Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Bank for International Settlements Basel Committee on Banking Supervision Consultative Document Introduction of Guidelines on Interaction and Cooperation Between Prudential and AML/CFT Supervision

February 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the to the Bank for International Settlements Basel Committee on Banking Supervision Consultative Document Introduction of Guidelines on Interaction and Cooperation Between Prudential and AML/CFT Supervision. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) in the consultation.

The ability of the world's financial ecosystem to curb fraud, terrorist financing and other illicit financial activity, is hindered by its reliance on outdated processes for identity verification. Financial institutions face the following fundamental challenge in identity management: low quality, non-uniform data sources are not easy to implement, prevent interoperability and promote inefficiency, which limits the capacity to add value to the surveillance process.

It is stated in the Consultative Document that international banking group structures and cross border activities pose an important money laundering (ML) and financing of terrorism (FT) risk factor. The ML/FT problem is global and require interaction and cooperation between prudential and anti-money laundering and countering financing of terrorism (AML/CFT) supervision not only in domestic but also in a cross-border context. GLEIF suggests that the Legal Entity Identifier, the global standard for unique identification and verification of legal entities, can be part of the solution by making sure that the information related to the bank and/or customers that is shared is correct and unambiguous. The Wolfsberg Group also underlined that it is important to know the branch information of a legal entity for further transparency and included the LEI in their Correspondent Banking Due Diligence Questionnaire. The LEI provides both the international branch and direct and ultimate parent information of a legal entity.

GLEIF's proposal is also consistent with the Bank of International Settlement Committee on Payments and Market Infrastructures' (CPMI) recommendation in the document "Correspondent Banking" published in July 2016. In addition to the general promotion of LEIs for legal entities, CPMI encouraged relevant stakeholders to consider promoting the use of the LEI for all banks involved in correspondent banking as a means of identification that should be provided in KYC utilities and information-sharing arrangements.

GLEIF would like to emphasize that providing more clarity about the type of data, such as a foundational required field for the LEI of the entity, be incorporated into the information exchange modalities can greatly help communication and coordination between supervisory authorities for identifying the right entity and reduce false positives.

The value of the LEI in combatting financial crime and enhancing AML framework has already been confirmed by several market participants and regulators. For example, the recent Payments Market Practice Group (PMPG) White Paper on Adoption of LEI in Payment Messages, underlines that Single Euro Payments Area (SEPA), Foreign Account Tax Compliance Act (FATCA), AML and sanctions regulations all require extensive data cleansing, data validation, conversion exercises and customer screening. Under Financial Action Task Force (FATF) standards, it is compulsory that payment messages identify the originator and beneficiary of cross border wire transfers. In the Global LEI System, the name and address are available in their original character sets in addition to transliterations in Latin Alphabet. This avoids inaccuracies and is value-add for customers in countries using non-Latin Alphabet. The LEI removes the ambiguity associated with names and helps avoids false positives in sanctions screening. With the current 1.5 million and continuously expanding LEI population, "white lists" of non-sanctioned legal entities can be created.

In a joint report published by the Asian Development Bank (ADB) and the United Nations Economic and Social Commission for Asia and Pacific (ESCAP), the LEI is highlighted among three initiatives to help bridge gaps in trade finance, as the LEI enables allows unique identification of large and small firms at low cost and helps to improve transparency on anti-money-laundering and know-your-customer concerns.

In the Financial Stability Board's Thematic Review on Implementation of the Legal Entity Identifier, it is stated that higher LEI coverage for all entities would support regulatory uses for AML/CFT, as well as other business and industry uses in know your customer (KYC) processes and the transfer of funds, especially across borders.

GLEIF also would like to highlight that the LEI is already being embedded into digital certificates, allowing it to be used for digital financial documentation. Within GLEIF's 2018 annual report, GLEIF's LEI is embedded within the digital certificates of GLEIF's signing executive officers. These certificates, for the first time, connect the role of the signatory to an organization through the LEI and can therefore be used to verify – automatically, through the shared LEI – that the filed document and the signatories represent the same organization. Incorporating a company's LEI within digital certificates of its executive officers used to sign financial statements provides reassurance on the data's reliability and that the information has not been tampered with, despite permitted access to the filed document via any public server globally. Deploying digital signatures, including that of the auditor, also enables efficient report production and distribution processes, the elimination of paper and increased certainty and trust.

The digital certificates of GLEIF's signing executive officers included with its 2018 annual report are compliant with the European Union's Electronic Identification and Trust Services (eIDAS) Regulation. The European Telecommunications Standards Institute (ETSI) published the technical standards for the inclusion of LEIs in eIDAS certificates and seals in August 2019. To achieve this, GLEIF applied for Object Identifiers (OIDs) for the LEI and the role of the person acting on behalf of the legal entity so that these could be embedded in digital certificates. GLEIF also has contributed to the working group of the International Organization for Standardization (ISO) currently revising the ISO 17442 LEI standard to include details in this standard on how to embed LEIs and roles in digital certificates.

As demonstrated in the FATF's recent Draft Guidance on Digital Identity, identification goes digital worldwide and this direction brings new ML/FT challenges. Refinitiv, a global provider of financial markets data and infrastructure, highlighted in an article that with a move towards a more digital

economy and with the EU's 5th AML Directive, mandating the globally recognized Legal Entity Identifier (LEI) in the EU would be welcome.

GLEIF has conducted further research on the use of LEIs for digital transactions focusing on the use of the LEI in digital verifiable credentials (DVCs) which can be secured cryptographically and contribute to overall cybersecurity. Decentralized identity management systems offer an alternative to centralized identity management. Such systems run using distributed ledger technology. Entities represent themselves via digital verifiable credentials. Such credentials allow for real time access to services or applications. DVCs are interoperable, cryptographically-verifiable and facilitated by distributed ledger or blockchain technology. By leveraging the LEI within digital verifiable credentials, counterparties can more easily accomplish the tasks of identity verification, authentication, and authorization and digitally identify persons able to act officially on behalf of a legal entity.

The LEI is a quality-controlled unique identifier supported by a transparent infrastructure of local identity validation and a centralized open data challenge service. The LEI also acts as an identification key between databases/platforms. Use of the LEI requires no special access arrangements to use the LEI data and no concern to expose any confidential information.