Response of the Global Legal Entity Identifier Foundation (GLEIF) to to the European Banking Authority Consultation Paper Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37

July 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the European Banking Authority Consultation Paper on the Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37.

GLEIF will focus on the use of the Legal Entity Identifier (LEI) in the consultation.

First, GLEIF would like to respond to the Question 2 and make a comment on the added Guideline *1.14: Firms should ensure that their business-wide risk assessment is tailored to their business profile and takes into account the factors and risks specific to the firm's business, whether the firm draws up its own business-wide risk assessment or contracts an external party to draw up its business-wide risk assessment. Similarly, where a firm is part of a group that draws up a group-wide risk assessment, the firm should consider whether the group-wide risk assessment is sufficiently granular and specific to reflect the firm's business and the risks to which it is exposed as a result of the group's links to countries and geographical areas, and complement the group-wide risk assessment if necessary. If the group is headquartered in a country associated with a high level of corruption, then the firm should reflect this in its risk assessment even if the group-wide risk assessment stays silent on this point*.

The Report The Report submitted by the EU Commission to the European Parliament confirms that recent money laundering cases in the European Union involved banking activities undertaken in different parts of a group structure, through branches established in different Member States or third countries, or through subsidiaries located in Member States different than the headquarters. Group structures often complicate customer due diligence and risk analysis. A starting point to reduce the complexity is to ensure that financial institutions effectively identify their customers during the due diligence phase so as to enable group-wide risk assessment. The Legal Entity Identifier (LEI - ISO 17446) is the only global standard for legal entity identification. GLEIF suggests that the LEI should be a foundational step in all customer due diligence processes to ensure that the financial institution has clearly identified the customer and its parent relationships. This would greatly improve communication within the financial institution regarding transactions involving entities in group structures and with

regulatory authorities receiving reporting on such transactions (e.g. suspicious transaction reports). GLEIF would like to share a financial institution's LEI record (https://search.gleif.org/#/record/6SHGI4ZSSLCXXQSBB395) and a corporate entity's LEI record (https://search.gleif.org/#/record/KY37LUS27QQX7BB93L28) as examples of displaying the subsidiary information across different jurisdictions in the Global LEI Repository in a standardized way.

The EBA added Guidelines 4.9 to 4.11 that set out the importance of financial inclusion and that financial institutions should balance the need for financial inclusion to mitigate ML/TF risks. Specifically, it is mentioned in the Guideline 4.10 (a) that "*Where a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation, firms should consider mitigating ML/TF risk in other ways, including by adjusting the level and intensity of monitoring in a way that is commensurate to the ML/TF risk associated with the customer, including the risk that a customer who may have provided a weaker form of identity documentation may not be who they claim to be*…"

In some developing countries, local systems for entity identification are not easily accessible, may not be transparent, and sometimes lack quality standards. In countries who lack transparency and identity, more than 50% of economic activity is conducted by unregistered businesses and as a result firms remain cut off from essential services such as payments, credit facilities, and supply chains.

This is where the Global LEI System can play an important role in enabling these enterprises access to a trusted identity that is recognized universally and provides transparency across the global marketplace. GLEIF's discussions with financial institutions show that some financial institutions already use the Global LEI Repository as the first step for creating the profile of a legal entity. However, EBA's explicit recommendation to the financial institutions that the Global LEI System should be used as the first step in identity verification and validation of legal entities as a trusted source would help financial institutions to standardize their data around the LEI. The standardization of legal entity data internally and improving data management capabilities in financial institutions serves to establish a robust frontier against money laundering and terrorism financing attempts.

Guidelines 4.12 to 4.25 clarify the CDD expectations regarding the beneficial owners, in particular the use of beneficial ownership registers, new developments on how to identify the customer's senior managing officials, or the beneficial owner of a public administration or a state-owned enterprise.

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 on an international standard for identifying official organizational roles, that is planned to be used within these credentials to clearly state the roles of persons acting on behalf of legal entities, is under development at the International Standardization Organization (ISO).

GLEIF would like to comment on the newly added guidelines 8.20 to 8.25 specific to correspondent banking relationships.

For a correspondent bank, establishing the identity of the respondent bank is a fundamental area of due diligence. As suggested in the report of the International Finance Corporation (IFC) of the World Bank, encouraging emerging market banking customers to obtain LEIs, where appropriate, would further support banks' capacity for CDD and AML/CFT. Therefore, the EBA could consider encouraging correspondent banks to consistently leverage the LEI for respondent bank identification to enhance its CDD and AML/CFT capacities.

Lastly, GLEIF thinks that EBA's prescriptive approach in the guidelines for each relevant sector helps financial institutions to determine whether a situation presents a high or a low ML/TF risk, and which type of CDD (simplified or enhanced) might be appropriate to manage that risk. Regardless of the type of CDD performed, the EBA could consider recommending financial institutions to obtain an LEI for each legal entity client. This would result in the following benefits for financial institutions and regulatory authorities:

Broader adoption of the LEI in the financial sector can help overcome cross-border challenges associated with reconciling names and addresses – for example abbreviations of common terms, differences in translations, and the provision of transliteration for in non-Latin character sets. Parsing text is inefficient and causes confusion within a financial institution and in its communications with regulatory authorities. In some countries, it is possible that several entities/persons may have exactly the same names which make it challenging to identify the particular payer and payee without additional information. Today, name-matching techniques for AML screening work either through deterministic or probabilistic matching technology. For instance, a matching relationship between two records is only direct or deterministic when a customer name exactly matches with the name in the sanction list(s). However, the existence of more than one "John Brown" or "John Trading Inc" causes a tremendous number of false positives for financial institutions. In reality, matching software may report possible matches when customer information is the same or similar to the watch list entity information. In order to reduce false positives for legal entity clients, a consistent, quality controlled, and open means of identifying the client is needed. The LEI is fit for this purpose.

Financial institutions can increase the efficiency of compliance checks processing through the LEI in an automated way:

- identity-based compliance made possible by LEI adoption increases the effectiveness of financial institutions screening thereby facilitating better, more robust compliance checks.
- inclusion of the LEI in payment messages facilitates more automated AML, CTF and sanctions screening processes. This also facilitates the reporting of suspicious transactions to Financial Intelligence Units.

- facilitating information sharing in a standard format in correspondent banking; so as to reduce the risk and cost associated with due diligence process.