

Alert | Financial Regulatory & Compliance/
Blockchain & Digital Assets



December 2020

FinCEN Proposes to Extend Recordkeeping, Reporting, and Identity Verification Requirements to Certain Virtual Currency and Digital Asset Transactions

On Dec. 18, 2020, the U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) published a [notice of proposed rulemaking](#) (NPRM) that would impose on **banks and money services businesses** (MSBs) new recordkeeping, reporting, and identity verification requirements for certain transactions involving convertible virtual currency (CVC) and digital assets with legal tender status (LTDA) held in “unhosted wallets,” i.e., wallets not hosted by a financial institution, or “otherwise covered wallets,” i.e., wallets held at a financial institution that is not subject to the U.S. Bank Secrecy Act (BSA) and is located in a certain high-risk foreign jurisdiction identified by FinCEN (currently, Burma, Iran, and North Korea). The NPRM proposes to exclude from its ambit other types of financial institutions that are subject to BSA requirements such as broker-dealers, futures commission merchants and mutual funds but requests comment on whether these and other types of financial institutions should be subject to the proposed rule. As outlined below, these proposed changes, if promulgated into law without change, would impose substantial new requirements on banks and MSBs, together with as-yet-to-be-quantified burdens and costs.

As background on its genesis, the NPRM notes that although digital payments (including CVC payments) present substantial benefits – including improving access to financial services, reducing inefficiencies, and lowering costs – CVC is also used in illicit financial activity. FinCEN notes that illicit finance risk involving CVC is heightened when users engage with CVC through unhosted wallets or wallets hosted by a foreign financial institution not subject to effective anti-money laundering (AML) regulations.

Proposed Expansion of Recordkeeping and Reporting Requirements

The NPRM would require banks and MSBs to identify and verify hosted-wallet customers who conduct transactions in excess of \$3,000 in CVC or LTDA with an unhosted or otherwise covered wallet counterparty, and to collect and retain information (i.e., name and physical address) concerning the customer's counterparties.

The NPRM would also require banks and MSBs to report and keep records of transactions over \$10,000 between their customers' CVC/LTDA-hosted wallets and unhosted or otherwise covered wallets flowing into or out of the bank/MSB customers' CVC/LTDA-hosted wallets. The proposed form to be filed for reporting these transactions **would be similar, but distinct from**, the Currency Transaction Report (CTR) that these financial institutions use to report cash transactions over \$10,000. The form would require the bank/MSB to report information on the financial institution filer, the transaction, the hosted-wallet customer, and each counterparty (i.e., name and physical address).¹

The NPRM proposes to base value measurements for purposes of recordkeeping and reporting thresholds on the "prevailing exchange rate" of the CVC/LTDA at the time of the transaction. The term "prevailing exchange rate" would be defined as a "rate reasonably reflective of fair market rate of exchange available to the public for the CVC/LTDA at the time of the transaction." The preamble also indicates that banks and MSBs would be expected to document their method for determining the prevailing exchange rate.

Aggregation

Similar to the CTR aggregation requirement, the NPRM would impose an aggregation requirement if the bank/MSB has knowledge that CVC/LTDA transactions are by or on behalf of a single person and result in value in or value out of CVC/LTDA above the \$10,000 threshold during a 24-hour period. The 24-hour period for aggregation of CVC/LTDA transactions deviates from the business-day aggregation period for CTR reporting of cash transactions. This discrepancy is one that must be addressed by FinCEN to ensure effective compliance by banks and MSBs with the NPRM. The NPRM provides that CVC/LTDA transactions and cash transactions would be aggregated separately for purposes of their respective reporting requirements.

The NPRM would also add a new aggregation requirement that is not found in the cash CTR requirements, namely, a requirement to aggregate CVC/LTDA transactions across all offices and records of the bank/MSB, wherever they may be located. Additionally, foreign-located MSBs must comply with the proposed CVC/LTDA transaction reporting requirements and the aggregation requirement, with respect to their activities in the United States.

No aggregation would be required for purposes of the \$3,000 recordkeeping requirement.

¹ FinCEN expects that banks and MSBs will follow risk-based procedures, consistent with their AML programs, to determine whether to obtain additional information about their customer's counterparties or take steps to verify counterparty information for purposes of both recordkeeping and reporting requirements.

Recordkeeping and Verification Requirements for Transactions Over \$3,000

As stated above, the NPRM would also require banks and MSBs to keep records of a customer's CVC or LTDA transactions and counterparties, including verifying the identity of their customers, if a counterparty is using an unhosted or otherwise covered wallet and the transaction (into or out of the bank or MSB) is greater than \$3,000. Recordkeeping and verification would need to be completed before a transaction could be conducted. The information that would need to be collected and maintained includes:

- (i) the name and address of the bank/MSB customer;
- (ii) the type of CVC or LTDA used in the transaction;
- (iii) the amount of CVC or LTDA 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 bank/MSB customer;
- (vii) the name and physical address of each counterparty to the transaction, as well as other counterparty information that the Secretary may prescribe as mandatory on the reporting form;
- (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 bank/MSB customer.

Identity Verification and Recordkeeping Requirements

The NPRM would require banks and MSBs to verify and record the identity of their customer engaged in a transaction covered by the NPRM (to include verifying the identity of the person accessing the customer's account; this may be someone conducting a transaction on the customer's behalf). Again, banks and MSBs would be expected to complete recordkeeping and verification before a transaction is conducted. In the case where the bank or MSB customer is the recipient, the bank or MSB would need to obtain the required recordkeeping and verification information as soon as practicable.

Banks and MSBs would be expected to incorporate policies and procedures to address instances where they are unable to obtain the required information, such as by terminating the customer's account in appropriate circumstances. Furthermore, consistent with the bank or MSB's AML program, the bank or MSB would need to establish risk-based procedures for verifying their hosted-wallet customers' identities and ensure these are sufficient to enable the bank or MSB to form a reasonable belief that it knows the true identity of its customers.

Exceptions

The NPRM would exempt from reporting and recordkeeping requirements transactions between a bank/MSB's hosted-wallet customer and a counterparty-hosted wallet at a financial institution that is either: (i) regulated under the BSA or (ii) located in a foreign jurisdiction that is not identified on the "Foreign Jurisdictions List," which FinCEN proposes to establish for purposes of the NPRM. The Foreign Jurisdictions List, initially, would be comprised of jurisdictions designated by FinCEN as jurisdictions of primary money laundering concerns (i.e., Burma, Iran, and North Korea), but FinCEN could expand this list to include jurisdictions identified as having significant deficiencies in their regulation of CVC/LTDA.

The preamble to the NPRM explains that, prior to applying the exemption, 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 a Foreign Jurisdictions List. In analyzing whether a counterparty's wallet is hosted by a BSA-regulated MSB, financial institutions would be expected to ensure that the MSB is registered with FinCEN. In determining whether the exemption would apply 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 a Foreign Jurisdiction 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.

Request for Comments

While FinCEN seeks comments on all aspects of the NPRM, FinCEN has specifically requested comments with respect to 24 questions, several which could result in significantly expanding the coverage of the NPRM. For example, FinCEN inquires about the costs and benefits of applying the reporting requirement to all CVC/LTDA transactions by hosted wallets, including those with hosted-wallet counterparties, and extending reporting obligations to other financial institutions such as broker-dealers, futures commissions merchants, and mutual funds.

Significantly, the NPRM breaks with the traditional 30- to 60-day comment period and provides only 15-days for public comments. Written comments on the NPRM must be submitted to FinCEN no later than **Jan. 4, 2021**.

FinCEN attempted to justify the short comment period by explaining that significant national security imperatives require a quick proposal and implementation of a final rule, and warning that "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 wallets or otherwise covered wallets." The crypto industry is strongly pushing back on the NPRM, and requests for extensions to the comment period have been filed. Legal challenges to the final rule are almost certain, particularly if an extension to the comment period is not granted.²

² See, for example, [statements published by Coin Center](#) and [tweet by Coinbase CEO Brian Armstrong](#).

Authors

This GT Alert was prepared by:

- [Carl A. Fornaris](#) | +1 305.579.0626 | fornarisc@gtlaw.com
- [Kyle R. Freeny](#) | +1 202.331.3118 | freenyk@gtlaw.com
- [Marina Olman-Pal](#) | +1 305.579.0779 | olmanm@gtlaw.com
- [Rosemarie Aleman](#) | +1 305.579.0733 | alemanr@gtlaw.com
- [Claudio J. Arruda](#) | +1 305.579.0874 | arrudac@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.~ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan. » Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.* Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ~Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. »Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.*