (a).

(b) Except as exempted by paragraph (d) or otherwise exempted by regulation, each bank or money services business, as defined in § 1010.100, shall file a report of each deposit, withdrawal, exchange, or other payment or transfer, by, through, or to such financial institution which involves a transaction in convertible virtual currency or a digital asset with legal tender status with a value of more than $10,000. Such report shall include, in a form prescribed by the Secretary, the name and address of each counterparty, and such other information as the Secretary may require.

(c) For purposes of paragraphs (a) and (b):

(1) Convertible virtual currency means a medium of exchange (such as cryptocurrency) that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status.

(2) Digital assets with legal tender status means any type of digital asset issued by the United States or any other country that is designated as legal tender by the issuing country and

accepted as a medium of exchange in the country of issuance.

(d) Banks and money services businesses are not required to file a report under paragraph (b) in relation to a transaction in convertible virtual currency or a digital asset with legal tender status that is between the financial institution's customer and a counterparty whose account is held at a financial institution regulated under the BSA, or at a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the List of Foreign Jurisdictions Subject to this section and § 1010.410(g) Recordkeeping, which is maintained on FinCEN's Web site on the Resources page. If a single transaction involves multiple counterparties, the transaction is only subject to this exemption if the account of each counterparty to the transaction is held at a financial institution regulated under the BSA, or at a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the List of Foreign Jurisdictions Subject to this section and § 1010.410(g) Recordkeeping.

9. Amend § 1010.410 by adding paragraph (g) to read as follows:

§ 1010.410 - Records to be made and retained by financial institutions.

* * * * *

(g) Each bank or money services business, as defined by 31 CFR 1010.100, is subject to the requirements of this paragraph (g) with respect to a withdrawal, exchange or other payment or transfer, by, through, or to such financial institution which involves a transaction in convertible virtual currency or a digital asset with legal tender status, as those terms are defined in § 1010.316(c), with a value of more than $3,000.

(1) *Recordkeeping Requirements:* For each withdrawal, exchange, or other payment or transfer, by, through, or to such financial institution which involves a transaction in convertible virtual currency or a digital asset with legal tender status, as those terms are defined in § 1010.316(c), a bank or money services business shall obtain and retain an electronic record of the following information:

(i) The name and address of the financial institution's customer;

(ii) The type of convertible virtual currency or legal tender digital assets used in the transaction;

(iii) The amount of convertible virtual currency or legal tender digital assets in the transaction;

(iv) The time of the transaction;

(v) The assessed value of the transaction, in dollars, based on the prevailing exchange rate at the time of the transaction;

(vi) Any payment instructions received from the financial institution's customer;

(vii) The name and physical address of each counterparty to the transaction of the financial institution's customer, as well as other counterparty information the Secretary may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to § 1010.316(b);

(viii) Any other information that uniquely identifies the transaction, the accounts, and, to the extent reasonably available, the parties involved; and,

(ix) Any form relating to the transaction that is completed or signed by the financial institution's customer.

(2) *Verification:* In addition to obtaining and retaining the information required in paragraph (g)(1) of this section, before concluding any transaction in relation to which records must be retained under this paragraph, a financial institution shall verify the identity of its customer engaging in the transaction. Consistent with the financial institution's anti-money laundering and countering the financing of terrorism program, the financial institution should establish risk-based procedures for verifying the identity of its customer. The procedures must enable the financial institution to form a reasonable belief that it knows the true identity of its customer engaging in a transaction. These procedures must be based on the financial institution's assessment of the relevant risks, including those presented by the nature of its relationship with

its customer, the transaction activity, and other activity associated with the convertible virtual currency or digital assets with legal tender status involved in the transaction.

Note to paragraph (g)(2): If a bank or money services business has knowledge that a person has accessed the bank's or money services business's customer's wallet to conduct a transaction for which records must be maintained who is not the bank's or money services business's customer, the bank or money services business should treat that person as a customer for the purposes of this paragraph, and verify both the person accessing the account and the customer.

(3) *Retrievability.* The information that a financial institution must retain under paragraphs (g)(1) and (g)(2) of this section shall be retrievable by the financial institution by reference to the name or account number of the financial institution's customer, or the name of a counterparty to the financial institution's customer's transaction. This information need not be retained in any particular manner, so long as the financial institution is able to retrieve the information required by this paragraph, either by accessing records directly or through reference to some other record maintained by the financial institution.

(4) *Exceptions*. Banks and money services businesses are not required to retain records under this subsection in relation to a transaction in convertible virtual currency or a digital asset with legal tender status that is between the financial institution's customer and a counterparty whose account is held at a financial institution regulated under the BSA, or at a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the List of Foreign Jurisdictions Subject to 31 CFR § 1010.316 Reporting and § 1010.410(g) Recordkeeping, which is maintained on FinCEN's Web site on the Resources page.

PART 1020 – RULES FOR BANKS

10. The authority citation for part 1020 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C. 5311-5314 and 5316-5332; title III, sec. 314, Pub. L. 107-56, 115 Stat. 307; sec. 701, Pub. L. 114-74, 129 Stat. 599.

11. Revise § 1020.310 to read as follows:

§ 1020.310 Reports of transactions in currency, convertible virtual currency, and digital assets with legal tender status.

The reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status requirements for banks are located in subpart C of part 1010 of this chapter and this subpart.

12. Revise § 1020.312 to read as follows:

§ 1020.312 Identification required.

Refer to § 1010.312 of this chapter for identification requirements for reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status filed by banks.

13. Revise § 1020.313 to read as follows:

§ 1020.313 Aggregation.

Refer to § 1010.313 of this chapter for reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status aggregation requirements for banks.

14. Amend § 1020.315 by:

a. Revising paragraphs (a), (b)(4) and (5), (b)(6) introductory text and (b)(7) introductory text;

b. Adding paragraph (c)(2)(iii); and

c. Revising (g)(1) and (3), and (h).

The addition and revisions read as follows:

§ 1020.315 Transactions of exempt persons.

(a) *General*. (1) No bank is required to file a report otherwise required by § 1010.311 with respect to any transaction in currency between an exempt person and such bank, or, to the extent provided in paragraph (e)(6) of this section, between such exempt person and other banks affiliated with such bank. (A limitation on the exemption described in this paragraph (a) is set

forth in paragraph (f) of this section.)

(2) No bank is required to file a report otherwise required by § 1010.316 with respect to any transaction in convertible virtual currency or digital assets with legal tender status between an exempt person defined in paragraphs (b)(1) to (3) of this section and such bank, or, to the extent provided in paragraph (e)(6) of this section, between such exempt person and other banks affiliated with such bank. (A limitation on the exemption described in this paragraph (a) is set forth in paragraph (f) of this section.)

(b) * * *

(4) Solely for purposes of the exemption applicable to any transaction in currency in paragraph (a)(1) of this section, any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stock or interests listed under the separate "NASDAQ Capital Markets Companies" heading), provided that, for purposes of this paragraph (b)(4), a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;

(5) Solely for purposes of the exemption applicable to any transaction in currency in paragraph (a)(1) of this section, any subsidiary, other than a bank, of any entity described in paragraph (b)(4) of this section (a "listed entity") that is organized under the laws of the United States or of any State and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity, provided that, for purposes of this paragraph (b)(5), a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;

(6) Solely for purposes of the exemption applicable to any transaction in currency in paragraph (a)(1) of this section, to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts, any other commercial enterprise (for

purposes of this section, a “non-listed business”), other than an enterprise specified in paragraph (e)(8) of this section, that:

* * * * *

(7) Solely for purposes of the exemption applicable to any transaction in currency in paragraph (a)(1) of this section, with respect solely to withdrawals for payroll purposes from existing exemptible accounts, any other person (for purposes of this section, a “payroll customer”) that:

* * * * *

(c) * * *

(2) * * *

(iii) A bank is not required to file a FinCEN Form 110 with respect to the transfer of convertible virtual currency or digital assets with legal tender status to or from any exempt person as described in paragraphs (b)(1) to (3) of this section.

* * * * *

(g) * * *

(1) No bank shall be subject to penalty under this chapter for failure to file a report required by § 1010.311 or § 1010.316 of this chapter with respect to a transaction in currency, convertible virtual currency, or digital assets with legal tender status by an exempt person with respect to which the requirements of this section have been satisfied, unless the bank:

* * * * *

(3) A bank that files a report with respect to a currency, convertible virtual currency, or digital asset with legal tender status transaction by an exempt person rather than treating such person as exempt shall remain subject, with respect to each such report, to the rules for filing reports, and the penalties for filing false or incomplete reports that are applicable to reporting of transactions in currency, convertible virtual currency, or digital assets with legal tender status by persons other than exempt persons.

(h) Obligations to file suspicious activity reports and maintain system for monitoring transactions in currency, convertible virtual currency, or digital assets with legal tender status.

(1) Nothing in this section relieves a bank of the obligation, or reduces in any way such bank's obligation, to file a report required by §1020.320 with respect to any transaction, including any transaction in currency, convertible virtual currency, or digital assets with legal tender status, that a bank knows, suspects, or has reason to suspect is a transaction or attempted transaction that is described in §1020.320(a)(2)(i), (ii), or (iii), or relieves a bank of any reporting or recordkeeping obligation imposed by this chapter (except the obligation to report transactions in currency, convertible virtual currency, or digital assets with legal tender status, pursuant to this chapter to the extent provided in this section). Thus, for example, a sharp increase from one year to the next in the gross total of currency transactions made by an exempt customer, or similarly anomalous transactions trends or patterns, may trigger the obligation of a bank under §1020.320.

15. Add § 1020.316 to read as follows:

§ 1020.316 Convertible virtual currency and digital assets with legal tender status filing obligations.

Refer to § 1010.316 of this chapter for reports of transactions in convertible virtual currency and digital assets with legal tender status filing obligations for banks.

PART 1022 – RULES FOR MONEY SERVICES BUSINESSES

16. The authority citation for part 1022 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C. 5311-5314 and 5316-5332; title III, sec. 314, Pub. L. 107-56, 115 Stat. 307; sec. 701, Pub. L. 114-74, 129 Stat. 599.

17. Revise § 1022.310 to read as follows:

§1022.310 Reports of transactions in currency, convertible virtual currency, and digital assets with legal tender status.

The reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status requirements for money services businesses are located in subpart C of part 1010 of this chapter and this subpart.

18. Revise § 1022.312 to read as follows:

§ 1022.312 Identification required.

Refer to § 1010.312 of this chapter for identification requirements for reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status filed by money services businesses.

19. Revise § 1022.313 to read as follows:

§ 1022.313 Aggregation.

Refer to § 1010.313 of this chapter for reports of transactions in currency and transactions in convertible virtual currency and digital assets with legal tender status aggregation requirements for money services businesses.

20. Add § 1022.316 to read as follows:

§ 1022.316 Convertible virtual currency and digital assets with legal tender status filing obligations.

Refer to § 1010.316 of this chapter for reports of transactions in convertible virtual currency filing obligations for money services businesses.

By the Department of the Treasury.

Kenneth A. Blanco
Director
Financial Crimes Enforcement Network

[FR Doc. 2020-28437 Filed: 12/18/2020 4:15 pm; Publication Date: 12/23/2020]