Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission's Targeted Consultation on the Review of the Regulation on Improving Securities Settlement in the European Union and on Central Securities Depositories (CSDs)

February 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the European Commission's Consultation's Targeted Consultation on the Review of the Regulation on Improving Securities Settlement in the European Union and on Central Securities Depositories (CSDs). GLEIF will focus its comments on how the use of the Legal Entity Identifier (LEI) can contribute to the full potential of these technological innovations with regard to the settlement of securities.

GLEIF would like to respond to the "*Question 19. Do you consider that the book-entry requirements under CSDR are compatible with crypto-assets that qualify as financial instruments*?".

According to CSDR, any issuer established in the EU that issues, or has issued, transferable securities which are admitted to trading or traded on trading venues, is required to arrange for such securities to be represented in book entry form. Any new security must be issued in book-entry form starting in January 2023, and all securities must be in book-entry form by January 2025.

According to Article 5 of the Commission Delegated Regulation (EU) 2018/1229 "*Account operators referred to in point (c) shall include entities that have a contractual relationship with a CSD and that operate securities accounts maintained by that CSD by means of recording book entries into those securities accounts*."

The CSD has a responsibility to verify that it has the correct credentials in place for issuers that wish to issue securities into its system. The CSD should verify that the LEI is for the correct entity, and that it is current (i.e. the status of the LEI shall be either "Issued", "Pending Transfer" or "Pending archival"). If the CSD finds out that the LEI status of an issuer is not current, it should put in place enforceable rules according to which appropriate validation should be carried out upstream by an issuer's agents, so that accurate up-to-date details are provided. This should apply in relation to all the information that issuers have to provide to CSDs under CSDR.

GLEIF would like to highlight that the LEI requirement is essential for both traditional financial instruments and crypto-asset issuers. Legal entities, such as the issuer of crypto-assets, the platform where the crypto-assets are distributed and/or transacted, and the provider of custody/safekeeping services should all be easily identified, as their traditional counterparties.

According to GLEIF's best knowledge, the CSDR explicitly avoids imposing one particular method for the initial book-entry recording. That being said, similar to traditional issuers, any crypto-asset issuer and crypto-asset service provider falling under the scope of the Commission's Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 shall be eligible for book-entry requirements under CSDR.

The Regulation (EU) 2019/1937 requires that crypto-asset service providers shall report their LEI before they apply for authorization as a crypto-asset service provider to the competent authority of the Member State where they have their registered office (Article 57). Additionally, the same Regulation requires that the ESMA register contains the LEI of the issuer of asset referenced tokens.

GLEIF also would like to provide its comments for the "*Question 20. Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment?".*

CSDR plays a pivotal role in the post-trade harmonization efforts in the EU, enhancing the legal and operational conditions in particular for cross-border settlement in the Union, while promoting cross-border competition within the single market. There have been diverging interpretations and application of the requirements related to cross-border activity.

GLEIF suggests that further clarity on the "*Rules on requirements for participation*" in a distributed ledger technology (DLT) environment would be useful. The fundamental concept of DLT is that it is a shared database which is accessible to multiple users or participants. One of the key characteristics is that the distributed ledger is maintained by its participants, and not by a central database administrator or party. Since these technologies aim to remove intermediary parties; who joins these permissioned networks is playing a significant role. Given crypto-assets operate cross-border, developing a prudential treatment will require global standards. The LEI, a global standard (ISO 17442), could be leveraged by all regulators, as well as participants in a crypto-asset transaction, across jurisdictions for uniquely identifying entities involved in creation of crypto-assets. In particular, parties involved in crypto-asset transactions could easily exchange information in a protected and private manner; but leverage the LEI to access the publicly available LEI data pool in order to identify precisely who is involved in a particular transaction when a transacting party is a legal entity.

For example, in this article published on Forbes, it is mentioned that moving settlement processes entirely to DLT enabled networks makes the settlement process more efficient since it decreases the associated transaction costs and reduces involved risks, including counterparty risk. However, in the same article it is also highlighted that counterparty risk does not become obsolete just by leveraging DLT networks. It is essential for policymakers to ensure that the participation requirements in these networks is precisely defined in order to reduce counterparty risk.

For the identification of senior managing officials and beneficial owners GLEIF would like to provide an update on its latest work in Verifiable Credentials (VCs). Thanks to advances in distributed ledger/blockchain technology, digital identity management with the additional feature of decentralized identity verification is now possible. Based on a concept known as Self Sovereign Identity (SSI), this new approach to authentication and verification of digital identity began as a means by which a person, the identity owner, has ownership of his/her personal data together with control over how, when, and to whom that data is revealed. In several proof of concepts (PoCs), GLEIF challenged SSI providers to extend the basic concept of 'individual wallets' and to create "organization wallets". In these wallets, the basis for identity is the organization's LEI, and the VCs issued to persons in their official roles within or in relation to the legal entity are tied to the organization and its LEI. Critical to this is the fact that the contents of the wallet credentials, in the form of a digital schema, can be designed by each organization to cover the particular identification and verification needs that the organization may have. The initial PoCs conducted by GLEIF simulated a regulatory filing. In this scenario, the SSI provider and GLEIF enabled a trust chain by connecting VCs anchored in the blockchain. The regulator was able to verify the

authenticity of the VCs of persons in official roles at the legal entity, the legal entity itself, the LEI Issuer, as well as GLEIF. Work recently has begun at ISO for identifying official organizational roles. This is planned to be used within these credentials to clearly state the roles of persons acting on behalf of legal entities.

Lastly, GLEIF would like to provide an update on its work regarding the standardization of messages among virtual asset service providers (VASPs). As already recognized in Regulation (EU) 2019/1937, the licensing and registration of VASPs is an essential step to curb anonymity and reduce money laundering risks. Furthermore, 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 the question of precisely what firms are engaging in these new markets and where. This makes analyzing risk at a global or regional level, which is necessary in order to reduce contagion, impossible. As noted in the European System Risk Board's recent LEI Recommendation (ESRB/2020/12): *In particular, the clear identification of contractual parties in a network of global financial contracts processed electronically at a very high speed permits authorities to make use of existing technologies to analyse interconnectedness, identify potential chains of contagion, and track market abuse for financial stability purposes. The LEI has also become critical for connecting existing datasets of granular information on entities from multiple sources.*

If all jurisdictions identify registered VASPs via the LEI and exchange the LEI of VASPs among supervisory authorities, a more precise and transparent financial ecosystem would emerge for virtual asset transactions.