(BILLINGCODE: 4810-02-P)

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

31 CFR Chapter X, Part 1010

RIN 1506-AB64

Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern

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

ACTION: Notice of proposed rulemaking.

SUMMARY: FinCEN is issuing a notice of proposed rulemaking (NPRM), pursuant to section 311 of the USA PATRIOT Act, that proposes requiring domestic financial institutions and domestic financial agencies to implement certain recordkeeping and reporting requirements relating to transactions involving convertible virtual currency (CVC) mixing.

DATES: Written comments on the notice of proposed rulemaking must be submitted on or before [INSERT DATE 90 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER.]

ADDRESSES: Comments must be submitted by one of the following methods:

- *Federal E-rulemaking Portal:* https://www.regulations.gov. Follow the instructions for submitting comments. Refer to Docket Number FINCEN–2023–0016 in the submission.

- *Mail*: Financial Crimes Enforcement Network, P.O. Box 39, Vienna, VA 22183. Refer to Docket Number FINCEN–2023–0016 in the submission.

Please submit comments by one method only, and note that comments submitted in responses to this NPRM will become a matter of public record.

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

SUPPLEMENTARY INFORMATION:

I. Statutory Provisions

Section 311 of the USA PATRIOT Act (section 311), codified at 31 U.S.C. 5318A, grants the Secretary of the Treasury (Secretary) authority, upon finding that reasonable grounds exist for concluding that one or more classes of transactions within or involving a jurisdiction outside of the United States is of primary money laundering concern, to require domestic financial institutions and domestic financial agencies to take certain "special measures."[1] The authority of the Secretary to administer section 311 and the Bank Secrecy Act (BSA) has been delegated to FinCEN.[2]

The five special measures set out in section 311 are prophylactic safeguards that may be employed to defend the United States financial system from money laundering and terrorist financing risks. The Secretary may impose one or more of these special measures in order to

[1] On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56 (USA PATRIOT Act). Title III of the USA PATRIOT Act amended the anti-money laundering (AML) provisions of the Bank Secrecy Act (BSA) to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. The BSA, as amended, is the popular name for a collection of statutory authorities that FinCEN administers that is codified at 12 U.S.C. §§ 1829b, 1951-1960 and 31 U.S.C. §§ 5311-5314, 5316-5336, and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 CFR Chapter X.

[2] Pursuant to Treasury Order 180-01 (Jan. 14, 2020), the authority of the Secretary to administer the BSA, including, but not limited to, 31 U.S.C. § 5318A, has been delegated to the Director of FinCEN.

protect the U.S. financial system from such threats. Through special measure one, the Secretary may require domestic financial institutions and domestic financial agencies to maintain records, file reports, or both, concerning the aggregate amount of transactions or individual transactions.[3] Through special measures two through four, the Secretary may impose additional recordkeeping, information collection, and reporting requirements on covered domestic financial institutions and domestic financial agencies.[4] Through special measure five, the Secretary may prohibit, or impose conditions upon, the opening or maintaining in the United States of correspondent or payable-through accounts for or on behalf of a foreign banking institution, if the class of transactions found to be of primary money laundering concern may be conducted through such correspondent account or payable-through account.[5]

Before making a finding that reasonable grounds exist for concluding that a class of transactions is of primary money laundering concern, the Secretary is required to consult with both the Secretary of State and the Attorney General.[6] The Secretary is also required to consider such information as the Secretary determines to be relevant, including the following potentially relevant factors:

- The extent to which such class of transactions is used to facilitate or promote money laundering in or through a jurisdiction outside the United States, including any money laundering activity by organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction (WMD) or missiles;
- The extent to which such class of transactions is used for legitimate business purposes in the jurisdiction; and

[3] 31 U.S.C. 5318A(b)(1).
[4] 31 U.S.C. 5318A(b)(2)–(b)(4).
[5] 31 U.S.C. 5318A(b)(5).
[6] 31 U.S.C. 5318A(c)(1).

- The extent to which such action is sufficient to ensure that the purposes of section 311 are fulfilled and to guard against international money laundering and other financial crimes.[7]

Upon finding that a class of transactions is of primary money laundering concern, the Secretary may require covered financial institutions to take one or more special measures. In selecting one or more special measures, the Secretary "shall consult with the Chairman of the Board of Governors of the Federal Reserve System, any other appropriate Federal banking agency (as defined in section 3 of the Federal Deposit Insurance Act), the Secretary of State, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the National Credit Union Administration Board, and in the sole discretion of the Secretary, such other agencies and interested parties as the Secretary may find appropriate."[8]

In addition, the Secretary is required to consider the following factors when selecting special measures:

- Whether similar action has been or is being taken by other nations or multilateral groups;
- Whether the imposition of any particular special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States;
- The extent to which the action or the timing of the action would have a significant adverse systemic impact on the international payment, clearance, and settlement system, or on legitimate business activities involving the particular jurisdiction, institution, class of transactions, or type of account; and
- The effect of the action on United States national security and foreign policy.[9]

[7] 31 U.S.C. 5318A(c)(2)(B).
[8] 31 U.S.C. 5318A(a)(4)(A).
[9] 31 U.S.C. 5318A(a)(4)(B).

II. Summary of NPRM

Convertible Virtual Currency (CVC) mixing entails the facilitation of CVC[10] transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions.[11] Because CVC mixing is intended to make CVC transactions untraceable and anonymous, CVC mixing is ripe for abuse by, and frequently used by, illicit foreign actors that threaten the national security of the United States and the U.S. financial system. By obscuring the connection between the CVC wallet addresses used to receive illicit CVC proceeds and the CVC wallet addresses from which illicit CVC is transferred to CVC-to-fiat[12] currency exchangers, other CVC users, or CVC exchanges, CVC mixing transactions can play a central role in facilitating the laundering of CVC derived from a variety of illicit activity.

Indeed, CVC mixing transactions are frequently used by criminals and state actors to facilitate a range of illicit activity, including, but not limited to, money laundering, sanctions evasion and WMD proliferation by the Democratic People's Republic of Korea (DPRK or North Korea), Russian-associated ransomware attacks,[13] and illicit darknet markets. Further, a recent assessment by FinCEN determined that the percentage of CVC transactions processed by CVC mixers that originated from likely illicit sources is increasing.[14] CVC mixing often involves foreign jurisdictions because persons who facilitate or engage in CVC mixing transactions are often located abroad, including notable recent CVC mixing activity involving DPRK-affiliated threat actors, Russian ransomware actors, and buyers and sellers on Russian darknet markets.

[10] For the purposes of this NPRM, the term "CVC" is defined as a medium of exchange that either has an equivalent value as currency or acts as a substitute for currency, but lacks legal tender status. Although Bitcoin has legal tender status in at least two jurisdictions, the term "CVC" includes Bitcoin.
[11] A more detailed definition of this term is provided in Section IX of this NPRM.
[12] Fiat currency refers to traditional currency such as the U.S. dollar
[13] Notwithstanding the use of "attack" as a legal term of art in certain settings, FinCEN here and throughout intends only the colloquial meaning of the term.
[14] A more detailed examination of analysis is below in Section IV.A.3 of this NPRM.

Accordingly, because CVC mixing provides foreign illicit actors with enhanced anonymity that allows them to launder their illicit proceeds, FinCEN assesses that transactions involving CVC mixing within or involving a jurisdiction outside the United States are of primary money laundering concern, and, having undertaken the necessary consultations, also finds that imposing additional recordkeeping and reporting requirements would assist in mitigating the risks posed by such transactions. Such reporting will assist law enforcement with identifying the perpetrators behind illicit transactions and preventing, investigating, and prosecuting illegal activity, as well as rendering such transactions—through increased transparency—less attractive and useful to illicit actors. This NPRM (1) sets forth FinCEN's finding that transactions involving CVC mixing within or involving jurisdictions outside the United States are a class of transactions that are of primary money laundering concern; and (2) proposes, under special measure one, requiring covered financial institutions to implement certain recordkeeping and reporting requirements on transactions that covered financial institutions know, suspect, or have reason to suspect involve CVC mixing within or involving jurisdictions outside the United States.

III. Background

Although the United States supports innovation and advances in digital and distributed ledger technology for financial services, it must also consider the substantial implications that such technology has for national security and mitigate the attendant risks for consumers, businesses, national security, and the integrity of the broader U.S. financial system.[15] CVC can be used for legitimate and innovative purposes. However, it is not without its risks and, in

[15] White House, *Executive Order on Ensuring Responsible Development of Digital Assets Fact Sheet*, Mar. 9, 2022, *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/.

particular, the use of CVC to anonymize illicit activity undermines the legitimate and innovative uses of CVC.

A. *CVC mixing and its mechanisms*

The term "virtual currency" refers to a medium of exchange that can operate like currency but does not have all the attributes of "real," or fiat, currency. CVC is a type of virtual currency that either has an equivalent value as currency or acts as a substitute for currency and is therefore a type of "value that substitutes for currency." The label applies to any particular type of CVC, such as "digital currency," "cryptocurrency," "cryptoasset," and "digital asset."[16, 17]

The public nature of most CVC blockchains,[18] which provide a permanent, recorded history of all previous transactions, make it possible to know someone's entire financial history on the blockchain. Anonymity enhancing tools, including "mixers," are used to avoid this. To provide enhanced anonymity, CVC mixers provide a service—CVC mixing—that is intended to obfuscate transactional information, allowing users to obscure their connection to the CVC.

There are a number of ways to conduct CVC mixing transactions—one of the most common of which is the use of CVC mixers. CVC mixers can accomplish this through a variety of mechanisms, including: pooling or aggregating CVC from multiple individuals, wallets, or accounts into a single transaction or transactions; splitting an amount into multiple amounts and

---

[16] *See*, *e.g.*, FinCEN, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, May 9, 2019, *available at* https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (FinCEN 2019 CVC Guidance).

[17] FinCEN notes that CVC or "virtual currency" by itself does not meet the definition of a "currency" under 31 C.F.R. 1010.100(m). Additionally, potential characterization of CVC as currency, securities, commodities, or derivatives for the purposes of any other legal regime, such as the Federal securities laws or the Commodity Exchange Act, is outside the scope of this proposed rule. However, as described in the FinCEN 2019 CVC Guidance, if assets that other regulatory frameworks defined as commodities, securities, or futures contracts were to be specifically issued or later repurposed to serve as a currency substitute, then the asset itself could be a type of value that substitutes for currency and be defined as CVC for the purposes of this proposed rule, in addition to being subject to other applicable regulatory frameworks.

[18] Blockchain refers to a type of distributed ledger technology (DLT) that cryptographically signs transactions that are grouped into blocks. For more information on blockchain, *see* National Institute of Science and Technology, *Blockchain*, *available at* https://www.nist.gov/blockchain.

transmitting the CVC as a series of smaller independent transactions; or leveraging code to coordinate, manage, or manipulate the structure of the transaction; among other methods. Through such mechanisms, CVC mixers can functionally simulate a customer depositing funds from an anonymous account into a financial institution's omnibus account and withdrawing funds into a separate anonymous account.[19] For example, a criminal actor could take the illicit proceeds of their crime, send the CVC to a CVC mixer, and then on to an account they hold at a virtual asset service provider (VASP). At this point, the VASP would take custody of the illicitly sourced CVC, thereby allowing illicit funds to enter their omnibus account, all while being unaware of the origin of the illicit CVC. The critical challenge is that CVC mixing services rarely, if ever, provide to regulators or law enforcement the resulting transactional chain or information collected as part of the transaction.

CVC mixing does not, however, wholly rely on the use of CVC mixers. There are certain methods that CVC users—and CVC mixers—often employ in an effort to obfuscate their transactions. These methods include:

a. *Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts*: This method involves combining CVC from two or more persons into a single wallet or smart contract and, by pooling or aggregating that CVC, obfuscating the identity of both parties to the transaction by decreasing the probability of determining both intended persons for each unique transaction.

b. *Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions*: This method involves splitting a single transaction from sender to receiver

[19] *See* U.S. Department of the Treasury (Treasury), *DeFi Risk Assessment*, Apr. 2023, at p. 19, *available at* https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (Treasury April 2023 Defi Risk Assessment).

into multiple, smaller transactions, in a manner similar to structuring, to make transactions blend in with other, unrelated transactions on the blockchain occurring at the same time so as to not stand out, thereby decreasing the probability of determining both intended persons for each unique transaction.

c. *Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction*: This method involves the use of software that coordinates two or more persons' transactions together in order to obfuscate the individual unique transactions by providing multiple potential outputs from a coordinated input, decreasing the probability of determining both intended persons for each unique transaction.

d. *Creating and using single-use wallets, addresses, or accounts and sending CVC through these wallets, addresses, or accounts in a series of transactions*: This method involves the use of single-use wallets, addresses, or accounts—colloquially known as a "peel chain"—in a series of unnatural transactions that have the purpose or effect of obfuscating the source and destination of funds by volumetrically increasing the number of involved transactions, thereby decreasing the probability of determining both intended persons for each unique transaction.

e. *Exchanging between types of CVC, or other digital assets*: This method involves exchanges between two or more types of CVC or other digital assets—colloquially referred to as "chain hopping"—to facilitate transaction obfuscation by converting one CVC into a different CVC at least once before moving the funds to another service or

platform thereby decreasing the probability of determining both intended persons for each unique transaction.[20]

f. *Facilitating user-initiated delays in transactional activity:* This method involves the use of software, programs, or other technology that programmatically carry out pre-determined timed-delay of transactions by delaying the output of a transaction in order to make that transaction appear to be unrelated to transactional input, thereby decreasing the probability of determining both intended persons for each unique transaction.

B. *Use of CVC mixing by illicit foreign actors*

Illicit actors use enhanced anonymity on the blockchain to avoid detection by authorities as they launder their illicit proceeds. By obfuscating identity and preventing the attribution of ownership of CVC,[21] CVC mixing allows illicit actors, such as cyber threat actors carrying out ransomware attacks or cyber heists, to launder their CVC and convert it into fiat currency, minimizing the risk of being detected by involved financial institutions, including VASPs, or relevant authorities. Because wallet addresses are pseudonymous and CVC mixing severs the connection between the identity of users sending and receiving CVC, illicit actors are able to exploit vulnerabilities in anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory frameworks,[22] threatening the effectiveness of rules which require financial institutions to, among other things, know the identity of their customers and report suspicious activity to FinCEN.

[20] FinCEN, Financial Trend Analysis, *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*, Oct. 15, 2021, at p. 13, *available at* https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf (FinCEN October 2021 FTA).
[21] Users employ digital wallets to hold their CVC. These wallets appear on the blockchain as a string of alphanumeric characters, but can be created using software at will, and are not directly tied to any individual person's identity.
[22] *See* Treasury April 2023 Defi Risk Assessment, at pp. 3-4, 28.

Over the past few years, Treasury has monitored, and expressed concern with, the increasing use of CVC mixing by illicit actors, including North Korea-affiliated cyber threat actors, ransomware actors, and darknet market[23] participants, to transfer and launder their illicit proceeds. In particular, the DPRK—already under pressure from robust United States, European Union, United Kingdom, and United Nations sanctions—relies upon CVC mixing to launder the proceeds of cyber heists in order to finance the DPRK's WMD program.[24] The Axie Infinity Ronin Bridge (Axie Infinity) heist—committed in March 2022, worth almost $620 million and carried out by the DPRK-controlled Lazarus Group—remains, for instance, the largest cyber heist to date,[25] and made high profile use of at least two mixers to launder the proceeds of the theft—Blender.io and Tornado Cash.[26]

CVC mixing is also commonly used to obfuscate the source of CVC obtained through other illicit activities, such as ransomware attacks and the use and operation of darknet markets. For example, between January 2021 and June 2021, the top 10 most common ransomware variants reported in suspicious activity report (SAR) data, including several Russian-affiliated

---

[23] "Darknet" is a term used to refer to networks that are only accessible through the use of specific software or network configurations. Darknet content is not indexed by web search engines, and is often accessed via anonymized, encrypted systems like the software The Onion Router (TOR). Darknet markets are online markets only accessible with the use of software like TOR, and because they are not indexed, can only be found if the domain name and URL are already known to the user. As a result of the inherent anonymity of the darknet infrastructure, darknets facilitate criminal activity because of the difficulty involved for law enforcement in identifying users, infrastructure, and even domains associated with the sale of illicit goods and services. FinCEN's August 2021 publicly available assessment of a civil money penalty against an exchange noted that darknet marketplaces actively promote CVC mixers as the primary method for obfuscating CVC transactions.

[24] United Nations, *UN Panel of Experts Letter,* S/2023/171, Mar. 7, 2023, at p. 4, *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement (UN March 2023 Experts Letter); *see* Wall Street Journal, *North Korea Suspected of Plundering Crypto to Fund Weapons Programs*, July 1, 2022, *available at* https://www.wsj.com/articles/north-korea-suspected-of-plundering-crypto-to-fund-weapons-programs-11656667802.

[25] Office of Foreign Assets Control (OFAC), *U.S. Treasury issues First Ever Sanctions on Virtual Currency Mixer, Targets DPRK Cyber Threats,* May 6, 2022, *available at* https://home.treasury.gov/news/press-releases/jy0768 (U.S. Treasury May 2022 Press Release); *see* Elliptic, *North Korea's Lazarus Group Identified as Exploiters Behind $540 Million Ronin Bridge Heist*, Apr. 14, 2022, *available at* https://www.elliptic.co/blog/540-million-stolen-from-the-ronin-defi-bridge.

[26] OFAC*, Treasury Designates DPRK Weapons Representative*, Nov. 8, 2022, *available at* https://home.treasury.gov/news/press-releases/jy1087 (U.S. Treasury November 2022 Press Release).

variants, sent approximately $35.2 million to CVC mixers and $252 million to darknet markets.[27] Indeed, darknet marketplaces actively promote CVC mixers as the primary method for obfuscating related transactions, and, indeed, multiple CVC mixers historically interacted with Hydra, the former Russian darknet market that accounted for approximately 80 percent of all darknet market CVC transactions in 2021 before being shut down by United States and German law enforcement.[28] Because darknet marketplaces are fundamentally illicit in nature, FinCEN assesses that illicit actors using darknet markets to purchase or sell illicit goods favor the ability to reduce the odds of being identified and leverage CVC mixing to enhance anonymity to that end. Similarly, ransomware actors also prefer an opportunity to successfully launder their illicit funds by using CVC mixing to enhance anonymity.

The multiple U.S. Government actions against CVC mixers, often in coordination with international partners, demonstrate that CVC mixing provides illicit actors with enhanced anonymity in CVC transactions, allowing them to more easily launder their illicit proceeds in CVC.[29]

[27] *See* FinCEN October 2021 FTA, at p. 17.
[28] U.S. Department of Justice (DOJ), *Justice Department Investigation Leads To Shutdown Of Largest Online Darknet Marketplace*, Apr. 5, 2022, *available at* https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.
[29] FinCEN, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws*, Oct. 19, 2020, *available at* https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws (First Bitcoin "Mixer" Penalized by FinCEN, October 19, 2020); DOJ, *Ohio Resident charged operating darknet based bitcoin mixer laundered over 300 million*, Feb. 13, 2020, *available at* https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million; DOJ, *Justice Department Investigation leads to takedown of Darknet cryptocurrency mixer processed over $3 billion of unlawful transactions*, Mar. 15, 2023, *available at* https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3 (DOJ March 2023 Press Release); U.S. Treasury November 2022 Press Release.

IV. Finding that transactions that involve CVC mixing within or involving a jurisdiction outside the United States are a class of transactions of primary money laundering concern

Pursuant to 31 U.S.C. 5318A(a)(1), FinCEN finds that reasonable grounds exist for concluding that transactions involving CVC mixing within or involving a jurisdiction outside the United States are a class of transactions that is of primary money laundering concern. In making this finding, FinCEN considered the following statutory factors: (1) the extent to which the class of transactions is used to facilitate or promote money laundering in or through a jurisdiction outside of the United States, including money laundering activity with connections to international terrorism, organized crime, and proliferation of WMDs and missiles; (2) the extent to which a class of transactions is used for legitimate business purposes; and (3) the extent to which action by FinCEN would guard against international money laundering and other financial crimes.

A. *The extent to which the class of transactions is used to facilitate or promote money laundering in or through a jurisdiction outside the United States, including any money laundering activity by organized criminal groups, international terrorists, or entities involved in the proliferation of WMD and missiles*

FinCEN assesses that foreign CVC mixing transactions are used to facilitate or promote money laundering in or through jurisdictions outside the United States, including by organized criminal groups, international terrorists, or entities involved in the proliferation of WMD and missiles. FinCEN based this assessment on information available to the agency, including both public and non-public reporting, and after thorough consideration of each of the following factors: (1) that transactions involving CVC mixing often occur within, or involve, jurisdictions outside of the United States; (2) that CVC mixing is used to launder proceeds of large-scale CVC theft and heists, and support the proliferation of WMD, in particular, by the DPRK; and (3) that

CVC mixing is similarly used by ransomware actors and darknet markets to launder illicit proceeds.

1. *CVC mixing transactions often occur within or involve jurisdictions outside the United States*

CVC mixers conduct business with opaque operational structures and take steps to avoid the discovery of where they and their users are located. CVC mixers commonly obscure their locations, including (1) employing The Onion Router (TOR) to conceal the location of their servers;[30] (2) failing to register as a business in any jurisdiction; and (3) failing to maintain any activity logs. Based on public and non-public information, FinCEN assesses that CVC mixing activity often occurs within or involves numerous jurisdictions outside the United States and, indeed, throughout the world. The U.S. Department of Justice (DOJ) and open source reporting identified an increase in the use of CVC in terror finance, including by Hamas and the Islamic State of Iraq and Syria (ISIS), and the use of CVC mixers to obfuscate source of funds to protect the identity of their donors.[31] In addition, FinCEN has identified the use of CVC mixing services as a prevalent money laundering typology for the top 10 ransomware strains identified in BSA data from January 2021 to June 2021, and, notably, open source analysis of CVC payments indicates that up to 74 percent of ransomware activity is associated with Russia.[32]

The global nature of the problem is further demonstrated by the fact that no CVC mixers are currently registered with FinCEN. CVC mixers are required to register with FinCEN if they

[30] *See* DOJ March 2023 Press Release.
[31] DOJ, *Four Defendants Charged with Conspiring to Provide Cryptocurrency to ISIS*, Dec. 14, 2022, *available at* https://www.justice.gov/usao-edny/pr/four-defendants-charged-conspiring-provide-cryptocurrency-isis; TRM Labs, *Terrorist Financing Six Crypto Related Trends to Watch in 2022*, Feb. 16, 2023, *available at* https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023.
[32] Chainalysis, *Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity*, Feb. 14, 2022, *available at* https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/.

do business as money transmitters wholly or in substantial part within the United States.[33] To the extent foreign CVC mixers are operating beyond United States jurisdiction, they are not subject to U.S. regulations that require financial institutions to, among other things, know the identity of their customers and report suspicious activity to FinCEN. Nevertheless, FinCEN assesses that other forms of CVC mixing, that do not involve the use of CVC mixers, do occur within the United States.

Recent U.S. and foreign enforcement actions also reflect CVC mixing transactions within or involving numerous foreign jurisdictions, including DPRK, Russia, Luxembourg, the Netherlands, and Vietnam. Office of Foreign Assets Control (OFAC) actions in 2022, for instance, highlighted the links between the DPRK and CVC mixers Blender.io[34] and Tornado Cash[35]—through their respective involvement in the Axie Infinity heist[36] in March 2022 and Tornado Cash's involvement in the Harmony Horizon Bridge (Harmony) heist[37] in June 2022.[38] The coordinated international takedown of ChipMixer, a darknet CVC "mixing" service operated by Vietnamese national Minh Quốc Nguyễn in Hanoi, Vietnam, by the DOJ and the German Federal Criminal Police (Bundeskriminalamt or BKA) on March 15, 2023, and shutdown of

[33] 31 C.F.R. 1010.100(ff).
[34] *See* U.S. Treasury May 2022 Press Release.
[35] *See* U.S. Treasury November 2022 Press Release.
[36] Federal Bureau of Investigation (FBI), *FBI Statement of Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea*, Apr. 14, 2022, *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea.
[37] FBI, *FBI Confirms Lazarus Group, APT 38 Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft*, Jan. 23, 2023, *available at* https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft (FBI January 23, 2023 Press Release).
[38] *See* Dutch Fiscal Information and Investigation Service, *Arrest of suspected developer of Tornado Cash*, Aug. 12, 2022, *available at* https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/; DOJ, *Tornado Cash Founders Charged with Money Laundering and Sanctions Violations*, Aug. 23, 2023, *available at* https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations; OFAC, *Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash*,Aug. 23, 2023, *available at* https://home.treasury.gov/news/press-releases/jy1702; OFAC, *Sanctions List Search*, Aug. 24, 2023, *available at* https://sanctionssearch.ofac.treas.gov/Details.aspx?id=44718.

Bestmixer.io and associated seizure of servers located in the Netherlands and Luxembourg by the Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and Luxembourg authorities on May 22, 2019,[39] similarly demonstrate the international character of CVC mixing transactions—spanning jurisdictions across Europe and Asia.

2. *CVC mixing is used to launder proceeds of large-scale CVC theft and heists*

FinCEN assesses that CVC mixing is used to launder the proceeds of large-scale CVC theft and heists by both state and non-state sponsored actors. Whether heists are carried out by state or non-state actors, the need for CVC mixing is the same—illicit CVC must be laundered, and CVC mixing provides the enhanced anonymity to separate illicitly obtained CVC from the underlying illicit activity.

Non-state-affiliated actors commonly use CVC mixing services to launder their proceeds from large scale heists. The proceeds from the heists that targeted a CVC exchanger[40] and cross-chain bridge Nomad[41] were, for instances, laundered using the Tornado Cash CVC mixer.

In addition to the use of CVC mixing by non-state-affiliated actors, FinCEN assesses that, based on public and non-public reporting, DPRK state-sponsored or -affiliated cyber threat actors are responsible for a substantial portion of illicit or stolen CVC funds sent to CVC mixers,[42] and that the DPRK utilized CVC mixing to launder proceeds in an attempt to obfuscate

---

[39] The European Union Agency for Law Enforcement Cooperation (Europol), *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*, May 22, 2019, *available at* https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down; DOJ March 2023 Press Release.

[40] CoinDesk, *Crypto.com's Stolen Ether Being Mixed Through Tornado Cash* (Updated May 11, 2023), *available at* https://www.coindesk.com/business/2022/01/18/cryptocoms-stolen-ether-being-laundered-via-tornado-cash/; *see* Halborn, *Explained: the Crypto.com Hack (January 2022)*, Jan. 24, 2022, *available at* https://halborn.com/explained-the-crypto-com-hack-january-2022/ (accessed Nov. 15, 2022).

[41] *See* U.S. Treasury November 2022 Press Release; Reuters, *U.S. crypto firm Nomad hit by $190 million theft*, Aug. 3, 2022, *available at* https://www.reuters.com/technology/us-crypto-firm-nomad-hit-by-190-million-theft-2022-08-02/.

[42] *See* Chainalysis, *The Crypto Crime Report 2023*, *available at* https://go.chainalysis.com/2023-crypto-crime-report.html (The 2023 Crypto Crime Report).

its connection to those funds. The DPRK uses the mixed proceeds of these thefts to support its WMD program.[43, 44] A publicly available analysis in February 2021 determined that individuals acting for or on behalf of the North Korean government laundered more than 65 percent of stolen CVC through CVC mixers—an increase from 42 percent in 2020 and 21 percent in 2019.[45] Further, publicly available analysis in February 2022 assessed that the DPRK is a systematic money launderer and that its use of multiple CVC mixers is a calculated attempt to obscure the origins of its ill-gotten CVCs while converting them into fiat currency.[46] In the same year, there was a notable increase in large scale heists carried out by, or in support of, the DPRK, with associated use of CVC mixing and CVC mixers. OFAC sanctioned two CVC mixers, Blender.io and Tornado Cash, used to launder illicit proceeds of the March 2022 Axie Infinity heist and the June 2022 Harmony heist, both of which were carried out by North Korea's Lazarus Group.[47, 48] In addition, DOJ has determined that ChipMixer processed over $700 million in Bitcoin associated with wallet addresses identified as containing stolen CVC, including CVC related to the Axie Infinity and the Harmony heists.[49] The Federal Bureau of Investigation (FBI) has also determined that North Korean cyber actors laundered over $60 million worth of Ethereum stolen

[43] *See* U.S. Treasury November 2022 Press Release; *see also* FinCEN, *Imposition of Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern*, 81 FR 78715, Nov. 9, 2016, *available at* https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf (FinCEN 2016 Imposition of Special Measure Against North Korea).
[44] *See* UN March 2023 Experts Letter, at p. 4.
[45] Chainalysis, Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022, Jan. 26, 2023, *available at* https://blog.chainalysis.com/reports/crypto-money-laundering-2022/. (Crypto Money Laundering: Four Exchange).
[46] Chainalysis, *The 2022 Crypto Crime Report*, Feb. 2022, *available at* https://go.chainalysis.com/2022-crypto-crime-report.html (The 2022 Crypto Crime Report); *see* Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, Jan. 13, 2022, *available at* https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.
[47] *See* U.S. Treasury May 2022 Press Release.
[48] *See* U.S. Treasury November 2022 Press Release.
[49] *See* DOJ March 2023 Press Release.

during the Harmony heist through RAILGUN, a United Kingdom-based CVC mixer.[50, 51, 52] Importantly, DPRK-sponsored and -affiliated actors' desire to rely on CVC mixing appears unlikely to abate. Most recently, in August 2023 the FBI attributed the June 2023 Atomic Wallet heist to the Lazarus Group, and open-source reporting indicates that the Lazarus Group used specific services including Sinbad, a CVC mixer, to launder the stolen CVC.[53, 54]

In brief, non-state actors and, significantly, DPRK state-sponsored or -affiliated cyber threat actors have repeatedly used, and continue to use, CVC mixing to launder illicit proceeds from large-scale CVC theft and heists.

3. *CVC mixing is used by ransomware and darknet markets*

CVC mixing services that obfuscate blockchain trails are attractive for cybercriminals looking to launder illegal proceeds from malicious cyber-enabled activities, including ransomware attacks.[55] FinCEN assesses that threat actors avoiding reusing wallets, using CVC mixing services, and "chain hopping" have been prevalent associated money laundering typologies.[56] Open-source analysis in July 2022 reported that nearly 10 percent of all CVC sent

[50] According to open-source reporting, RAILGUN is headquartered in London, England.
[51] FinCEN assesses that RAILGUN falls under the umbrella of CVC mixing, as defined by this NPRM, because it uses its privacy protocol to manipulate the structure of the transaction to appear as being sent from the RAILGUN contract address, thus obscuring the true originator.
[52] *See* FBI January 23, 2023 Press Release.
[53] FBI, *FBI Identifies Cryptocurrency Funds Stolen by DPRK*, Aug. 22, 2023, *available at* https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk.
[54] Elliptic, *North Korea's Lazarus Group likely responsible for $35 Million Atomic Crypto Theft*, June 6, 2023, *available at* https://hub.elliptic.co/analysis/north-korea-s-lazarus-group-likely-responsible-for-35-million-atomic-crypto-theft/#:~:text=Elliptic's%20analysis%20suggests%20that%20North,with%20five%20million%20users%20worldwide.
[55] Europol, *One of the darkweb's largest cryptocurrency laundromats washed out*, Mar. 15, 2023, *available at* https://www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out.
[56] *See* FinCEN October 2021 FTA. FinCEN examined ransomware-related SARs filed between January 1, 2021, and June 30, 2021, to determine trends. The full data set consisted of 635 SARs reporting $590 million in suspicious activity. From this data, FinCEN identified the top 10 most common ransomware variants and analyzed their indicators of compromise through commercially available analytics tools. USD figures cited in this analysis are based on the value of BTC when the transactions occurred.

from addresses tied to illicit activity were sent to CVC mixers, while no other service type exceeded a 0.3 percent CVC mixer sending share.[57] FinCEN's analysis of the top 10 CVC mixers by volume per commercially available data determined that approximately 33 percent of all deposits as of August 2022 were attributed to high risk sources, with 13 percent of all deposits coming from known illicit activities.[58] More significantly, only a portion of the activity in the CVC ecosystem with exposure to CVC mixing is captured by BSA reporting. As a result, FinCEN assesses that high-risk deposits into CVC mixers are likely underreported, and the percent of CVC tied to illicit activity is likely higher.

The relationship between CVC mixing and malicious cyber-enabled and other criminal activities is evident through the reliance of ransomware actors on CVC mixing. The Financial Action Task Force (FATF) identified this connection, noting in 2022 the ongoing and growing threat of criminal misuse of CVC for the receipt and laundering of illicit proceeds from ransomware attacks, expressing particular concern that ransomware cybercriminals are increasingly using CVC mixers to launder their illicit proceeds.[59] Similarly, between January and June 2021, FinCEN observed the use of CVC mixing services (as reflected in BSA reporting of suspicious activity) with the top 10 ransomware strains identified as sending approximately $35.2 million to CVC mixers. During this same time period FinCEN also observed "chain hopping" by ransomware actors to obfuscate the orgin of their proceeds as well as that

[57] Chainalysis, *Crypto Mixer Usage Reaches All-time Highs in 2022 With Nation State Actors and Cybercriminals Contributing Significant Volume*, July 14, 2022, *available at* https://blog.chainalysis.com/reports/cryptocurrency-mixers/.

[58] In August 2022, FinCEN analyzed 10 mixers, finding that these services processed more than $20 billion in total volume between January 2011 and August 2022. The majority of this total occurred between January 2021 and August 2022. FinCEN assessed what sources constituted high risk and illicit activites based on commercial source attributions of entities.

[59] FATF, *Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers,* June 2022, p. 24, *available at* https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF Standards-Virtual Assets-VASPs.pdf.

ransomware actors layered funds through multiple wallet addresses and avoided reusing wallet addresses for each attack. The most prevalent ransomware variants observed by FinCEN between January and June 2021 were Russia-affiliated REvil/Sodinokibi, and Conti,[60] and Russian-speaking DarkSide, Avaddon, and Phobos.[61, 62]

The relationship between CVC mixing and illicit activities is likewise prevalent in transactions involving darknet markets. CVC mixing services often deliberately operate opaquely and advertise their services as a way to pay anonymously for illicit items such as illegal narcotics, firearms, and child sexual abuse material.[63] According to DOJ, the mixer Bitcoin Fog—the longest running Bitcoin money laundering service on the darknet—laundered CVC from darknet marketplaces tied to illegal narcotics, computer fraud and abuse activities, and identity theft.[64] Additionally, according to the Government Accountability Office and DOJ, the dismantled darknet market Alphabay allegedly not only sold and purchased various illegal drugs, illicit goods, and services with CVC, but also allegedly provided mixing services, via the CVC mixer Helix, to obfuscate CVC transactions on the site.[65, 66]

As these examples demonstrate, illicit actors of all types conducting illicit cyber activity, including ransomware attacks and transactions on darknet markets, frequently seek out services that mask their illicit transactions and favor the enhanced anonymity provided by CVC mixing.

---

[60] *See* U.S. Treasury May 2022 Press Release. OFAC identified Conti and Sodinokibi as Russian-linked malign ransomware groups in their designation of Blender.io on May 6, 2022.
[61] *Id.*
[62] *See* FinCEN October 2021 FTA.
[63] *See* First Bitcoin "Mixer" Penalized by FinCEN, October 19, 2020.
[64] DOJ, *Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency 'Mixer'*, Apr. 28, 2021, *available at* https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.
[65] United States Government Accountability Office, *VIRTUAL CURRENCIES Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, Dec. 2021, p. 29, *available at* https://www.gao.gov/assets/gao-22-105462.pdf.
[66] DOJ, *Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million*, Aug. 18, 2021, *available at* https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

Furthermore, FinCEN assesses that the percentage of mixing activity attributed to illicit activity is increasing. According to publicly available analysis reported in January 2023, the total amount of CVC sent to CVC mixers fell significantly, likely due to OFAC designation of two CVC mixers, Blender.io and Tornado Cash. However, the analysis noted the CVC that was sent to CVC mixers in 2022 was more likely to come from illicit sources than in previous years—24 percent of the $7.8 billion[67] processed by mixers in 2022 versus 10 percent of the $11.5 billion processed by mixers in 2021.[68] This shift constitutes a 62.78 percent increase in the illicit value flowing through CVC mixers, year over year.[69]

B. *The extent to which the class of transactions is used for legitimate business purposes*

FinCEN recognizes that there are legitimate reasons why responsible actors might want to conduct financial transactions in a secure and private manner given the amount of information available on public blockchains. FinCEN also recognizes that, in addition to illicit purposes, CVC mixing may be used for legitimate purposes, such as privacy enhancement for those who live under repressive regimes or wish to conduct licit transactions anonymously.[70] Still, CVC mixing presents an acute money laundering risk because it shields information from responsible third parties, such as financial institutions and law enforcement.

FinCEN is concerned that CVC mixing makes CVC flows untraceable by law enforcement and makes potentially suspicious transactions unreportable by responsible financial

---

[67] *See* The 2023 Crypto Crime Report, p. 46.
[68] *See* Crypto Money Laundering: Four Exchange.
[69] Although this analysis assessed only CVC sent to CVC mixers without considering other forms of CVC mixing (as identified by this NPRM), its findings are nevertheless instructive.
[70] Chainalysis, *Crypto Mixers and AML Compliance*, August 23, 2022, *available at* https://blog.chainalysis.com/reports/crypto-mixers/; *see* Elliptic, *What are Bitcoin Mixers & Are They Compliant With AML Standards?*, May 7, 2018, *available at* https://elliptic.co/blog/bitcoin-mixers-assessing-risk-bitcoin-transactions.

institutions—thereby fostering illicit activity as described elsewhere in this document. More importantly, FinCEN assesses that the percentage of CVC mixing activity attributed to illicit activity is increasing. At the same time, because of the lack of available transactional information, FinCEN cannot fully assess the extent to which, or quantity thereof, CVC mixing activity is attributed to legitimate business purposes.

Thus, the legitimate applications of CVC mixing must be carefully weighed against the exposure of the U.S. financial system to ongoing illicit use of CVC mixing. Given the substantial risks posed by CVC mixing, the fact that CVC mixing can be used for some legitimate business purposes does not alter FinCEN's conclusion that this class of transactions is of primary money laundering concern.

C. *The extent to which action by FinCEN would guard against international money laundering and other financial crimes*

Given the threats posed to U.S. national security and the U.S. financial system by obfuscation of illicit proceed flows through CVC mixing, FinCEN believes that imposing recordkeeping and reporting requirements under special measure one would guard against international money laundering and other financial crimes by increasing transparency in these transactions, and thus render them less attractive to illicit actors while also providing additional information to support law enforcement investigations.

This additional transparancy would serve two purposes. First, it would enable investigations by law enforcement and regulators to support money laundering investigations, including cases against North Korean and Russian cybercriminals that pose a threat to U.S national security and the U.S. financial system. Second, it would highlight the risks and deter illicit actors' use of CVC mixing services, including by foreign state-sponsored or -affiliated cyber actors' laundering proceeds of CVC theft to facilitate WMD proliferation, ransomware

attackers' laundering of ransoms, and obfuscation of transactions associated with the use of illicit darknet markets.

V. Proposed enhanced recordkeeping and reporting by covered financial institutions where a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing within or involving a jurisdiction outside the United States

Having found that transactions involving CVC mixing within or involving a jurisdiction outside the United States are a class of transactions that are of primary money laundering concern, FinCEN proposes imposing recordkeeping and reporting obligations on covered financial institutions under special measure one. Such recordkeeping and reporting obligations would require covered financial institutions to report certain information when they know, suspect, or have reason to suspect a CVC transaction involves the use of CVC mixing within or involving a jurisdiction outside the United States.

FinCEN believes that this special measure is the best available tool to mitigate the risks posed by CVC mixing. It would appropriately collect information, which will discourage the use of CVC mixing by illicit actors, and is necessary to better understand the illicit finance risk posed by CVC mixing and investigate those who seek to use CVC mixing for illicit ends. At the same time, this special measure will minimize the burden upon financial institutions and those who seek to use mixing for legitimate purposes. The reporting obligations under this special measure apply to covered financial institutions that directly engage with CVC transactions, such as exchangers, and do not encompass indirect fiat transactions by covered U.S. financial institutions, such as a bank sending funds on behalf of a CVC exchanger that is acting on behalf of a customer purchasing CVC previously processed through a CVC mixer.

As proposed by FinCEN, special measure one would require recordkeeping and reporting of biographical and transactional information related to transactions involving CVC mixing,

increasing transparency and thereby rendering the use of CVC mixing services by illicit actors less attractive. Furthermore, the information generated by this special measure would support investigations into illicit activities by actors who make use of CVC mixing to launder their ill-gotten CVC by law enforcement. At present, there is no similar or equivalent mechanism possessed by law enforcement to readily collect such information, depriving investigators of the information necessary to more effectively understand, investigate, and hold illicit actors accountable. Collectively, the outcomes of the proposed recordkeeping and reporting requirement—discouraging the use of CVC mixing by illicit actors and closing the information gap in service of increased investigation of those illicit actors who continue to make use of CVC mixing—will aid in the protection of the U.S. financial system.

FinCEN has determined that imposition of special measure one would most appropriately collect necessary information while limiting the burden placed on covered financial institutions and users of CVC mixing. As set out further below in Section V.B., FinCEN believes that the existing risk-based approach to AML/CFT compliance used by covered financial institutions already largely encompasses the information FinCEN is requesting. Despite this ready availability of information, covered financial institutions do not, and often need not, universally report that information to FinCEN at present. The proposed reporting requirement would address this reporting gap.

FinCEN considered the other special measures available under section 311. As discussed further in Section V.E. below, it determined that none of them would appropriately balance the interests in permitting secure and private financial transactions while addressing the risks posed by CVC mixing, or were otherwise ill-suited to CVC-related transactions, and thus incapable of collecting information necessary to add transparency to them. Moreover, FinCEN also

considered the appropriate scope of the proposed recordkeeping and reporting requirements, and determined that the proposed approach would best capture necessary information and mitigate risks associated with CVC mixing and facilitate investigations of illicit actors, while preserving legitimate actors' ability to continue conducting secure and private financial transactions.

In proposing this special measure, FinCEN consulted with the Chairman of the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Secretary of State, certain staff of the Securities and Exchange Commission, the Commodity Futures Trading Commission, the National Credit Union Administration Board, the Federal Deposit Insurance Corporation, and the Attorney General. These consultations involved obtaining interagency views on the imposition of the proposed recordkeeping and reporting requirements and the effect that such a recordkeeping and reporting requirements would have on the domestic and international financial system.

Below is a discussion of the relevant statutory factors FinCEN considered in proposing these recordkeeping and reporting requirements.

A. *Whether similar action has been or is being taken by other nations or multilateral groups*

FinCEN is not aware of any other nation or multilateral group that has imposed, or is currently imposing, similar recordkeeping and reporting requirements relating to transactions involving CVC mixing. However, having likewise identified the significant money laundering threat that CVC mixing poses, numerous other nations and certain multilateral groups have issued public statements regarding the risks presented by CVC mixing, called for appropriate regulation, and/or taken action against specific CVC mixers. Several countries—such as Australia, Canada, and Seychelles—and multilateral groups, such as FATF and Europol, have identified CVC mixing as a risk indicator for money laundering or terrorist financing and have

found that CVC mixing can make it more difficult for law enforcement to trace and attribute transactions, complicating investigations.[71] Japan requires information from VASPs on their exposure to CVC mixing services to assess their risk exposure and assign risk ratings.[72] Moreover, as discussed above, numerous countries have investigated and prosecuted individual CVC mixers and associated persons engaged in or facilitating illicit activities. These efforts are generally not as expansive as FinCEN's proposed rule would be. However, FinCEN's identification of CVC mixing as a class of transactions of primary laundering concern and proposed special measure may support efforts of other countries by clearly outlining the illicit finance risks associated with CVC mixing and demonstrating means of enhancing transparency as well as mitigating these risks.

B. Whether the imposition of any particular special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States

While FinCEN assesses that the recordkeeping and reporting requirements proposed in this NPRM will place some cost and burden on domestic financial institutions, these burdens are neither undue nor inappropriate in view of the threat posed by the obfuscation of illicit activity enabled by CVC mixing. The existing risk-based approach to AML/CFT compliance used by

[71] *See* AUSTRAC, *Preventing the Criminal Abuse of Digital Currencies Financial Crime Guide*, Apr. 2022, pp. 1, 15-17, *available at* https://www.austrac.gov.au/sites/default/files/2022-04/AUSTRAC_FCG_PreventingCriminalAbuseOfDigitalCurrencies_FINAL.pdf; Government of Canada, *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, Mar. 2023, *available at* https://www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html; Republic of Seychelles, *ML/TF Overall National Risk Assessment for VA & VASPs*, July 2022, pp. 32, 43, *available at* https://www.cbs.sc/Downloads/publications/aml/Report Seychelles ONRA ML-TF of VA and VASP - 26.08.2022.pdf; Europol, *Seizing the Opportunity: 5 Recommendations For Crypto-Assets Related Crime And Money Laundering* (2022), p. 6, *available at* https://www.europol.europa.eu/cms/sites/default/files/documents/2022_Recommendations_Joint_Working_Group_on_Criminal_Finances_and_Cryptocurrencies_.pdf; FATF, Updated Guidance for a Risk-Based Approach, Oct. 2021.

[72] *See* FATF, Updated Guidance for a Risk-Based Approach, Oct. 2021, at p. 94.

covered financial institutions already largely encompasses the information FinCEN is requesting. While the information is available to covered financial institutions, at present it is not universally reported to FinCEN. That is to say, FinCEN assesses that covered financial institutions already possess customer information and can identify when their customers engage in a covered transaction. This proposed rule would compel covered financial institutions to attribute a covered transaction to the involved customer(s) and report this information to FinCEN. Accordingly, the collection of the information in question would not create any undue costs or burdens on covered financial institutions. Covered domestic financial institutions may need to modify or replace the current systems in place used to detect other types of illicit activity in virtual currency transactions, such as sanctions compliance systems, to detect transactions involving CVC mixing. Such burdens are commensurate with established AML/CFT protocols.

C. The extent to which the action or the timing of the action would have a significant adverse systemic impact on the international payment, clearance, and settlement system, or on legitimate business activities involving CVC transactions

FinCEN assesses that imposition of the proposed special measure would have minimal impact upon the international payment, clearance, and settlement system, or on legitimate business activities involving CVC transactions. As noted in the February 16, 2022, Financial Stability Board's Assessment of Risks to Financial Stability, direct connections between CVC and systemically important financial institutions and core financial markets are limited at present.[73] Volatility and disruptions in the CVC ecosystem have been contained within the CVC markets and have not significantly spilled over to financial markets and infrastructures.

[73] Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets,* Feb. 16, 2022*,* at p. 5, *available at* https://www.fsb.org/wp-content/uploads/P160222.pdf.

D. The effect of the proposed action on United States national security and foreign policy

As described above, CVC mixers are used by DPRK-affiliated and Russia-affiliated threat actors, among others, to facilitate illicit activities ranging from WMD proliferation to ransomware attacks affecting victims in both the United States and around the world, and whose interests are adversarial to the national security interests of the United States. Imposing recordkeeping and reporting requirements on transactions that involve CVC mixing will enhance financial intelligence on the identity of illicit users who rely upon mixers to obfuscate their identities and sources of CVC, as well as provide insight into those CVC mixers that facilitate such illicit activity. Such a rule would therefore best serve the national security interests of the United States and support efforts to protect the United States financial system from illicit finance threats.

E. Consideration of alternative special measures

In assessing the appropriate special measure to impose, FinCEN considered alternatives to imposing recordkeeping and reporting requirements under special measure one. However, FinCEN believes that recordkeeping and reporting requirements under special measure one would most effectively safeguard the U.S. financial system from the illicit finance risks posed by CVC mixing.

In particular, none of the other special measures available under section 311 would appropriately balance the interests in permitting secure and private financial transactions while addressing the risks posed by CVC mixing or would be suited to CVC-related transactions. For instance, FinCEN considered special measure two, which is designed to obtain beneficial ownership information relating to accounts opened in the United States by certain foreign persons or their agents. However, FinCEN determined that such a special measure would fail to

collect key information of interest relating to CVC transactions that involve CVC mixing such as the identity of the participants and beneficial owners of the CVC involved. FinCEN also considered special measures three through five, which are focused upon transactions conducted through payable-through accounts and correspondent banking relationships and determined that these are less relevant in the context of CVC transactions, including those that involve CVC mixing, as CVC transactions are conducted outside of the traditional banking system.

More broadly, FinCEN also considered the appropriate scope of the proposed recordkeeping and reporting requirements. Of note, FinCEN considered issuing a rule pursuant to section 311 that would have been narrowly scoped to address terror finance involving Hamas and ISIS and/or North Korea-sponsored and -affiliated actors. However, FinCEN determined that such a narrow approach would be insufficient to address the relevant risks detailed elsewhere in this action. Given the nature and use of CVC mixing, covered financial institutions would typically have insufficient information to determine whether the CVC transaction was initiated North Korean-affiliated actors. FinCEN believes this would be true of any similarly narrow approach, regardless of the actors involved. Therefore, FinCEN has determined that additional recordkeeping and reporting requirements set forth in this proposed rule would best mitigate the risks associated with CVC mixing, deter illicit actors, facilitate law enforcement investigations into illicit activity, and adequately protect the U.S. financial system from the illicit financial risk posed by CVC transactions that involve CVC mixing, while preserving legitimate actors' ability to conduct secure and private financial transactions.

VI. Section-by-section analysis of proposed regulations

The goal of this proposed rule is to implement an effective and efficient reporting regime to combat and deter money laundering associated with CVC mixing and increase transparency in a sector of the United States virtual currency ecosystem with identified illicit finance risks.

A. *Definitions*

1. *Definition of convertible virtual currency*

The term "convertible virtual currency" or CVC, means a medium of exchange that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status.[74] Although Bitcoin has legal tender status in at least two jurisdictions, the term CVC includes Bitcoin for the purposes of this proposed rule.

2. *Definition of CVC mixing*

The term "CVC mixing" means the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used, such as: (1) pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts; (2) using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction; (3) splitting CVC for transmittal and transmitting the CVC through a series of independent transactions; (4) creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or

[74] As noted in note 17, FinCEN notes that CVC or "virtual currency" by itself does not meet the definition of a "currency" under 31 C.F.R. 1010.100(m). Additionally, the potential characterization of CVC as currency, securities, commodities, or derivatives for the purposes of any other legal regime, such as the Federal securities laws or the Commodity Exchange Act, is outside the scope of this proposed rule. However, as described in the FinCEN 2019 CVC Guidance, if assets that other regulatory frameworks defined as commodities, securities, or futures contracts were to be specifically issued or later repurposed to serve as a currency substitute, then the asset itself could be a type of value that substitutes for currency and be defined as CVC for the purposes of this proposed rule, in addition to being subject to other applicable regulatory frameworks.

accounts through a series of independent transactions; (5) exchanging between types of CVC or other digital assets; or (6) facilitating user-initiated delays in transactional activity.

This definition excepts the use of internal protocols or processes to execute transactions by banks, broker-dealers, or money services businesses, including VASPs, that would otherwise constitute CVC mixing, provided that these financial institutions preserve records of the source and destination of CVC transactions when using such internal protocols and processes, and provide such records to regulators and law enforcement, where required by law. This exemption is designed to avoid capturing transactions with known VASPs that use these internal protocols or processes as part of their business purpose and that are positioned to appropriately respond to inquiries by law enforcement and other relevant authorities. However, if the covered financial institution is unsure if these processes are used as part of a business purpose, they should collect the recordkeeping and reporting information.

FinCEN is seeking to address the primary money laundering concern posed by CVC mixing. The proposed definition of CVC mixing is designed to capture methodologies used by illicit actors to break the traceability of their illicit proceeds and create a mechanism on which which covered businesses would be required to report when they observe CVC mixing transactions. The exception to the definition is crafted to avoid imposing undue burden on covered businesses, provided they are also taking appropriate steps to ensure information is being retained as prescribed by law.

3. *Definition of CVC mixer*

The term "CVC mixer" means any person, group, service, code, tool, or function that facilitates CVC mixing. FinCEN acknowledges this definition is relatively broad; however, given the nature of CVC mixing, FinCEN deems the breadth of this definition to be necessary.

4. *Definition of covered financial institution*

The proposed rule defines ‘‘covered financial institution’’ as the term is defined 31 C.F.R. 1010.100(t), which in general includes the following:

- A bank (except bank credit card systems);
- A broker or dealer in securities;
- A money services business, as defined in 31 CFR 1010.100 (ff). This would include VASPs and other persons that provide money transmission services, which ". . . means the acceptance of . . . value that substitutes for currency from one person and the transmission of . . . value that substitutes for currency to another location or person by any means. . .";[75]
- A telegraph company;
- A casino;
- A card club;
- A person subject to supervision by any state or Federal bank supervisory authority;
- A futures commission merchant or an introducing broker-commodities; and
- A mutual fund.

5. *Definition of covered transaction*

The term "covered transaction" means a transaction as defined in 31 CFR 1010.100(bbb)(1) in CVC by, through, or to the covered financial institution that the covered financial institution knows, suspects, or has reason to suspect involves CVC mixing within or

[75] 31 CFR 1010.100(ff)(5)(A).

involving a jurisdiction outside the United States. The reference to FinCEN's definition of "transaction" means that a covered transaction includes the following: a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, security, contract of sale of a commodity for future delivery, option on any contract of sale of a commodity for future delivery, option on a commodity, purchase or redemption of any money order, payment or order for any money remittance or transfer, purchase or redemption of casino chips or tokens, or other gaming instruments or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected. To this end, FinCEN would expect covered financial institutions to employ a risk-based approach to compliance of this proposed rule, and more broadly, the Bank Secrecy Act, including by using the variously available free and paid blockchain analytic tools commonly available.[76]

The limitation to transactions "in CVC" means that the reporting obligations under this special measure apply to covered financial institutions that directly engage with CVC transactions, such as a CVC exchange. It also means that covered transactions do not include transactions that are only indirectly related to CVC, such as when a CVC exchanger sends the non-CVC proceeds of a sale of CVC that was previously processed through a CVC mixer from the CVC exchanger's bank account to the bank account of the customer selling CVC.

It is critical that all financial institutions, including those with visibility into CVC flows, such as CVC exchangers—generally considered money services businesses (MSBs) under the Bank Secrecy Act—identify and quickly report suspicious activity, and conduct appropriate risk-

[76] FinCEN is not, at this time, proposing that covered financial instutitons would be required to perform a lookback to identify covered transactions that occurred prior to issuance of a final rule.

based customer due diligence or, where required, enhanced due diligence. For example, in appropriately conducting a review to identify suspicious activity associated with potential sanctions evasion and to comply with existing FinCEN 311s on Iran and DPRK, financial institutions must know if transactions originate from or are destined to prohibited jurisdictions, such as Iran[77] or DPRK.[78] Indeed, FinCEN can, and has, assessed civil monetary penalties on covered financial institutions that have failed to conduct such due diligence, including, recently, in enforcement actions against Bittrex[79] and BitMex.[80] In light of the existing compliance practices of covered financial institutions, FinCEN expects that complying with this proposed rule should not add a significant additional burden. FinCEN invites public comment on this assessment.

B. *Reporting and Recordkeeping Requirements*

1. *Information to be Reported*

Although FinCEN recognizes much of the information that would be collected under this proposed rule is already provided to the most frequent reporters in the CVC ecosystem, imposing additional recordkeeping and reporting requirements is necessary to address the money laundering threat posed by CVC mixing because, at present, covered financial institutions do not regularly report when their customers send or receive CVC in transactions with indicia of CVC

---

[77] *See* FinCEN, *Imposition of Fifth Special Measure against the Islamic Republic of Iran as a Juridiction of Primary Money Laundering Concern*, 84 FR 59302, Nov. 4, 2019, *available at* https://www.fincen.gov/sites/default/files/shared/2019-23697.pdf.

[78] *See* FinCEN 2016 Imposition of Special Measure Against North Korea.

[79] *See* FinCEN, *FinCEN Announces $29 million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act*, Oct. 11, 2022, *available at* https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service.

[80] *See* FinCEN, *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, Aug. 10, 2021, *available at* https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures#:~:text=Despite%20BitMEX's%20public%20representation%20that,trading%20platform%20and%20circumvent%20internet.

mixing. Reporting that links customers to the CVC mixing transactions will aid law enforcement and national security investigations of illicit activity involving CVC. The following addresses the types of information the rulemaking proposes to collect.

(i) Reportable information regarding the covered transaction

In connection with all covered transactions, FinCEN proposes to collect the following information:

- *The amount of any CVC transferred, in both CVC and its U.S. dollar equivalent when the transaction was initiated:* The amount of CVC transferred would aid in performing analysis using a risk-based approach. The proposed rule would require the amount in CVC and U.S. dollar equivalent when the transaction was initiated to account for volatile CVC prices and aid in consistent monitoring and risk management purposes.
- *CVC type*: The proposed rule would require reporting of the type of CVC used in a covered transaction. The type of CVC used would allow for trend analysis of preferred usage of different types of CVC, as well as ensure the correct blockchain analysis can be done given each CVC exists on different blockchains. Taken together with the amount of any CVC transferred, this information would inform trend analysis and allow for an improved understand of laundering typologies.
- *The CVC mixer used, if known*: The proposed rule would require reporting of the CVC mixer used in the covered transaction. That information would assist in understanding trends of mixing activity as well as aid in understanding the quantity of CVC mixers in the CVC ecosystem.

- *CVC wallet address associated with the mixer*: The proposed rule would require reporting of the CVC wallet address of the CVC mixer, if one is used, to aid in understanding of addresses associated with each CVC mixer. This information would assist with understanding the size, scale, and methodologies of CVC mixers by facilitating aggregate analysis of transactional data of CVC mixers.
- *CVC wallet address associated with the customer*: The proposed rule would require reporting of the CVC wallet address of the customer to assist in the investigation of the covered transaction, including blockchain analysis to determine if the wallet is associated with illicit activities.
- *Transaction hash*: The proposed rule would require reporting of the transaction hash, which will allow an investigation of the specific transaction and assist in the identification of specific wallet addresses involved in the transaction(s), as well as more specific transactional meta data such as the date and time the transaction was completed.
- *Date of transaction*: The proposed rule would require reporting of the date of transaction, which would assist in enforcing the proposed regulation, as well as assist in corroborating other reported information.
- *IP addresses and time stamps associated with the covered transaction:* The proposed rule would require reporting of the IP address to obtain geographical information related to the covered transaction, which would assist trend analysis of patterns of covered transactions by geographic location.
- *Narrative*: The proposed rule would require a description of activity observed by the covered financial institution, including a summary of investigative steps taken,

provide additional context of the behavior, or other such information the covered financial institution believes would aid follow on investigations of the activity. As the covered financial institution would have insight into the normal pattern of its customers' transactions, this narrative would assist with understanding if there is an uncharacteristic change in pattern of behavior.

Importantly, under the proposed rule, covered financial institutions would continue to have an obligation to file a SAR when warranted, regardless of whether the covered financial institutions also filed a report required under the proposed rule.

(ii) Reportable information regarding the customer associated with the covered transaction

In respect of customers associated with covered transactions, FinCEN proposes to collect the following information:

- *Customer's full name*: The proposed rule would require reporting of the full name of the covered financial institution's customer, as it appears in the customer's proof of identification and related documents, such as passport or driver's license or non-driver identification card, used by the customer when they validated their identity with the covered financial institution.
- *Customer's date of birth*: The proposed rule would require reporting of the full date of birth of the covered financial institution's customer, as it appears in the customers onboarding file.
- *Address*: The proposed rule would require reporting of the most appropriate address (residential or business) of the customer engaged in a covered transaction. Specifically, if the customer is a business, the business address would be reported, and, if the customer is an individual, the residential address would be reported.

- *Email Address associated with any and all accounts from which or to which the CVC was transferred*: The proposed rule would require email address(es) used by a customer involved in a covered transaction and known to the covered institution.
- *Unique identifying number*: For individuals, the proposed rule requires reporting of customers' Internal Revenue Service (IRS) Taxpayer Identification Number (TIN) or, if the individual does not have one, a foreign equivalent. If the customer has neither a TIN nor a foreign equivalent, the proposed rule would require reporting of a non-expired United States or foreign passport number or other government-issued photo identification number, such as a driver's license. For entities, the proposed rule would require reporting of the entity's IRS TIN or, if the entity does not have one, a foreign equivalent or a foreign registration number. TINs and other unique identifying numbers provide law enforcement with the most efficient means to identify individuals potentially involved in illicit activity.

2. *Filing Procedures*

The proposed regulation would require a covered financial institution to collect, maintain records of, and report to FinCEN within 30 calendar days of initial detection of a covered transaction, in the manner that FinCEN may prescribe, certain information regarding covered transactions that involve CVC mixing. This includes certain information the covered financial institution shall provide with respect to each covered transaction which is examined in detail below. This proposed reportable information is similar to the information already collected by financial institutions to comply with their AML/CFT obligations; however, at present covered businesses would not necessarily report such information. Notably, the proposed regulation only requires a covered financial institution to report information in its possession, and thus does not

require a covered institution to reach out to the transactional counterparty to collect additional information on the CVC mixing transaction.

3. *Recordkeeping requirements*

Pursuant to the proposed rule, covered financial institutions would be required to maintain any records documenting compliance with the requirements of this regulation.

VII. Request for Comments

FinCEN invites comments on all aspects of the proposed rule, including the following *specific matters*:

A. *CVC mixing as a class of transactions of primary money laundering concern*

1. What impact would this proposed rule have on legitimate activity conducted by persons in the course of conducting financial transactions?
2. What impact would the proposed rule have on blockchain privacy or pseudonymity, noting that filings reported to FinCEN are not publicly releasable and the similarities of this proposal to the recordkeeping and reporting requirements of transactions using the traditional financial system, such as with wire or Automated Clearing House (ACH) transactions?
3. Does the impact on privacy and legitimate applications identified in Section IV.B potentially outweigh the risks posed by illicit activity facilitated by CVC mixing?
4. What challenges are anticipated with respect to identifying the foreign nexus of a CVC mixing transaction?

5. Are there any other methods that covered financial institutions can use to be able to readily determine if covered transactions stemming from non-mixer CVC mixing have a foreign nexus?
6. Are there sufficient tools available, either free or paid, that would aid covered financial instutitions to determine if covered transactions occurred outside the United States?
7. Are there any other methods that covered financial institutions can use to be able to readily determine if covered transactions stemming from non-mixer CVC mixing have a foreign nexus?
8. Has FinCEN appropriately weighed the legitimate and illicit activities associated with the use of CVC mixing? What other factors should be considered?

B. ***Definitions***

1. Please provide suggested revisions to the proposed definitions that would better tailor the intended recordkeeping and reporting obligations to the objectives and uses described in this proposal. Where possible, please provide information or examples to illustrate how the recommended revisions improve upon the definitions as proposed.
2. Does the proposed definition of CVC mixing adequately capture the activity of concern? If not, please provide suggested revisions to the proposed definition that would better capture such activity. Where possible, please provide information or examples to illustrate how the recommended revisions would improve upon the definition as proposed.

3. Does the proposed exception to the definition of CVC mixing adequately account for legitimate activity conducted by VASPs and other financial institutions? If not, please provide suggested revisions to the proposed definition that would better capture such activity. Where possible, please provide information or examples to illustrate how the recommended revisions would improve upon the definition as proposed.

C. ***Alternatives***

1. Is FinCEN's proposal of enhanced recordkeeping under section 311's special measure one most appropriate to the objectives of this proposed rule? Where possible, please provide suggestions for alternative means of achieving the objectives and illustrate how such means would work in practice.
2. Would section 311's special measures two through five be more appropriate to apply? If so, please explain why.

D. ***Recordkeeping and reporting***

1. Is the scope of the recordkeeping requirement appropriate?
2. Is the list of information to be collected and reported appropriate to address the stated primary money laundering concern?
3. Is the proposed mechanism for submission appropriate for the purpose of this proposed rule?
4. Are there any alternative methods of submitting reports in an efficient and effective manner that FinCEN should consider utilizing?
5. Are the proposed reporting and recordkeeping requirements discussed in Section VI.B.1 and 3 appropriately scoped? Are there additional types of

information regarding reportable transactions or customers that should be collected?

6. Should the proposed reporting and recordkeeping requirements apply to covered financial institutions that are the originator institution, the beneficiary institution, or both?
7. In cases where the customer of a covered financial institution is a legal entity, should the implementation of special measure one also require the beneficial ownership of that legal entity be reported, in addition to the other proposed reporting requirements?

E. ***Burden and other impacts of this proposed rule***

1. Does FinCEN accurately account for the burden and impact of this proposed rule when a covered financial institution knows, suspects, or has reason to suspect a transaction involves CVC mixing?
2. Is there a less burdensome way of collecting information regarding the details of a CVC transaction, which the BSA's AML/CFT objectives require financial institutions to collect, including know-your-customer and customer due diligence?
3. Would the adoption of special measure one reporting and recordkeeping requirements, as proposed, impose expected costs to covered financial institutions; state, local, or tribal governments; or the private sector in excess of $177 million annually? $200 million annually? Where possible, please provide data or studies from an identifiable source that would support the response or describe why a source cannot be identified.

4. To what extent should FinCEN consider the potential costs to currently unregistered or otherwise non-reporting entities that, if compliant, would incur costs if special measure one is adopted as proposed? If possible, please illustrate either quantitatively or qualitatively (by way of example or anecdote) how the recommended level of consideration would improve FinCEN's estimate of regulatory impact.
5. Are there any material facts, data, circumstances, or other considerations that, had they been included in FinCEN's regulatory impact analysis, would have both improved the precision and accuracy of the analysis and substantially altered the assessment of the proposed rule's impact? If so, please provide, including attribution to the sources of such information, where possible.
6. Would the adoption of special measure one reporting and recordkeeping requirements, as proposed, impose significant costs on covered financial institutions that are small entities? On other small entities that are not covered financial institutions? Where possible, please provide data or studies from an identifiable source that would support the response or describe why a source cannot be identified.
7. Are the due diligence requirements appropriately scoped in this proposed rule?
8. What impact will this proposal have on augmenting law enforcement's ability to track and trace CVC derived from cyber heists, ransomware, or similar illicit activity to aid the return of victim's CVC?

9. Are there any international efforts to address illicit finance risks stemming from mixing not addressed in the NPRM?
10. What effect would the proposed rule have on international efforts to address the illicit use of CVC mixing?
11. Are there specific examples of "covered transactions" or sample scenarios that FinCEN could have provided to assist financial institutions and other affected parties in further understanding the intended applicability of the proposed definition of "covered transactions"? Alternatively, are there other clarifications to the definitions in this NPRM, or other modifications to the proposed regulatory text that would meaningfully clarify when a covered transaction occurs that would warrant reporting? If so, please describe.
12. Is FinCEN correct in its assessment that covered financial institutions would have access to reasonable and appropriate services or tools, whether free or paid, to be able to effectively identify covered transactions? If not, what are impediments to accessing such tools, and what costs would be associated with gaining access?
13. To what extent could public guidance or other informational materials regarding compliance with the requirements of proposed special measure one (such as FAQs, pre-recorded instructional audio-visual resources, or in-person presentations with industry groups) meaningfully reduce costs to covered financial institutions? Please describe any preferred method(s), as well as any qualitative or quantitive estimates of the extent to which costs are expected to be reduced.

VIII. Regulatory Impact Analysis

FinCEN has analyzed this proposed rule under Executive Orders 12866, 13563, and 14094, the Regulatory Flexibility Act,[81] the Unfunded Mandates Reform Act,[82] and the Paperwork Reduction Act.[83]

As discussed above,[84] the intended effects of the imposition of special measure one to CVC mixing are twofold. The rule is expected to: (1) facilitate the investigation and prosecution of illicit activities by parties using CVC mixing in furtherance of their unlawful objectives[85] and, in many cases,[86] consequent private enrichment; and (2) disincentivize the use of CVC mixing in connection with money laundering and other financial crimes by reducing the likelihood that such CVC mixing will adequately insulate the underlying transactions from identification and traceability.[87] In the analysis below, FinCEN discusses the economic effects that are expected to accompany adoption of the rule as proposed and assess such expectations in more granular detail. This discussion includes a detailed explanation of certain ways FinCEN's conclusions may be sensitive to methodological choices and underlying assumptions made in drawing inferences from available data. Throughout, these have been outlined so that the public may review and provide comment.[88]

A. *Assessment of Impact*

By requiring covered financial institutions to implement special measure one, the proposed rule would impose additional obligations on these institutions to report transactions that

[81] 5 U.S.C. 603.
[82] 12 U.S.C. 1532, Public Law 104–4 (Mar. 22, 1995).
[83] 44 U.S.C 3507(a)(1)(D).
[84] *See, specifically* discussion *supra* Section IV. C. *See generally* discussion *supra* Section II.
[85] *See, e.g.*, discussion of Axie Infinity heist *supra* Section III.B.
[86] *See, e.g.*, discussion of use in connection with darknet market transactions and laundering the proceeds of ransomware attacks *supra* Sections III.B and IV.A..
[87] *See* discussion *supra* Section IV.C.
[88] *See* Section VII.E.

they know, suspect, or have reason to suspect involve CVC mixing because FinCEN has determined that CVC mixing, as a class of transactions, is of primary money laundering concern.

The imposition of this special measure may require a shift in reporting practices, particularly with regard to the determination a covered financial institution would otherwise first need to make: that a transaction involving CVC mixing is suspicious and therefore reportable under the applicable SAR Rule.[89] The reporting and recordkeeping requirements under special measure one would instead guide a covered financial institution to presume transactions that involve CVC mixing are inherently of primary money laundering concern. Therefore, under this proposal, the implied burden would shift from determining when a CVC transaction is reportable to determining when it is not reportable.

FinCEN has considered the regulatory impact of the proposed rule and the economic consequences these changes would entail. The subsequent analysis details FinCEN's finding that, in proportion to the thousands of covered financial institutions subject to FinCEN's general reporting and recordkeeping requirements, relatively few are exposed to CVC mixing and, additionally, proportionally few transactions per exposed financial institution covered under the proposed rule are likely to trigger the new recordkeeping and reporting requirements, of which fewer still may provide actionable information. However, any one reportable transaction, by nature of the underlying illicit and potentially dangerous activity it facilitates, could provide large benefits to FinCEN and law enforcement if identified, or, alternatively framed, could impose substantial costs and serious national security risks if unreported.[90]

[89] *See, e.g.,* FinCEN 2019 CVC Guidance *supra* note 16 and FinCEN, *Reporting Suspicious Activity A Quick Reference Guide for Money Services Businesses*, September, 2007, *available at* https://www.fincen.gov/sites/default/files/shared/report_reference.pdf.

[90] *See, e.g.*, discussion *supra* Sections III.B and IV.A.

1. *Broad Economic Considerations*

At present, in the absence of an obligation to comply with special measure one requirements, a covered financial institution may determine that a financial transaction exposed, directly[91] or indirectly,[92] to CVC mixing bears indicia of illicit activity. Given the potential link to illicit activity, this financial institution might file a SAR in compliance with existing BSA requirements. However, there are a number of potential reasons why any one individual institution may not file such a report, including that in terms of economic fundamentals, such reporting may not be privately optimal. Consequently, the absence of the proposed special measure one reporting requirement might naturally result in systematic underreporting of CVC mixing-related suspicious activity, particularly when the exposure to CVC mixing does not involve a CVC mixer. As discussed above, preliminary evidence suggests that this underreporting occurs.[93]

In terms of economic fundamentals, reporting on transactions exposed to CVC mixing produces a positive externality insofar as the reporting entity incurs expenses in connection with such reporting that are not directly, fully compensated. As such, the marginal social benefit of reporting exceeds the private costs. Consequently, in the absence of imposing a social (compliance-related) cost to non-reporting, the entity-specific equilibrium level of reporting will always be less than the social optimum. Furthermore, from a microeconomic- or a more industrial-organization-level of analysis, there are competitive reasons why, absent a uniform reporting requirement, no single covered financial institution that knows, suspects, or has reason to suspect CVC mixing would benefit from competing lower on the perceived level of quality in

[91] *See infra* note 121.
[92] *See infra* note 122.
[93] *See* discussion *supra* Section IV.A.3.

privacy. In such a setting, achieving the socially optimal level of reporting would again be unobtainable in the absence of a policy intervention (such as the proposed reporting and recordkeeping requirements).

In this proposal, FinCEN is mindful that certain unintended, responsive changes in behavior may reduce the efficacy of this rule or otherwise attenuate the intended net benefits by limiting the scope of benefits or by increasing the costs of compliance. Additionally, the attendant costs and benefits per reported transaction may not be uniformly distributed across the affected covered financial institutions. There may also be broader programmatic costs or repercussions to: (1) the specific framing of CVC mixing and CVC mixers as proposed;[94] (2) the framing of CVC mixing activity as categorically foreign-state-operated, -located, or otherwise -adjacent; (3) the reporting and recordkeeping requirements being applicable to domestic financial institutions only; and (4) allowing an in-the-course-of-business exemption to covered financial institutions, that each remain unquantified in the following impact analysis. Nevertheless, FinCEN has made a studied[95] and advised[96] determination that these considerations are outweighed by the primary money laundering concern that animates this proposal and are therefore not further incorporated in the subsequent discussion.

2. *Institutional Baseline and Affected Parties*

In proposing this rule, FinCEN considered the incremental impacts of imposing special measure one relative to the current state of the affected markets and their participants. This baseline analysis of the parties that would be affected by the proposed rule, their current

[94] *See* invitation for public comment on potential costs and repercussions *supra* Section VII.B.
[95] 31 U.S.C. 5318A(a)(4)(B). *See* discussion *supra* Section I.
[96] *See* discussion of 31 U.S.C. 5318A(c)(1) requirements *supra* Section I. *See also* discussion of 31 U.S.C. 5318A(a)(4)(A) *supra* Sections I and V.

obligations, and common activities satisfies certain analytical best practices[97] by detailing the implied alternative of not pursuing the proposed, or any other, regulatory action. This baseline also forms the counterfactual against which the quantifiable effects of the rule are measured; therefore, substantive errors in or omissions of relevant data, facts, or other information may affect the conclusions formed regarding the general and/or economically significant impacts of the rule. Additionally, because it is unclear that the imposition of special measure one would, independently, alter the registration and compliance choices already made by such affected parties, quantitative portions of the subsequent analysis have not attempted to estimate the number of, or magnitude of effects on, unregistered or otherwise non-compliant entities that FinCEN qualitatively might expect to be affected by the rule. Because both these considerations may have first-order effects on the expected magnitude of certain outcomes, the public is invited to provide further insights or information—particularly, data or quantitative studies—that could contribute to a more precise or more accurate estimation of impact.[98]

(i) Baseline of Affected Parties

(A) Covered Financial Institutions

The parties expected to comply with the special measure one include any and all domestic covered financial institutions as defined in 31 CFR 1010.100(t).[99] Table 1 (below) reports an annual maximum of potentially affected entities based on FinCEN's most recent estimates of the total number of entities that meet the respective regulatory definitions.[100]

[97] *See specifically* E.O. 12866 Section 1(a) ("In deciding whether and how to regulate, agencies should assess all costs and benefits of available regulatory alternatives, including the alternative of not regulating.").
[98] *See, e.g., supra* Section VII.E.
[99] *See* discussion *supra* Section VI.A.4; *see also* proposed amendment 31 CFR 1010.662(a)(4) *infra* Section IX.
[100] Numbers presented here may differ slightly from those presented in other, concurrent agency rulemaking because estimates in this analysis are rounded to the nearest ten for ease of aggregation. Such differences are not expected to be economically meaningful.

Estimates of potentially affected money services businesses by subcategories as defined in 31 CFR 1010.100(ff) are intended to aid in subsequent discussion, which details our assumptions about differences in expected compliance burdens by group. Estimates in parentheses reflect the total number of registered money services businesses that self-identified their business by the given service subcategory as defined in 31 CFR 1010.100(ff), among others.[101] Money services business subcategory estimates outside parentheses represent the number of entities that self-identified as registering (and reporting) singularly due to the requirements for that subcategory.

Table 1. Estimates of Affected Financial Institutions by Type

FINANCIAL INSTITUTION TYPE[a]	NUMBER OF ENTITIES
BANK[b]	9, 850[c]
BROKER/DEALER IN SECURITIES[d]	3,540[e]
MONEY SERVICES BUSINESS[f]	25,710[g]
DEALER IN FOREIGN EXCHANGE[h]	190 (3,000)[i]
CHECK CASHER[j]	5,960 (21,970)[k]
ISSUER/SELLER OF TRAVELER'S CHECKS/MONEY ORDERS[l]	380[m]
PROVIDER OF PREPAID ACCESS[n]	20 (130)[o]
SELLER OF PREPAID ACCESS[p]	40 (2,220)[q]
U.S. POSTAL SERVICE[r]	0[s]
MONEY TRANSMITTER[t]	450 (16,460)[u]
TELEGRAPH COMPANY[v]	0[w]
CASINO[x]	990[y]
CARD CLUB[z]	270[aa]
PERSON SUBJECT TO SUPERVISION BY ANY STATE OR FEDERAL BANK SUPERVISORY AUTHORITY[bb]	N/A[cc]
FUTURES COMMISSION MERCHANT[dd]	60[ee]
INTRODUCING BROKER IN COMMODITIES[ff]	970[gg]
MUTUAL FUND[hh]	1,380[ii]

[a] As typographically grouped in 31 CFR X 1010.100(t) and (ff), respectively.
[b] *See* 31 CFR 1010.100(t)(1); *see also* 31 CFR 1010.100(d).
[c] Counts of certain types of banks, savings associations, thrifts, and trust companies are from Q1 2023 Federal Financial Institutions Examination Council (FFIEC) Call Report data, *available at* https://cdr.ffiec.gov/public/pws/downloadbulkdata.aspx. Data for institutions that are not insured, are insured under non-FDIC deposit insurance regimes, or do not have a Federal functional regulator are from the FDIC's Research Information System, *available at* .https://www.fdic.gov/foia/ris/index.html. Credit union data are from the NCUA for Q1 2023, *available at* https://www.ncua.gov/analysis/credit-union-corporate-call-report-data.
[d] 31 CFR 1010.100(t)(2).
[e] According to the SEC, the number of brokers or dealers in securities for the fiscal year 2022 is 3,538. *See* Securities and Exchange Commission, *Fiscal Year 2024 Congressional Budget Justification*, p. 32, *available at* https://www.sec.gov/files/fy-2024-congressional-budget-justification_final-3-10.pdf.
[f] 31 CFR 1010.100(t)(3).

[101] For the full list of non-exclusive subcategories a money services business may use to self-identify when submitting a registration *see* msb.fincen.gov/definitions/msbKey.php.

[g] From FinCEN's publicly available MSB data (https://www.fincen.gov/msb-registrant-search) as of September 1, 2023.
[h] 31 CFR 1010.100(ff)(1).
[i] Value in parentheses reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search on August 1, 2023, including MSB Activities key 415. Alternative value reflects entries with exclusively key 415.
[j] 31 CFR 1010.100(ff)(2).
[k] Value in parentheses reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search on August 1, 2023, including MSB Activities key 408. Alternative value reflects entries with exclusively key 408.
[l] 31 CFR 10101.100(ff)(3).
[m] Value reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search on August 1, 2023 with, exclusively, one of the MSB Activities keys 401 (Issuer of traveler's checks), 402 (Seller of traveler's checks), 404 (Issuer of money orders), or 405(Seller of money orders). Because of the numerous (134) alternative combinations of at least one of the 4 keys with at least one of the other three keys and, in some cases, other keys as self-reported by registrants, no suitable alternative combination of key values could be determined as most appropriately and uniquely representative in light of concerns about multiplicative counting of affected parties. FinCEN estimates therefore default to the upper bound of all MSB registrants for this category of parties collectively incurring a regulatory compliance burden.
[n] 31 CFR 1010.100(ff)(7)(i)-(ii).
[o] Value in parentheses reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search on August 1, 2023 including MSB Activities key 414(Provider of prepaid access). Alternative value reflects entries with exclusively key 414.
[p] 31 CFR 1010.100(ff)(4)(i)-(iii).
[q] Value in parentheses reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search including MSB Activities key 413. Alternative value reflects entries with exclusively key 413.
[r] 31 CFR 1010.100(ff)(6).
[s] FinCEN does not expect the U.S. Postal Service, as defined in 31 CFR 1010.100(ff)(6) to incur any recordkeeping or reporting obligations in connection with this rule.
[t] 31 CFR 1010.100(ff)(5).
[u] Value in parentheses reflects all entries in data downloaded from https://www.fincen.gov/msb-registrant-search including MSB Activities key 409. Alternative value reflects entries with exclusively key 409.
[v] 31 CFR 1010.100(t)(4).
[w] As an estimate of uniquely registered, potentially affected entities, FinCEN expects this category to contain no additional persons or organizations not already included in other counts, particularly as money transmitters.
[x] 31 CFR 1010.100(t)(5)(i)-(iii).
[y] According to the American Gaming Association (AGA), there are 468 commercial casinos and 523 tribal casinos as of Dec. 31, 2022. *See* American Gaming Association, *State of the States: annual report*, May 2023, *available at* https://www.americangaming.org/wp-content/uploads/2023/05/AGA-State-of-the-States-2023.pdf p. 16.
[z] 31 CFR 1010.100(t)(6)(i)-(ii).
[aa] According to the American Gaming Association (AGA), there are 266 card rooms as of Dec. 31, 2022.
[bb] 31 CFR 1010.100(t)(7).
[cc] It is unclear to FinCEN at this time whether any entities exist in this category that for purposes of being counted towards unique affected parties incurring burdens associated with the rule, if adopted as proposed, are not already captured by concurrent status in another category of financial institution under the 31 CFR 1010.100(t) definition. To the extent that additional data can better inform this estimate, public comment is invited.
[dd] 31 CFR 1010.100(t)(8).
[ee] There are 60 futures commission merchants as of June 30, 2023, according to the CFTC website. See Commodity Futures Trading Commission, *Financial Data for FCMs*, *available at* https://www.cftc.gov/MarketReports/financialfcmdata/index.htm.
[ff] 31 CFR 1010.100(t)(9).
[gg] According to CFTC, there are 969 introducing brokers in commodities as of April 30, 2023.
[hh] 31 CFR 1010.100(t)(10).
[ii] According to the SEC, as of December 2022 (including filings made through Jan 20, 2023) there are 1,378 open-end registered investment companies that report on Form N-CEN.

Based on these estimates, it is possible that up to approximately 42,800 covered financial institutions could incur new recordkeeping and reporting costs in complying with special measure one. However, the extent to which any of these institutions is expected to be economically impacted is limited insofar as they would need to engage in transactions[102] that involve CVC, and thereby the possibility of CVC mixing. This prerequisite[103] (that a transaction be in CVC) is expected to preclude many entities from experiencing any significant economic effects from the rule.[104] For example, FinCEN does not anticipate any direct effects to the U.S. Postal Service or to any registered telegraph company. Further, FinCEN analysis of public and non-public sources of information suggests that, categorically, domestic mutual funds, casinos, and card clubs have low exposure to CVC transactions. For the same reasons, money services businesses that provide services exclusively in one or more of the following subcategories are not expected to experience any substantial change to compliance burdens: dealer in foreign exchange, check casher, issuer/seller of traveler's checks or money orders, provider of prepaid access, and seller of prepaid access. Thus, FinCEN expects approximately 9,300 fewer than the total estimate of potentially affected entities to reasonably anticipate any noticeable effect.

On the other hand, the categories of affected parties that include the largest proportion of VASPs are expected to face the highest levels of potential exposure to CVC mixing. These entities are most concentrated in the money transmitter subcategory of money services businesses and futures commission merchants. In each case, these VASPs are a proper subset of their respective groups, and while they are expected to be the most directly affected by the rule because they have the highest exposure, the incremental burden of the rule is expected to be

[102] 31 CFR 1010.100(bbb)(1).
[103] *See* discussion *supra* Section VI.A.5; *see also* proposed amendment 31 CFR 1010.662(a)(5) *infra* Section IX.
[104] *See* discussion of expected economic effects on covered financial institutions *infra* Section VIII.A.4.

lowest for these entities because it imposes the least adaptation from current compliance practices and processes.

The covered financial institutions that are expected to face the greatest incremental burden as a consequence of the proposed recordkeeping and reporting requirements would be those with both higher likelihoods of being exposed to CVC mixing and lower tailoring of existing compliance programs because, for instance, virtual asset service provision has not historically been integral to the entity's core business function or model. FinCEN expects that this may characterize certain banks, or persons subject to supervision by a state or federal bank supervisory authority, broker/dealers, and introducing brokers in commodities. However, as these types of financial institutions are already heavily regulated and typically already feature robust monitoring and compliance programs, even as they may face the largest incremental burden, this economic impact might still be low.[105]

(B) CVC Mixing Service Providers[106]

While the proposed application of special measure one does not expressly impose requirements on CVC mixers that are not covered financial institutions or those able to rely on the proposed exemption,[107] it is reasonable to expect that the relative attractiveness of engaging with CVC mixers or the number of those who avail themselves of CVC mixing services might be affected. As a baseline matter of market structure, the centralized mixing services industry is expected to be characterized by large network externalities: the value of a CVC mixer should increase as the number of users increases, because the greater the number of parties that use a

[105] FinCEN is requesting comment on the reasonable bases for this expectation. *See* requests for comment *supra* Section VII.A and Section VII.E.
[106] In this section, FinCEN uses the term 'CVC mixer' as used in common parlance, noting this may commonly be understood to refer to only a proper subset of the entities/parties that would meet the definition of 'CVC mixer' as defined in this proposed rule. *See* discussion *supra* Section VII.A.3; *see also* proposed amendment 31 CFR 1010.662(a)(2) *infra* Section IX.
[107] At the time of this proposal, FinCEN observes no CVC mixers that meet either or both of these criteria.

particular CVC mixer, the easier it becomes for the mixer to anonymize each participant in a mixing transaction. This characterization is consistent with observable market behavior. Because network externalities generally reinforce high levels of market concentration, it may be reasonable to expect that the number of CVC mixers that can concurrently achieve and maintain a sustainable scale to continue operations is unlikely to grow. It may also imply that, to the extent that the demand for CVC mixing services remains relatively constant over time, in the event that any one CVC mixing service provider ceases to remain active, another active or new CVC mixer could greatly benefit from the subsequent increase in demand for its services.

(C) Clients of Primary Affected Parties

In the course of compliance with special measure one, covered financial institutions may be required to submit reports and retain records containing certain unique identifiers[108] and other personal information[109] of a party, or parties, to a CVC mixing-exposed transaction.[110] Based on a recent report,[111] this could affect more than 300 million users of unhosted CVC wallets insofar as a user's personal information may be reported if their wallet is deemed by a covered financial institution to be involved in a covered transaction. Because there is no restriction on the number of wallets an individual may have, this number may overestimate the number of unique individuals whose personal information may be required. To the extent that previously reported estimates[112] regarding the distribution of CVC mixer users by type—privacy-oriented versus

[108] Including name (*see* proposed amendment 31 CFR 1010.662(b)(1)(ii)(A) *infra* Section IX) and government issued (alpha)numeric identifier (*see* proposed amendment 31 CFR 1010.662(b)(1)(ii)(F) *infra* Section IX); *see also* discussion *supra* Section VI.
[109] Including a customer's CVC wallet address (*see* proposed amendment 31 CFR 1010.662(b)(1)(i)(E) *infra* Section IX), date of birth (*see* proposed amendment 31 CFR 1010.662(b)(1)(ii)(B) *infra* Section IX), address (*see* proposed amendment 31 CFR 1010.662(b)(1)(ii)(C) *infra* Section IX), and email address (*see* proposed amendment 31 CFR 1010.662(b)(1)(ii)(D) *infra* Section IX); *see also* discussion *supra* Section VI.
[110] *See* Section VI.B.1.
[111] Chainalysis Report, *On-Chain User Segmentation for Crypto Exchanges*, June 22, 2023, *available at* https://www.chainalysis.com/blog/crypto-exchanges-on-chain-user-segmentation-guide/.
[112] *See* discussion *supra* Section IV.A.3; *see also supra* note 58.

abusers of anonymity—are usable for inference, special measure one could require the reporting of personal information in connection with up to approximately 66 (87) percent of CVC mixer deposits in the absence of any other identifiable connection to high risk (illicit) activity.

FinCEN has weighed these considerations against the broader economic concern of systematic underreporting in the absence of special measure one requirements,[113] and concluded that the associated costs to privacy-oriented clients of covered financial institutions and CVC mixers are small in both relative[114] and absolute[115] terms. Further, there is no reason to believe the required records and personal information contained therein would be subject to any greater risk of improper access, use, or exposure than any other record or report filed with a federal agency or maintained by a covered financial institution.

(D) Other Affected Parties

FinCEN further anticipates second order economic effects of the proposed rule on parties ancillary to transactions between covered financial institutions, CVC mixing service providers, and clients of either or both, such as counsel, advisors, external forensic firms, independent auditors, IT services, and other compliance facilitators or third-party service providers. In particular, FinCEN expects the proposed requirements may affect the demand for services by third party blockchain analytics companies.[116] Such companies provide transaction screening and risk rating services to financial institutions that may hire them in lieu of, or to complement,

[113] *See* discussion *supra* Section IV.A.3; *see also* Section VIII.A.1.
[114] FinCEN considered costs here proportionally to the value of the information collected and reported in connection with illicit finance-related transactions. *See* discussion *supra* Section VIII.A; *see also supra* note 90.
[115] FinCEN considered here the aggregate potential informational exposure, which depends jointly on (1) the quanta of personal information collected and reported and (2) the expected number of instances in which access to that personal information is granted in the course of a legitimate investigative or prosecutorial activity.
[116] At present, it is unclear to FinCEN whether, in light of the proposed requirements, a covered financial institution would be more likely to treat these third party services as a substitute or a complement to in-house screening and risk-management activities. Therefore while there is an expected change to demand for these third party services, the direction of this change remains unsigned.

similar functions performed in-house. Because of the specialized experience and expertise required to build a program, reporting in near real time, that not only monitors multiple blockchains, but also incorporates a multitude of additional data sources to enrich a given blockchain's transaction- and transaction party-related information, few such companies exist and the market is consequently concentrated to fewer than ten main entities.

Separately, because the proposed rule is limited in scope to only the mixing of CVC, to the extent that digital token mixing and its service providers are considered viable substitutes for CVC mixing or could otherwise be employed to obfuscate CVC mixing, the demand for token mixing and its service providers may increase as a consequence of adopting the rule as proposed.

(ii) Regulatory and Market Baseline

(A) Current Requirements

The ten categories of financial institutions covered by the proposed rule, as defined in 31 CFR 1010.100(t) are expected to already be compliant with the required activities as outlined in 31 CFR 1020 (Banks), 1021 (Casinos and Card Clubs), 1022 (Money Service Businesses) 1023 (Brokers or Dealers in Securities), 1024 (Mutual Funds), and 1026 (Futures Commission Merchants and Introducing Brokers in Commodities), as applicable. These rules include requirements for financial institutions to: (1) create and maintain compliance policies, procedures, and internal controls; (2) engage in customer identification verification; (3) file reports with FinCEN; (4) create and retain records; and (5) respond to law enforcement requests, and have guided financial institutions' understanding of FinCEN's expectations of compliant reporting and recordkeeping activity since before the advent of virtual currency. Where the original rules are silent on the application of, or compliance with, these requirements with

respect to CVC, FinCEN and OFAC have historically provided successive, iterative guidance[117] and other information[118] that clarifies expectations with respect to required practices. Furthermore, FinCEN has historically issued advisories and press releases based on FATF guidance to financial institutions,[119] including VASPs, concerning processes and legal obligations that apply to transactions involving high risk and sanctioned juridictions.

Preliminarily, evidence suggests that at least some covered financial institutions have long anticipated and appreciated the applicability of SAR and currency transaction reporting requirements to transactions involving CVC: the first SAR including language specific to a CVC was filed thirteen years ago in 2010, predating FinCEN's 2013 Guidance, and the first SAR filed by a VASP, approximately two months after the 2013 Guidance was issued, is already a decade old. Since the issuance of that guidance, FinCEN has received CVC-related SARs from approximately 4,500 distinct filers. As such, the reporting and recordkeeping requirements that would be introduced by the proposed rule may build incrementally onto an existing regulatory compliance framework, inclusive of CVC, that is well understood, and where a nontrivial proportion of covered financial institutions demonstrate willingness and ability to meet existing reporting and recordkeeping obligations.

(B) Current Market Practices

---

[117] *See* FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, Mar. 18, 2013, *available at* https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf (2013 Guidance); *see also* FinCEN 2019 CVC Guidance.

[118] *See generally* OFAC, *Questions on Virtual Currency*, *available at* https://ofac.treasury.gov/faqs/topic/1626; *see, specifically* OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry*, Oct. 2021, *available at* https://ofac.treasury.gov/media/913571/download?inline.

[119] *See, e.g.,* FinCEN, *Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies*, June 29, 2023, *available at* https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-and-4; FIN-2021-A003 "Advisory on the Financial Action Task Force-Identified Jursdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferations Deficiencies" *available at* https://www.fincen.gov/sites/default/files/advisory/2021-03-11/FATF%20February%202021%20Advisory%20FINAL%20508.pdf.

When assessing relevant baseline elements of current market practice against which to forecast the regulatory and economic impacts of special measure one requirements as proposed, FinCEN—in addition to the current regulatory requirements—also considered certain factors of current practices including: (1) the extent to which covered financial institutions are identifiably exposed to CVC mixing; and (2) the availability of reliable tools and methods with which to detect the kinds of CVC mixing exposure that would trigger the proposed reporting and recordkeeping requirements.

As a component of this analysis, FinCEN conducted an independent historical review of CVC mixing exposure occurring in the ordinary course of business at the largest registered CVC exchanges from their respective first trade dates until present.[120] As these are some of the affected covered financial institutions with highest expected exposure to CVC mixing, their relative volumes of CVC mixing-exposed transactions is likely to present a reasonable upper-bound on the proportion of currently identifiable transactions that could incur additional record-keeping and reporting requirements in connection with the imposition of the first special measure. This study found that during the period reviewed, mean (median) daily transaction volume with observable direct exposure[121] was approximately 0.010 percent (0.009 percent), while mean (median) observable indirect exposure[122] was approximately 0.234 percent (0.168 percent) of daily transaction volume. The analysis yielded comparable results when proportions

[120] This study incorporated both public and non-public data as well as certain proprietary and non-proprietary computer programs to analyze transactions occurring between calendar year 2010 at the earliest (given that each exchange has a unique start date) and the date the study was concluded (August 3, 2023).
[121] Direct exposure refers to transactions where CVC is sent from one CVC wallet address to another CVC wallet address, without the use of an intermediary. For example, if a VASP received funds from -- or sent funds to -- a CVC mixer without first going through an intermediary, that VASP has direct exposure to CVC mixing.
[122] Indirect exposure refers to transactions where CVC is sent from a CVC wallet address through at least one other wallet address to arrive at the intended recipient. For example, if CVC was sent from a CVC mixer to a CVC wallet address and then to a VASP, that VASP has indirect exposure to CVC mixing. Similarly, if CVC sent from a VASP to a CVC wallet address was subsequently send to a CVC mixer, it would be indirectly exposed to CVC mixing.

were based on share of total transactions instead of U.S. Dollar value equivalent. It would therefore appear that, to the extent that future CVC mixing exposure is consistent with past and current trends, the number of transactions that would require reporting and recordkeeping as a unique consequence of adopting special measure one as proposed is extremely low in relative terms.

FinCEN also reviewed the availability of tools, other than the use of third party blockchain analytics companies, that a financial institution currently has the option to employ to detect exposure to CVC mixing transactions in the course of complying with existing SAR and/or CTR related requirements. CVC mixing exposure can occur (directly[123] or indirectly[124]) in the process of sending CVC to, or receiving CVC from, a covered financial institution (such as a CVC exchange) and can be detected via a range of free and paid commercial software programs.[125] Free programs, such as common block explorers, can easily reveal direct[126] exposure to a CVC mixer if the CVC mixer infrastructure is relatively stable and well known, such as in the case of many Ethereum-based CVC mixers. Indirect[127] exposure may be also discoverable using these programs but might require supplementary manual investigative work to uncover. Paid commercial programs employ suites of heuristics to more comprehensively identify CVC mixers, and market themselves on their ability to automatically detect bi-directional indirect[128] and direct[129] exposure to CVC mixing activity for any blockchain address supported by the service. On blockchains supporting native smart contract capability, these

[123] *See* definition *supra* note 121.
[124] *See* definition *supra* note 122.
[125] FinCEN notes that the extent to which exclusive use of any of these tools (free or commercial software programs) would fully satisfy either existing reporting and recordkeeping requirements, or those imposed by the proposed special measure one, is a matter of facts and circumstances.
[126] *Id.* at note 121.
[127] *Id.* at note 122.
[128] *Id.* at 122.
[129] *Id.* ar 121.

automated attribution capabilities can be easily defeated if a user routes funds through token contracts or other digital asset entities providing on-chain exchange services. In such cases, analysts can still perform manual blockchain forensic tracing to identify the origin of funds.

3. *Description of the Proposed Reporting and Recordkeeping Requirements of the First Special Measure*

Imposing special measure one as proposed would introduce novel but, in many cases, incrementally modest additional recordkeeping and reporting obligations, requiring the collection and transmission of certain information in its possession when a covered financial institution knows, suspects, or has reason to suspect a transaction occurred that involved the use of CVC mixing within or involving a jurisdiction outside the United States.[130] The affected institution at which a covered transaction is conducted or attempted would need to collect required information about the covered transaction and, within 30 days of initial detection of a covered transaction, provide a report to FinCEN containing as much of the reportable required information as available to the affected institution—via electronic filing or other agency-prescribed manner.[131]

Additionally, for a specified period of time (five years[132]) after filing its report, each covered financial institution would engage in new recordkeeping activities because it would need to document its compliance with the filing procedures and the reporting requirements by: (1) maintaining a copy of any records related to CVC mixing transactions they have filed; and (2) obtaining and recording copies of documentation relating to compliance with the regulation.[133]

[130] *See* Section VI. *See also* Section IX.
[131] *See* discussion *supra* Section VI.B.2; *see also* proposed amendment 31 CFR 1010.662(b)(2) *infra* Section IX.
[132] 31 CFR 1010.430
[133] *See* discussion *supra* Section VI.B.3; *see also* proposed amendment 31 CFR 1010.662(b)(3) *infra* Section IX.

The required information would identify and describe certain unique features and characteristics of both the reportable covered transaction and the customer associated with the covered transaction. The required informational components concerning the covered transaction pertain to the CVC when transferred (currency type,[134] amount,[135] and U.S.-dollar equivalent[136]), the CVC mixer (identity[137] and/or wallet address[138]), and the transaction (hash,[139] date,[140] IP addresses and timestamps,[141] and narrative description[142]), while the required informational components concerning the associated customer include name[143], date of birth[144], addresses (physical,[145] CVC wallet,[146] and associated email[147]), phone number[148], and an entity-specific government-issued (alpha)numeric identifier.[149]

---

[134] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(B) *infra* Section IX.
[135] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(A) *infra* Section IX.
[136] *Id.*
[137] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(C) *infra* Section IX.
[138] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(D) *infra* Section IX.
[139] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(F) *infra* Section IX.
[140] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(G) *infra* Section IX.
[141] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(H) *infra* Section IX.
[142] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(I) *infra* Section IX.
[143] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(A) *infra* Section IX.
[144] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(B) *infra* Section IX.
[145] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(C) *infra* Section IX.
[146] *See* discussion *supra* Section VI.B.1(i); *see also* proposed amendment 31 CFR 1010.662(b)(1)(i)(E) *infra* Section IX.
[147] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(D) *infra* Section IX.
[148] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(E) *infra* Section IX.
[149] *See* discussion *supra* Section VI.B.1(ii); *see also* proposed amendment 31 CFR 1010.662(b)(1)(ii)(F) *infra* Section IX.

4. *Expected Economic Effects on Covered Financial Institutions*

As discussed above, the parties expected to incur an economic burden as they comply with the first special measure include all financial institutions as defined in 31 CFR 1010.100(t) insofar as they engage in CVC transactions that could be exposed to CVC mixing within or involving a jurisdiction outside the United States.[150] In light of FinCEN's review of the anticipated differential effects on covered financial institutions due to variations in both expected exposure and preexisting monitoring and detection infrastructure, as well as FinCEN's assessment of current market practices,[151] FinCEN expects that the largest portion of the novel costs incurred in complying with the first special measure will be associated with indirect[152] exposure to CVC mixing at financial institutions not currently operating primarily in the provision of virtual asset services and cases where the jurisdictions involved or under which CVC mixing occurs are particularly difficult to ascertain. However, it is unclear whether this proportion of expected novel compliance costs would itself be large because it would be difficult to uniquely identify expenses incurred distinctly as a function of special measure one compliance from expenses incurred in the course of pre-existing BSA requirements,[153] as both would largely rely on use of the same activities, technology, and services.

It is also unclear whether future relative distributions of direct[154] versus indirect[155] exposure would continue in the same pattern as historically observed, but at present do not have

[150] *See* discussion of covered financial transactions (clarifying the definitional requirement that a reportable transaction must occur in CVC) *supra* Section VI.A.4,
[151] *See* discussion of anticipated differential effects *supra* Section VIII.A.2(i)(A); s*ee also* discussion of current market practices *supra* Section VIII.A.2(ii)(B).
[152] *Id.* at note 122.
[153] *See* discussion of existing BSA requirements regarding identification and monitoring of financial transaction associations with foreign jurisdictions and geographic locations *supra* Section VI.A.5. *See also* discussion of FinCEN requirements under FATF guidance *supra* Section VIII.A.2(ii)(A).
[154] *Id.* at note 121.
[155] *Id.* at note 122.

empirical evidence that would suggest substantial changes are imminent. Detecting indirect[156] exposure may require certain financial institutions to newly obtain commercial programs and/or services to facilitate compliance with the rule as proposed as CVC mixing practices continue to evolve. The cost of these services, based on current market prices, could run in excess of tens of thousands of dollars per license and would require analysts to remain continually engaged in blockchain tracing to stay up to date with emerging trends in the rapidly developing digital asset industry. It is unclear at this time whether financial institutions or third party service providers would incur the majority of costs associated with analytical updating as CVC mixing practices evolve, or the extent to which these cost increases may be passed through to a financial institution's customers. It is also unclear how these compliance-related costs might scale with the proposed increased reporting and recordkeeping requirements because it requires speculation about how the potential for new entrants to the third party mixing detection service market and/or technological advancements (that would not occur but for the proposed compliance obligations making them economically attractive investments) would affect costs.[157]

FinCEN acknowledges to that to the extent that a covered transaction might require the filing of both a SAR and special measure one related report, concurrent satisfaction of both sets of reporting and recordkeeping requirements might result in some duplicative costs related to any overlap.

To the extent that the forgoing analysis has failed to take into consideration any material facts, data, circumstances, or other considerations that, had they been considered, would have

[156] *Id.*
[157] *See* discussion *supra* Section VIII.A.2(i)(D).

substantially altered the balance of costs and benefits attendant to the proposed special measure(s), FinCEN has invited public comment.[158]

5. *Economic Consideration of Available Regulatory Alternatives*

FinCEN has considered a number of alternative policies that could have been proposed to accomplish the same objectives.[159] These policies included the selection of one, or a combination of, other special measure(s) or, alternatively the selection of the same special measure with a narrower scope.

(i) Special Measure Two: Beneficial Ownership Information Requirements

Instead of recordkeeping and reporting requirements, FinCEN could have pursued the application of special measure two, which would have required domestic financial institutions and agencies to obtain and retain the beneficial ownership information of any account at a depository institution opened or maintained by a foreign person or their representative that the institution or agency knows, suspects, or has reason to suspect is involved in a CVC mixing transaction. While this information about beneficial ownership related to CVC mixing transaction participants could be similar to certain elements required under the current proposal and hence of comparable value, the alternative focus of special measure two on the ownership of accounts instead of the nature of transactions is expected to impose similar compliance costs with lower attendant benefits both in quantity of useful information obtained and in scope of financial institutions to whom the information-gathering requirements would apply. As such, the imposition of special measure two instead of special measure one would be strictly less efficient in addressing the class of transactions of primary money laundering concern.

[158] *See* Sections VII.A. and VII.E.
[159] *See* discussion *supra* Section V.E.

(ii) Special Measures Three through Five

Alternatively, FinCEN could have proposed to impose special measure three, four, five, or some combination thereof. Special measures three and four would simply require domestic financial institutions and agencies to obtain certain identifying information regarding the customer or their representative as a condition to open or maintain a payable-through[160] or correspondent[161] account, respectively, if the financial institution or agency knows, suspects, or has reason to suspect the account and transactions conducted through it involve CVC mixing. More severely, special measure five could have imposed prohibitions or conditions[162] on the opening or maintenance of a correspondent or payable-through account if the domestic covered financial institution or agency knows, suspects, or has reason to suspect that transactions conducted through the account involve CVC mixing.

Because the expected results of imposing special measures three, four, or both, absent special measure five would likely be similar to expectations with respect to special measure two, that analysis is not repeated here. Instead, an approach that would impose special measures three or four, or both, in conjunction with special measure five is considered. As discussed above,[163] FinCEN determined that these special measures are less relevant in the context of CVC transactions, including those that involve CVC mixing, as CVC transactions are conducted outside of the traditional banking system. Therefore, expected benefits would also be lower than under proposed special measure one requirements due to the limited intersection between transactions in CVC and the foreign use of domestic traditional bank accounts. Given these considerations, this alternative approach was rejected.

[160] 31 U.S.C. 5318A(b)(3)
[161] 31 U.S.C. 5318A(b)(4)
[162] 31 U.S.C. 5318(b)(5)
[163] *See* Section V.E.

(iii)Alternate Specification of Special Measure One: Specified Terror Finance-Related Actors and Transactions Only

Finally, FinCEN considered an alternative that would employ the same special measure but with greater specificity of covered transactions that would limit the scope of interest in CVC mixing-exposed transactions to only those identifiably sponsored by or affiliated with terror finance by Hamas, ISIS, or the DPRK. This alternative is expected to incur higher costs related to, among other things, the additional burden a financial institution would have in making a determination about a transaction's connection to an identifiable source or affiliate of the applicable terrorist organization. It would also limit the potential informational benefits of the measure by discarding similar reports and records that may be of equal or greater value to investigating, prosecuting, or disincentivizing CVC mixing supported illicit activities but lack an identifiable connection to Hamas, ISIS, or the DPRK. Because of these dual inefficiencies, special measure one as proposed is considered to strike a more appriopriate balance.

B. ***Executive Orders***

Executive Orders 12866, 13563, and 14094 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, 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.

It has been determined that this proposed rule is not a significant regulatory action under section 3(f) of Executive Order 12866, as amended. However, in light of the nature of this proposed rule, FinCEN has prepared an economic analysis to help inform its consideration of the impacts of the proposed rule.

C. *Regulatory Flexibility Act*

When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (RFA) requires the agency to ''prepare and make available for public comment an initial regulatory flexibility analysis''(IRFA) that will ''describe the impact of the proposed rule on small entities.''[164] However, Section 605 of the RFA allows an agency to certify a rule, in lieu of preparing an analysis, if the proposed rulemaking is not expected to have a significant economic impact on a substantial number of small entities.

1. *Estimate of the Number of Small Entities to Whom the Proposed Rule Will Apply*

The reporting and recordkeeping requirements proposed under the first special measure requires certain covered financial institutions to report to FinCEN information associated with transactions or attempted transactions involving CVC mixing and maintain certain related records for a fixed period of time.[165] Table 2 (below) presents FinCEN estimates of the number of affected institutions that may be deemed small entities. To identify whether a financial institution is small, FinCEN generally uses the Small Business Administration's (SBA) latest annual size standards for small entities in a given industry, unless otherwise noted.[166] FinCEN also uses the U.S. Census Bureau's publicly available 2017 Statistics of U.S. Businesses survey data (Census survey data).[167] FinCEN applies SBA size standards to the corresponding industry's receipts in the 2017 Census survey data and determines what proportion of a given

---

[164] 5 U.S.C. 603(a)

[165] See discussion supra Section VIII.A.2-3

[166] *See* U.S. Small Business Administration's *Table of Size Standards, available at* https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.

[167] *See* U.S. Census Bureau, *U.S. & states, NAICS, detailed employment sizes (U.S., 6-digit and states, NAICS sectors)* (2017), *available at* https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html. The Census survey documents the number of firms and establishments, employment numbers, and annual payroll by State, industry, and enterprise every year. Receipts data, which FinCEN uses as a proxy for revenues, is available only once every five years, with 2017 being the most recent survey year with receipt data.

industry is deemed small, on average. FinCEN considers a financial institution to be small if it has total annual receipts less than the annual SBA small entity size standard for the financial institution's industry. FinCEN applies these estimated proportions to FinCEN's current financial institution counts for brokers/dealers in securities, money services businesses, casinos, card clubs, futures commission merchants, introducing brokers in commodities, and mutual funds to determine the proportion of current small financial institutions in those industries. Numbers have been rounded as in Section VIII.A.2(i)(A) to facilitate aggregation.

TABLE 2.
ESTIMATES OF SMALL AFFECTED FINANCIAL INSTITUTIONS BY TYPE

FINANCIAL INSTITUTION TYPE[a]	NUMBER OF ENTITIES
BANK[b]	7,970[c]
BROKER/DEALER IN SECURITIES[d]	3,450[e]
MONEY SERVICES BUSINESSES[f]	24,010[g]
TELEGRAPH COMPANY[h]	0[i]
CASINO[j]	930[k]
CARD CLUB[l]	250[m]
PERSON SUBJECT TO SUPERVISION BY ANY STATE OR FEDERAL BANK SUPERVISORY AUTHORITY[n]	N/A[o]
FUTURES COMMISSION MERCHANT[p]	56[q]
INTRODUCING BROKER IN COMMODITIES[r]	900[s]
MUTUAL FUND[t]	1,380[u]

[a] As typographically grouped in 31 CFR 1010.100(t).

[b] *See* 31 CFR 1010.100(t)(1); *see also* 31 CFR 1010.100(d). The SBA currently defines small entity size standards for banks as follows: less than $850 million in total assets for commercial banks, savings institutions, and credit unions.

[c] Counts of certain types of banks, savings associations, thrifts, trust companies are from Q1 2023 Federal Financial Institutions Examination Council (FFIEC) Call Report data, *available at* https://cdr.ffiec.gov/public/pws/downloadbulkdata.aspx. Data for institutions that are not insured, are insured under non-FDIC deposit insurance regimes, or do not have a Federal functional regulator are from the FDIC's Research Information System, *available at* https://www.fdic.gov/foia/ris/index.html. Credit union data are from the NCUA for Q1 2023, *available at* https://www.ncua.gov/analysis/credit-union-corporate-call-report-data. Because data accessed through FFIEC and NCUA Call Report data provides information about asset size for banks, trusts, savings and loans, credit unions, etc., FinCEN is able to directly determine how many banks and credit unions are small by SBA size standards. Because the Call Report data does not include institutions that are not insured, are insured under non-FDIC deposit insurance regimes, or that do not have a Federal financial regulator, FinCEN assumes that all such entities listed in the FDIC's Research Information System data are small, unless they are controlled by a holding company that does not meet the SBA's definition of a small entity, and includes them in the count of small banks. Consistent with the SBA's General Principles of Affiliation, 13 CFR 121.103(a), FinCEN aggregates the assets of affiliated financial institutions using FFIEC financial data reported by bank holding companies on forms Y-9C, Y-9LP, and Y-9SP, *available at* https://www.ffiec.gov/npw/FinancialReport/FinancialDataDownload, and ownership data, *available at* https://www.ffiec.gov/npw/FinancialReport/DataDownload, when determining if an institution should be classified as small. FinCEN uses four quarters of data reported by holding companies, banks, and credit unions because a "financial institution's assets are determined by averaging the assets reported on its four quarterly financial statements for the preceding year." *See* U.S. Small Business Administration's Table of Size Standards, p. 38 n.8, https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf. FinCEN recognizes that using SBA size standards to identify small credit unions differs from the size standards applied by the NCUA. However, for consistency in this analysis, FinCEN applies the SBA-defined size standards.

[d] 31 CFR 1010.100(t)(2).

[e] The SBA currently defines small entity size standards for investment banking and securities intermediation as less than $47 million in average annual receipts. *See* paragraph preceding table for details of analysis.

[f] 31 CFR 1010.100(t)(3).

[g] The SBA currently defines small entity size standards for financial transactions processing, reserve, and clearinghouse activities as less than $47 million in average annual receipts. See paragraph preceding table for details of analysis.

[h] 31 CFR 1010.100(t)(4).

[i] As an estimate of uniquely registered, potentially affected small entities, FinCEN expect this category to contain no additional persons or organizations not already included in other counts, particularly as money transmitters.

[j] 31 CFR 1010.100(t)(5)(i)-(iii).

[k] The SBA currently defines small entity size standards for casinos as less than $34 million in average annual receipts. See paragraph preceding table for details of analysis.

[l] 31 CFR 1010.100(t)(6)(i)-(ii).

[m] The SBA currently defines small entity size standards for other gambling industries as less than $40 million in average annual receipts. See paragraph preceding table for details of analysis.

[n] 31 CFR 1010.100(t)(7).

[o] It is unclear to FinCEN at this time whether any entities exist in this category that for purposes of being counted towards unique affected parties incurring burdens associated with the rule, if adopted as proposed, are not already captured by concurrent status in another category of financial institution under the 31 CFR 1010.100(t) definition. To the extent that additional data can better inform this estimate, public comment is invited.

[p] 31 CFR 1010.100(t)(8).

[q] The SBA currently defines small entity size standards for commodity contracts intermediation as less than $47 million in average annual receipts. See paragraph preceding table for details of analysis.

[r] 31 CFR 1010.100(t)(9).

[s] *Supra* note q.

[t] 31 CFR 1010.100(t)(10).

[u] The SBA currently defines small entity size standards for open-end investment funds as less than $40 million in average annual receipts. See paragraph preceding table for details of analysis.

2. *Expectation of Impact*

For the reasons discussed above in Section VIII.A, FinCEN does not expect all potentially affected financial institutions to be equally affected by the proposed rule.[168] These expectations of differential effects are of first-order relevance because, for the purposes of the IRFA, a rulemaking must be jointly impactful in both its breadth (substantial number) and depth (significant economic impact) on small entities to require additional, tailored analysis. FinCEN's categorical analysis of the financial institutions defined in 31 CFR 1010.100(t) does not support the need for an initial regulatory flexibility analysis because it determined that, in cases where a substantial number of financial institutions are small entities, the economic impact of the rule is not expected to be significant. Conversely, in cases where the economic impact is expected to be its most significant, it is not clear that a substantial number of affected institutions would meet the criteria to qualify as small entities.

To the extent that other small entities that are not financial institutions may be economically affected by the proposed rulemaking,[169] FinCEN did not include any estimates of affected parties or calculations of effects in this IRFA because those effects, for most non-financial institutions, are primarily expected to be benefits in the form of potential increases in demands for services. An attempt to quantify increased operating costs accompanying these increases in demand generally, and for small entities specifically, would be so speculative as to be uninformative. In the event that a more precise forecast could be reliably formed with available data and would alter the conclusions of this analysis, FinCEN is requesting information from the public.

[168] *See* discussion *supra* Section VIII.A.2(i)(A).
[169] *See, e.g.,* discussion *supra* Section VIII.A.2(i)(D).

3. *Certification*

When viewed as a whole, FinCEN does not anticipate that the proposals contained in this rulemaking will have a significant impact on a substantial number of small financial institutions or other potentially affected businesses. Accordingly, FinCEN certifies that this rule will not have a significant economic impact on a substantial number of small entities. FinCEN invites comments from members of the public who believe there will be a significant economic impact on small entities from the imposition of the first special measure regarding CVC mixers.[170]

D. *Unfunded Mandates Reform Act*

Section 202 of the Unfunded Mandates Reform Act of 1995[171] (Unfunded Mandates Reform Act), 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, adjusted for inflation.[172] If a budgetary impact statement is required, section 202 of the Unfunded Mandates Reform Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule.[173]

As discussed in the foregoing analysis,[174] it is unclear if either the gross or net cost of compliance to the private sector would exceed $177 million annually.[175] In the event that this is

[170] *See* Section VII.E.
[171] Public Law 104–4 (March 22, 1995).
[172] *Id.*
[173] *Id.*
[174] *See* Section VIII.A.4.
[175] The Unfunded Mandates Reform Act requires an assessment of mandates that will result in an annual expenditure of $100 million or more, adjusted for inflation. The U.S. Bureau of Economic Analysis reports the annual value of the gross domestic product (GDP) deflator in 1995, the year of the Unfunded Mandates Reform Act, as 71.823, and as 127.224 in 2022. *See* U.S. Bureau of Economic Analysis, "Table 1.1.9. Implicit Price Deflators for Gross Domestic Product" (accessed Friday, June 2, 2023) *available at* https://apps.bea.gov/iTable/?reqid=19&step=3&isuri=1&1921=survey&1903=13t. Thus, the inflation adjusted estimate for $100 million is 127.224/71.823 × 100 = $177 million.

so, FinCEN has performed the preliminary analysis above to address the potential need to satisfy the requirements of the Unfunded Mandates Reform Act.[176] FinCEN is additionally soliciting comments—preferably including data, studies, or other forms of quantitative analysis—that would specifically inform our quantification of expected compliance related expenditures by state, local, and tribal governments and/or the private sector in the event that such costs would, in light of more complete information, be demonstrably expected to exceed the annual $100 million threshold, adjusted for inflation ($177 million).

E. *Paperwork Reduction Act*

The recordkeeping and reporting requirements contained in this proposed rule will be submitted by FinCEN to the Office of Management and Budget for review in accordance with the Paperwork Reduction Act of 1995[177] (PRA). Under the PRA, 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 proposed information collection can be submitted by visiting www.reginfo.gov/public/do/PRAMain. Find this particular document by selecting ‘‘Currently under Review—Open for Public Comments’’ or by using the search function. Comments are welcome and must be received by [90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. In accordance with requirements of the PRA and its implementing regulations, 5 CFR part 1320, the following information concerning the collection of information as required by 31 CFR 1010.662 is presented to assist those persons wishing to comment on the information collections.

[176] *See generally,* discussion *supra* Section VIII.A; *see specifically,* discussion of alternatives considered *supra* Section V.E. and Section VIII.A.5.
[177] 44 U.S.C. 3507(d).

The provisions in this proposed rule pertaining to the collection of information can be found in section 1010.662(b)(1). The information required to be reported in section 1010.662(b)(1) will be used by the U.S. Government to monitor the class of transactions of primary money laundering concern. The information required to be maintained by section 1010.662(b)(3) will be used by federal agencies and certain self-regulatory organizations to verify compliance by covered financial institutions with the provisions of 31 CFR 1010.662. The class of financial transactions affected by the reporting requirement is identical to the class of financial transactions affected by the recordkeeping requirement. The collection of information is mandatory.

Frequency: Covered financial institutions would be required to file within 30 days of detecting a covered transaction.[178] As nothing prevents a covered financial institution from optimizing with respect to scale by filing later, while still within the 30-day limit, it is foreseeable that despite a distinct filing obligation per covered transaction, some entities may elect to file all required reports still within the same 30-day window at a single time, effectively reducing the frequency of filing.

Description of Affected Financial Institutions: Only those covered financial institutions defined in section 1010.662(a)(4) with engagement in the covered financial transactions as defined in section 1010.662(a)(5) would be affected.

Estimated Number of Affected Financial Institutions: Approximately 15,000[179]

[178] 31 CFR 1010.662(b)(2)

[179] This estimate is informed by public and non-public data sources regarding both an expected maximum number of entities that may be affected and the number of active, or currently reporting, registered financial institutions and takes into consideration the possibility of voluntary reporting by certain parties without an express obligation to file reports. *See* Section VIII.A.2(i)(A).

Estimated Average Annual Burden in Hours Per Affected Financial Institution: 98[180]

Estimated Total Annual Burden: 1,470,000 hours

FinCEN specifically invites comments on: (a) whether the proposed collection of information is necessary for the proper performance of the mission of FinCEN, including whether the information would have practical utility; (b) the accuracy of FinCEN's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information required to be maintained; (d) ways to minimize the burden of the required collection of information, including through the use of automated collection techniques or other forms of information technology; (e) estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to report the information.

IX. Regulatory Text

List of Subjects in 31 C.F.R. Part 1010

Administrative practice and procedure, Banks, Banking, Brokers, Crime, Foreign banking, Terrorism.

Authority and Issuance

For the reasons set forth in the preamble, FinCEN proposes amending 31 C.F.R. part 1010 as follows:

Part 1010-GENERAL PROVISIONS

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

[180] Assumes, on average, one full work-day per 30-day period is required to complete reporting and recordkeeping related tasks. Due to the anticipated skew in expected annual burden hours, this average is unlikely to represent a meaningful approximation for most covered financial institutions.

"Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C.5311-5314, 5316- 5336; title III, sec. 314, Pub. L. 107-56, 115 Stat. 307; sec. 2006, Pub. L. 114-41, 129 Stat. 458-459; sec. 701 Pub. L. 114-74, 129 Stat. 599; sec. 6403, Pub. L. 116-283, 134 Stat. 3388."

2. Add § 1010.662 to read as follows:

§ 1010.662 Special measures regarding CVC mixing transactions.

(a) *Definitions.* For purposes of this section, the following terms have the following meanings.

(1) *Convertible Virtual Currency (CVC*). The term "convertible virtual currency (CVC)" means a medium of exchange that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status. Although Bitcoin has legal tender status in at least two jurisdictions, the term CVC includes Bitcoin for the purpose of this section.

(2) *CVC Mixer.* The term "CVC mixer" means any person, group, service, code, tool, or function that facilitates CVC mixing.

(3) *CVC mixing.*

(i) The term "CVC mixing" means the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions, regardless of the type of protocol or service used, such as:

(A) Pooling or aggregating CVC from multiple persons, wallets, addresses, or accounts;

(B) Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction;

(C) Splitting CVC for transmittal and transmitting the CVC through a series of independent transactions;

(D) Creating and using single-use wallets, addresses, or accounts, and sending CVC through such wallets, addresses, or accounts through a series of independent transactions;

(E) Exchanging between types of CVC or other digital assets; or

(F) Facilitating user-initiated delays in transactional activity.

(ii) *Exception.* Notwithstanding paragraph (a)(3)(i), CVC mixing does not include the use of internal protocols or processes to execute transactions by banks, broker-dealers, or money services businesses, including virtual asset service providers that would otherwise constitute CVC mixing, provided that these financial institutions preserve records of the source and destination of CVC transactions when using such internal protocols and processes; and provide such records to regulators and law enforcement, where required by law.

(4) *Covered financial institution.* The term "covered financial institution" has the same meaning as "financial institution" in 31 C.F.R. § 1010.100(t).

(5) *Covered transaction.* The term "covered transaction" means a transaction as defined in 31 CFR § 1010.100(bbb)(1) in CVC by, through, or to the covered financial institution that the covered financial institution knows, suspects, or has reason to suspect involves CVC mixing within or involving a jurisdiction outside the United States.[181]

[181] This requirement would be independent of any recordkeeping requirement pursuant to 31 CFR 1010.410.

(b) *Reporting and recordkeeping requirements.* Covered financial institutions are required to report information in accordance with paragraph (b)(1) and maintain records demonstrating compliance in accordance with paragraph (b)(3) of this section.

(1) *Reporting.*

(i) *Reportable information regarding the covered transaction.* The covered financial institution shall provide the following reportable information in its possession, with respect to each covered transaction, within 30 calendar days of initial detection of a covered transaction:

(A) The amount of any CVC transferred, in both CVC and its U.S. dollar equivalent when the transaction was initiated;

(B) The CVC type;

(C) The CVC mixer used, if known;

(D) CVC wallet address associated with the mixer;

(E) CVC wallet address associated with the customer;

(F) Transaction hash;

(G) Date of transaction;

(H) The IP addresses and time stamps associated with the covered transaction; and

(I) Narrative

(ii) *Reportable information regarding the customer associated with the covered transaction.* The covered financial institution shall provide the following

reportable information in its possession, regarding the customer associated with each covered transaction:

(A) Customer's full name;

(B) Customer's date of birth;

(C) Customer's address;

(D) Email address associated with any and all accounts from which or to which the CVC was transferred;

(E) Phone number associated with any and all accounts from which or to which the CVC was transferred;

(F) Internal Revenue Service or foreign tax identification number, or if none are available, a non-expired United States or foreign passport number or other government-issued photo identification number, such as a driver's license; and

(2) *Filing procedures*. The reports required under paragraphs (b)(1) of this section shall be filed with FinCEN 30 calendar days from the date of detection in the manner that FinCEN prescribes.

(3) *Recordkeeping.* A covered financial institution is required to document its compliance with the requirements of this section.

Dated: October 19, 2023

Andrea M. Gacki
Director
Financial Crimes Enforcement Network