Submitted Via: http://www.regulations.gov

January 4, 2021

Kenneth A. Blanco
Policy Division, Financial Crimes Enforcement Network (FinCEN)
P.O. Box 39
Vienna, VA 22183 USA

RE: *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital* (Docket Number FINCEN-2020-0020; RIN 1506-AB47)

Dear Director Blanco,

Gemini appreciates the opportunity to provide comments to the United States Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") in response to FinCEN's proposal to enhance requirements for certain transactions involving "convertible virtual currency" ("CVC") or "digital assets with legal tender status" ("LTDA") that was published in the Federal Register on December 23, 2020 (the "Proposed Rule"). Although the provided 15-day response period is improperly abbreviated, we use this opportunity to strongly request a more appropriate response period and consideration of the points detailed below.

Gemini is a leading regulated United States digital asset exchange and custodian with a strong conviction that blockchain technology and cryptocurrency have the potential to transform the design of the Internet, and to improve our financial system and money in a way that fosters and protects the financial rights and dignity of the individual. If developed with the right balance of innovation and regulation, digital assets can advance personal financial freedom and economic progress.

To this end, we have built our business on a foundation of regulatory compliance, and we believe that sound regulation is necessary to enhance trust in -- and the integrity of -- cryptocurrency markets. We are committed to working with regulators and policymakers to

help shape appropriate regulatory frameworks that allow for the ongoing development of blockchain technologies, the ongoing leadership of United States-based innovation, and the effectuation of legitimate governmental objectives.

Gemini was founded with a "security-first" mentality, and ethos of asking for permission, not forgiveness. Gemini is a New York trust company regulated by the New York State Department of Financial Services ("NYSDFS"). Gemini is also registered with FinCEN as a money services business ("MSB") and maintains money transmitter licenses (or the statutory equivalent) in all states where this is required. We are subject to capital reserve requirements, cybersecurity requirements, and banking compliance standards set forth by the NYSDFS and the New York Banking Law. We are further subject to and compliant with the Bank Secrecy Act (BSA), and related FinCEN reporting requirements.

We submit this comment letter with serious concern regarding FinCEN's Notice of Proposed Rulemaking ("NPRM"). While we recognize that the Proposed Rule raises topics of appropriate regulatory and law enforcement interest, we are concerned that this hasty proposal will fail to satisfy those interests due to three primary deficiencies that could potentially be cured through thoughtful deliberation and engagement with key stakeholders, including the cryptocurrency industry.

The first primary deficiency is fundamental to the proposal. As conceived, the Proposed Rule would be unlikely to stem illicit financial activity, and it would instead have the inverse effect, likely driving cryptocurrency activity out of the regulatory purview of the well-regulated United States markets and into unregulated markets. This core deficiency is exacerbated by the fact that the Proposed Rule would have a material deleterious effect on individual privacy, without commensurate law enforcement benefits.

Second, the Proposed Rule is replete with ambiguity that would severely undermine good faith compliance efforts and could have a detrimental impact on the United States' ability to remain at the forefront of innovation. Specifically, among other things, this ambiguity could at best slow down decentralized finance ("DeFi") innovation, or at worst kill further development. Absent clarification, the United States cryptocurrency industry would be at a substantial disadvantage to global competitors and would likely have to step back from some of the most promising aspects of, and developments regarding, cryptocurrency and blockchain technology.

Finally, the Proposed Rule is undermined by a clear lack of process in its development, which undermines FinCEN's stated justification for its immediate implementation: national security concerns. As drafted, all that this rule will do is drive bad actors to first systematically withdraw their cryptocurrency from existing regulated United States exchanges into their personal wallets and then to proceed with whatever illicit activity they contemplated. FinCEN and other regulators will have less visibility into bad actors' use of cryptocurrency. That nefarious activity, to be clear, is a sliver of the overall activity associated with this promising technology. If FinCEN instead engages with the industry in order to better understand cryptocurrency technologies and markets through a normal, collaborative rulemaking process, then it would be possible to craft rules that properly serve legitimate governmental interests, while minimizing impact on law-abiding cryptocurrency market participants and United States citizens.

Level-Setting on the Issues at Hand

Before delving into the three issues noted above, it is important to level-set on the core topic raised in the Proposed Rule. Cryptocurrencies are by their very nature digital bearer instruments whereby the owner possesses a private key to control and prove ownership over an asset. This aspect is analogous to an individual literally holding physical cash, which demonstrates ownership over that cash and gives the individual the power to transfer it to someone else.

In response to this defining attribute -- cryptocurrency being a digital bearer instrument -- a range of custodial solutions have been developed in recent years in order to help individuals safeguard their assets. Solutions range from literally printing or writing a private key on a piece of paper to software that helps an individual store his or her keys to managed custodial systems where an intermediary like Gemini safeguards a customer's cryptocurrency assets. This latter category largely comprises the banks and MSBs subject to the Proposed Rule.

The full range of custodial solutions, however, is more of a continually developing spectrum of different approaches and services, which can be difficult to specifically define. While custody of cryptocurrency assets certainly raises important regulatory considerations, including proper application of the BSA and related AML/KYC requirements, it is important to understand the fundamentals and nuances of cryptocurrency assets and blockchain technology.

Indeed, it is only through careful consideration of the underlying technology and distinctions in custodial solutions that proper regulatory requirements can be created that will minimize

market disruption, while most effectively meeting regulatory objectives. Hasty regulation runs the real risk of driving activity out of the United States and into the shadows, chilling ongoing innovation, and damaging the role of the United States in developing global blockchain technologies and cryptocurrency markets.

The Proposed Rule Will Not Satisfy Core Regulatory Objectives, but Will Impose High Costs on United States Businesses (Questions 2, 4, 12, 18)

As a threshold matter, FinCEN's proposal will not effectively serve legitimate national security and law enforcement objectives. The goal of the BSA is to combat the illicit flow of funds and provide law enforcement with actionable information regarding potential proceeds of crime. The fundamental flaw in the Proposed Rule is how easily its objectives can be thwarted.

More specifically, if a customer of a bank or MSB -- who has already been subject to the entity's Know Your Customer ("KYC") protocols -- wants to send cryptocurrency to, or receive cryptocurrency from, a known bad actor, then all he or she needs to do is first send cryptocurrency to or receive cryptocurrency from a so-called "unhosted" or, more accurately defined, "self-hosted" wallet that the customer owns. The Proposed Rule would then readily permit that individual to send cryptocurrencies from his or her self-hosted wallet to the exchange or receive the cryptocurrency from the exchange to his or her self-hosted wallet. Once the cryptocurrency is in a self-hosted wallet, it can be transacted on the blockchain to or from another self-hosted wallet and not be captured by the requirements of the Proposed Rule.

This above reality means that bad actors will easily be able to circumvent the Proposed Rule. Rather than force activity further away from compliant, regulated banks and MSBs, FinCEN should pursue opportunities to collaborate with the regulated cryptocurrency industry participants[1] on ways to identify problematic activity without offering bad actors a clear roadmap of how to engage in financial crime transactions and avoid detection.

Additionally, the Proposed Rule will result in a substantial loss of personal privacy despite providing minimal law enforcement benefit. Indeed, a counterparty engaging in legitimate cryptocurrency transactions with a customer of a bank or an MSB will now have his or her information collected and sometimes reported to FinCEN without taking any affirmative steps (or even knowing) that such information is being reported. This type of mass

[1] In the Proposed Rule, FinCEN notes that in 2019 alone it had received "approximately $119 billion in suspicious activity reporting associated with CVC activity taking place wholly or in substantial part in the United States."

information-gathering is well outside of the BSA and United States privacy norms, especially given the breadth of subsequent blockchain surveillance.

The above dynamics should drive a deliberative re-think of the most effective way to solve for appropriate regulatory interests, while minimizing the impact on privacy. This is especially true when the burden of complying with the Proposed Rule is unduly onerous for the industry. In fact, in the preamble to the Proposed Rule, FinCEN emphasized that the "the reporting burden [under the Proposed Rule] will possibly be more complicated than the requirement to transmit information in the Funds Transfer / Travel Rule NPRM given the variety of information required by the reporting form." The NPRM also estimates that the total ***minimum*** annual burden hours imposed by the Proposed Rule will be 1,284,349 hours. Gemini believes that the actual burden will be significantly higher than this estimate, but even the NPRM's compliance estimate of over a million hours would be a significant cost to this industry.

More specifically, according to its own analysis, FinCEN estimates that 164% and 239% as many transactions would be covered by the requirements set forth in the Proposed Rule at the $10,000 level and in the $3,000 to $10,000 range, respectively, in comparison to the recordkeeping requirements in the Funds Transfer / Travel Rule NPRM. This would mark a substantial increase in process, and we anticipate it will require a substantial increase in compliance staff and resources. To impose this additional burden on the industry at a time when FinCEN is also proposing new requirements under the Travel Rule NPRM runs the risk of overwhelming the cryptocurrency industry in the United States and impeding its further development. FinCEN should weigh the associated burdens that would be imposed on the cryptocurrency industry against the minimal law enforcement benefit the Proposed Rule would likely provide.

The Proposed Rule Is Ambiguous, Which Will Undermine Compliance and Impede Promising Innovation (Questions 14, 24)

Given the fast-developing nature of the cryptocurrency industry and the definitional nuance noted above, it is critical that regulation be clear in its application and compliance requirements. Unfortunately, the Proposed Rule fails to define critical regulatory elements and fails to provide enough clarity to permit compliance. This ambiguity will either undermine compliance or broadly impede innovation in key areas, including DeFi.

With respect to definitions, the Proposed Rule fails to clarify or provide a workable definition for CVC, other than to say that CVC is a "medium of exchange, such as cryptocurrency [also not a defined term], that either has an equivalent value as currency, or acts as a substitute for currency but lacks legal tender status." This description of CVC is overly broad and may have the unintended consequence of being interpreted to encompass a variety of digital and blockchain-based assets. Gemini urges FinCEN to provide a more tailored definition for CVC to ensure it achieves the appropriate balance between addressing FinCEN's goals, while safeguarding individual privacy and reducing unnecessary compliance burdens borne by banks and MSBs covered by the Proposed Rule.

Given the lack of clear definition of CVC, there is an added layer of ambiguity concerning reporting obligations involving "multiple transactions in convertible virtual currency…" Based on the current language of the Proposed Rule, the aggregation requirements for "CVC" -- unlike fiat transaction -- could be interpreted to apply across different digital assets. This would appear to be unnecessarily more stringent and unduly punitive against the cryptocurrency industry, especially since as FinCEN has itself noted in the Proposed Rule, CVC "allow[s] a bank or MSB to identify the full transaction history of the CVC or LTDA value involved in the transaction (i.e., the entire transaction history of the value from the transaction block it was mined)." Gemini urges FinCEN to clarify its aggregation requirements to apply to transactions involving one type of CVC, consistent with fiat-related currency transaction reporting requirements.

The Proposed Rule also seeks to except from the requirement to retain certain records, transactions involving a "counterparty whose account is held at a financial institution regulated under the BSA, or at a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the List of Foreign Jurisdictions…"

The mere identification of whether a counterparty has an account with a financial institution or not is a challenge in the cryptocurrency ecosystem, as was previously laid out in a response to FinCEN's Travel Rule NPRM. Specifically, Gemini joined other members of the United States Travel Rule Working Group ("USTRWG")[2] in providing a response and articulating that applying a set of rules designed for fiat transactions to transactions involving CVC presents a unique set of challenges. In its response to FinCEN's Travel Rule NPRM, USTRWG explained that as it is currently written, the Travel Rule "presupposes that a receiving financial institution and

[2] https://beta.regulations.gov/comment/FINCEN-2020-0002-2787

beneficiary can be identified as part of the transmittal order and that information can be transmitted to the receiving financial institution with ease."

This is not the case in the CVC ecosystem. Rather, "[a]n originating [Virtual Asset Service Provider] knows the identity of its own customer, the USD-equivalent value of the transaction, and the destination address that appears on the blockchain. Yet generally, an originating VASP does not know other details about the transmittal which are relevant to Travel Rule compliance, including (1) whether the recipient address is associated with a VASP or an unhosted wallet; or (2) whether the receiving VASP and/or beneficiary are located in the United States or abroad." As with the Travel Rule NPRM, this Proposed Rule fails to take into account this aspect of CVC markets and transactions.

The Proposed Rule also fails to properly define an "unhosted wallet" amongst the many iterations of custody solutions that fall along the previously noted spectrum of solutions ranging from writing down a private key to using hardware or software products. This nuance matters because it gets to the core of what FinCEN will deem to be in scope for compliance. In other words, do the steps required to capture and assess counterparty name and address information vary depending on the custodial solution being deployed? How does one "prove" ownership over various wallet solutions, which at their essence are focused on ensuring possession of a private key?

Gemini strongly suggests that, should FinCEN move forward with aspects of this Proposed Rule notwithstanding these ambiguities, then it must adopt the standards outlined in FinCEN's Customer Due Diligence Requirements for Financial Institutions (the "CDD Rule").

Specifically, the CDD Rule clarifies that a covered financial institution may rely on the information supplied by the legal entity customers regarding the identities of those customers' beneficial owner or owners, provided that the financial institution has no knowledge of facts that would reasonably call into question the reliability of such information. Gemini urges FinCEN to follow the reasonable precedent it set in the CDD Rule, and to explicitly allow banks and MSBs to rely on information supplied by their customers regarding the "unhosted wallet" counterparty to and from which those customers transmit cryptocurrency.[3]

[3] "Counterparty information" shall include information concerning whether the counterparty's account is held by a financial institution and whether that financial institution is located in a jurisdiction listed on FinCEN's List of Foreign Jurisdictions.

To further reduce unnecessary operational burden on the banks and MSBs covered by the Proposed Rule, Gemini urges FinCEN to clarify the scope of accounts that would be covered by the exception[4], by removing "regulated under the BSA" from the scope of domestic financial institutions. As it currently reads, the Proposed Rule would impose a higher threshold for domestic financial institutions than it would for foreign financial institutions. This clarification would align accounts covered by the exception, whether held at domestic or foreign financial institutions, except for financial institutions listed on FinCEN's List of Foreign Jurisdictions that are not covered by the exception.

The Proposed Rule also introduces a number of additional ambiguities that, if implemented as currently drafted, would further complicate and increase the cost of compliance. For example, for purposes of aggregation with respect to the CVC/LTDA transaction reporting requirement, the Proposed Rule would require a bank or MSB to include "all of its offices and records, wherever they may be located." By contrast, for purposes of fiat aggregation, the current Aggregation rule[5] requires the inclusion of only "domestic branch offices, and any recordkeeping facility, wherever located, that contains records relating to the transactions of the institution's domestic offices." The rationale for this disparate treatment, according to FinCEN, is "[b]ecause a bank or MSB may provide CVC or LTDA hosting through distinct corporate structures and from different physical locations."

Yet, such unprecedented reach by a regulator is overly broad and provides little clarity with respect to rule applicability. FinCEN should not be seeking to impose even more stringent and costly regulations on the cryptocurrency industry as compared to general financial services providers. Gemini accordingly urges FinCEN to limit in-scope branches to domestic branches only.

The Proposed Rule would also introduce an ambiguity with respect to customer identity verification requirements. Specifically, the Proposed Rule, as written, would require a bank or an MSB "before concluding any transaction in relation to which records must be maintained under this paragraph…[to] verify the identity of its customer engaging in the transaction[6]." This would introduce an unprecedented requirement to re-verify the identity of a bank's or an MSB's customer each time the customer would seek to effect an in-scope transaction in excess of $3,000. Again, this requirement would appear to be punitive against the cryptocurrency industry and depart from regulatory norms.

[4] 31 CFR § 1010.316(d)
[5] 31 CFR § 1010.313(a)
[6] 31 CFR § 1010.410(g)(2)

Gemini accordingly urges FinCEN to remove the requirement to re-verify the identity of a customer each time a customer seeks to engage in an in-scope transaction, provided that a bank or an MSB has previously identified and verified the identity of its customer, subject to any ongoing customer due diligence requirements, as applicable.

Specific DeFi Ambiguity and Concerns

The existing ambiguity in the Proposed Rule is also of particular concern with respect to DeFi innovation. DeFi protocols are not managed by an institution or even an individual but instead by autonomous smart contract technology. Using blockchain-based smart contracts, DeFi replaces much of the functionality currently offered by traditional finance, and therefore it has the promise to drive greater automation, efficiency, and access to financial markets and services than the legacy systems provide. A failure by FinCEN to recognize this dynamic, and to craft appropriately nuanced regulations to govern it, would mark a failure to advance sound policy and would put United States innovation at a substantial disadvantage to global competitors.

As an initial matter, it is unclear whether the requirements of the Proposed Rule implicate DeFi (e.g., whether and to what extent "unhosted wallet" includes a smart contract wallet) and if it does, how a bank or MSB will meet the Proposed Rule's requirements when facilitating a transfer to or from a smart contract wallet at the direction of a customer. Smart contracts are programmed to automate certain activities when a user sends cryptocurrency to a contract address. Smart contracts are software, but a user does not necessarily control a private key to the smart contract's wallet. The contract's code ultimately determines how assets sent to the contract are transferred or utilized.

The Proposed Rule, however, offers no clarity on whether the sending and receiving of funds through an autonomous smart contract would constitute transactions with an "unhosted wallet." If such transactions are meant to be in scope of the Proposed Rule, FinCEN should specify how a bank or MSB should determine the counterparty when their users send funds to a smart contract. By design, control of autonomous smart contracts is decentralized. The contract itself is the counterparty. Stated otherwise, the very premise of an autonomous smart contract is that there is no such available information to collect. Such a network by definition lacks a central intermediary, direct owner, or an individual controlling the network.

Absent guidance or an appropriate safe harbor, the Proposed Rule would effectively cut off bank or MSB customer access to DeFi networks. This will have the draconian effect of prohibiting banks and MSBs to provide DeFi product offerings to its customers and in turn, preventing these customers' access to this innovative technology that will likely drive the next wave of inclusion and efficiency benefits to US markets. Alternatively, and as noted above, customers can simply remove cryptocurrency to a self-hosted wallet and then transact with the DeFi network -- this will *decrease* potential regulator access to information in the event illicit activity is suspected.

FinCEN should ultimately provide greater guidance, and perhaps consider a safe harbor regarding DeFi networks -- meaning, to exclude from the definition of an "unhosted wallet" those wallet addresses that are managed by autonomous smart contracts with no identifiable owner or controller. Absent such clarity, FinCEN will be choking off an important area of innovation that could deliver more value with less friction than the existing financial system.

The Proposed Rule Can be Substantially Improved and Satisfy Appropriate Regulatory Interests through Proper Procedure and a Deliberative Process

Gemini unequivocally supports the critical goal of FinCEN in protecting against illicit financial activity. Given the importance of this goal, however, an abbreviated 15-day comment period spanning two federal holidays is woefully inadequate to allow Gemini, or other industry stakeholders, the opportunity to properly understand the implications of the Proposed Rule and provide a comprehensive response to the many issues and questions outlined in the NPRM. Given our deep understanding of how cryptocurrency technology works and how we interact with it, Gemini wants to assist FinCEN in crafting appropriate regulations that successfully combat illicit financial activity. This truncated time period severely hinders our ability to do so.

If FinCEN's stated intention is to combat money laundering and terrorist financing activity, it would benefit both FinCEN and industry participants to have a more appropriate time period to understand, analyze and consider the proper framework for the Proposed Rule. The lack of a deliberative process yields hasty and confusing consequences. For example, it is concerning that the 72-page NPRM lacks a clear definition of what constitutes an "unhosted wallet," yet the proposal expects banks and MSBs to comply with these ambiguous requirements when interacting with an unhosted wallet.

As FinCEN is well aware, the cryptocurrency market is built on a technology with significant distinctions from that of the traditional financial markets, but this hasty, rushed process (and the NPRM) fail to properly account for such distinctions. Additionally, we note with concern additional procedural deficiencies with this rulemaking process: lack of a clear legal justification or rationale for such a process; the alarming departure from the more traditional 60 or 90-day comment period for significant regulatory actions; the lack of a rationale for disparate treatment of the cryptocurrency industry; and an apparent lack of compliance with the requirements in the Administrative Procedure Act.

Many of the above procedural deficiencies are further addressed in the response submitted by the Chamber of Digital Commerce (the "Chamber"), which Gemini is pleased to also join. The Chamber's response provides further analysis on key elements, including implementation and compliance challenges (and associated burdens) on the industry, lack of clarity as to the actual requirements of the Proposed Rule, and privacy risks in complying with the Proposed Rule.

Gemini would welcome a more fulsome opportunity to engage on the important issues raised by the Proposed Rule, and we encourage an open, deliberative, and collaborative regulatory process. To that end, we strongly encourage reconsideration of the unnecessarily abbreviated timeline indicated by this NPRM.

The United States regulatory system is the envy of the world because of our commitment to sound process and robust discussion. We appreciate your consideration, and hope for the opportunity to engage in further dialogue.

Sincerely,

Sydney Schaub
General Counsel
Gemini Trust Company, LLC