Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Notice of Proposed Rulemaking Regarding the Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

January 2021

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the Financial Crimes Enforcement Network (FinCEN), Department of Treasury, on "proposed rulemaking to seek public comments on a proposal to require banks and money service businesses ("MSBs") to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA") held in un-hosted wallets, or held in wallets hosted in a jurisdiction identified by FinCEN."

GLEIF encourages FinCEN to mandate the Legal Entity Identifier (LEI) within the client and counterparty identification and verification, and recordkeeping processes and submitted reports as defined within the certain sections of the Code of Federal Regulations (CFR), as applicable.

GLEIF would like to provide comments for the (19) "Describe the benefits to law enforcement from being able to access data verified and obtained based on the proposed recordkeeping and verification requirements" and (24) "Describe technical challenges to implementation to could impact reasonable ability to implement these requirements."

GLEIF agrees with the FinCEN that "unhosted" wallets and anonymized or pseudonymized information about the transaction record present significant illicit financial activity risks. Malign actors exploit gaps in identity verification, recordkeeping and reporting regimes across borders and engage in illicit financial activity without detection or traceability.

As the examples provided by FinCEN display, actors involved in money laundering schemes use legal entities as a shield to facilitate international terrorist financing, weapons proliferation, sanctions evasion, and transnational money laundering, as well as to buy and sell controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals.

Therefore, GLEIF suggests that a consistent, high quality and globally recognized identifier for legal entity clients is absolutely essential to tackle anti-money laundering in today's digital world. The LEI is the essential building block for legal entity "client identification" in AML programs as shared by GLEIF in its response to the FinCEN's Anti-Money Laundering Program Effectiveness Advance Notice of Proposed Rulemaking.

The LEI is the only global standard for legal entity identification. It is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information, including legal name and legal address, that enables clear and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure and thus answers the questions of 'who is who' and

'who owns whom'. Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace.

The value proposition of LEI has already been recognized by several U.S. regulators such as the Federal Reserve, Consumer Financial Protection Bureau, Municipal Securities Rulemaking Board, National Association of Insurance Commissioners, and U.S. Treasury. The U.S. Customs and Border Protection is working on the Global Business Identifier (GBI) Initiative, in which the Bureau will test the LEI as part of an evaluative proof of concept to determine the optimal GBI solution.

FinCEN highlights that some types of CVC pose particularly severe illicit finance challenges, such as the anonymity enhanced cryptocurrency ("AEC") protocols which limit the ability of investigators or other parties to follow transaction flows on the associated distributed public ledgers.

GLEIF thinks that parties to a crypto-asset transaction should never be considered anonymous and furthermore should be identified via a global standard, the LEI, so as to ensure that a framework for prudential treatment of crypto-assets may develop. This requirement should expand to hosted wallet providers and wallet owners; so that risk exposure of these parties can be better evaluated across borders. Therefore, GLEIF understands that although financial institutions or money service providers are regulated entities and have obligations under Bank Secrecy Act, identifying their customers via the LEI would be key for accurately establishing the risk profiles.

Therefore, GLEIF suggests that the proposed reporting requirement could apply to transactions involving CVC or LTDA between a bank's or MSB's hosted wallet customer and an unhosted or otherwise covered wallet and include transactions between hosted wallets.

Due to the global nature of these transactions, the proposed requirement that financial institutions require the collection of the name and physical address of the customer's counterparty, when engaging in a transaction reportable pursuant to the proposed CVC/LTDA transaction reporting requirement, is not sufficient.

In addition to the entity's name, the inclusion of the LEI would guarantee a unique and unambiguous identifier is associated with the entity. This identifier also links to the direct and ultimate parents of the legal entity. FinCEN could avoid name matching and the associated manual reconciliations of client identity and instead focus on the report's substantive details. Data lineage is a key component to tracking entities over time. As such, the LEI could be used as the primary entity identifier for tracking legal entities reported to FinCEN, thus creating a historical record per entity over time. The LEI could also be used to track all reports from each reporting financial institution historically. Aggregation of reported content could be achieved by associating the LEI of the entity to the LEI of the reporting financial institution.

Moreover, the proposed 31 CFR 1010.316 would exempt from required reporting those transactions that are between a filer's hosted wallet customer and a counterparty hosted wallet at a financial institution that is either regulated under the BSA or located in a foreign jurisdiction that is not on the Foreign Jurisdictions List. Given the Global LEI Repository provides headquarter and legal address of an entity in a standardized way, financial institutions can easily analyze if the counterparty is located in a jurisdiction identified on the Foreign Jurisdictions List.

The LEI would also help reporting financial institutions and MSBs to identify, verify and report transactions involving multiple senders and recipients.

Virtual Assets is a rapidly developing area in the global financial system. The licensing and registration of the VASP in the jurisdiction where it is created is an essential step to curb the anonymity and reduce the ML/FT risks. Ideally, all jurisdictions shall apply this requirement so as to prevent regulatory arbitrage worldwide. The LEI, a global standard (ISO 17442), could be leveraged by all regulators across jurisdictions for uniquely identifying entities providing/involved in virtual asset services. If all regulators worldwide require an LEI for each licensed and registered VASP, (i) anonymity of these new players and the risks that they could pose could be eliminated; (ii) LEIs of VASPs could be used by regulators to facilitate communication with each other; which would ensure precision in the identification of the entity in question (iii) updates to both entity and relationship data of the VASPs could be tracked (e.g. headquarter address change) via the open, publicly available, personal-data-free Global LEI Repository.

Recently, the LEI was adopted as an optional field in inter-VASP Messaging Standard IVMS101. The interVASP messaging standard is intended for use in the exchange of required data between VASPs. This opens the door for leveraging the LEI to bring transparency and enhance consumer protection for crypto-assets and tokenization transactions.

For the time being, although VASPs operate on a global basis and it is a concern for 200+ jurisdictions, only approximately 30 national competent authorities publish data for VASPs. Some of these authorities publish the LEI of the VASP, but not all of them. Therefore, globally there is no way to determine if the same service provider is registered with many regulators, which leads to uncertainty for national authorities as well as all participants in the global financial system. If all jurisdictions identify registered VASPs via the LEI and exchange the LEI of VASPs among each other and supervisory authorities, a more precise risk aggregation could be achieved at the global level.