Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission Public Consultation on Guidance on the Rules Applicable to the Use of Public-Private Partnerships in the Framework of Preventing and Fighting Money Laundering and Terrorist Financing

October 2021

GLEIF is pleased to provide comments to the European Commission Public Consultation on Guidance on the Rules Applicable to the Use of Public-Private Partnerships in the Framework of Preventing and Fighting Money Laundering and Terrorist Financing.

GLEIF would like to respond to Question 1. "*In which ways do you consider that the exchange of information between competent authorities and private sector entities can contribute to the prevention of and fight against money laundering and the financing of terrorism?*".

The flow of intelligence information is crucial between all involved parties in the fight against financial crime - supervisory authorities, financial institutions, and law enforcement bodies. However, there is a general frustration that intelligence sharing does not function well both at the domestic level and across borders. Intelligence sharing regarding the entity/individual is at the core of the public-private partnership. If the intelligence flow from a financial institution to supervisory authorities included the LEI as a global identifier for the legal entity, all parties would have a clear understanding of the entity's identity in question. Today identity is largely based on name matching, which is highly imprecise and prone to false positives. Making the LEI part of cross-border intelligence sharing mechanisms would bring maximum transparency to the global community. The LEI would enhance law enforcement agencies' and supervisory authorities' ability to aggregate data across financial institutions.

The LEI, a globally accepted open standard for unique and unambiguous identification of legal entities, is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). The code connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions including their ownership structure. Use of the LEI consistently can ensure an accurate and unique identification of all legal entities. Besides, the LEI data provides entity reference data in the native local language of the entity and in the transliterated version (as applicable). This enables users to understand the language used to represent the entity and also have a roman character representation of the name. And the GLEIF API is a globally accepted protocol for accessing identity information for legal entities in a digital and machine-readable fashion.

With the addition of the LEI to the flow of information between the financial institution and supervisory authorities, all parties would benefit from the wealth of information that accompanies the LEI. This includes the transliterated name of a legal entity and the legal name in the official language (this functionality is particularly important for legal entity names in Arabic, Russian, Chinese, Greek, etc.) and information on the direct and ultimate accounting consolidation parents.

Tagging all relevant entities with their LEI in Suspicion Activity Reports (SARs) is particularly important for automation and data efficiency in SARs processing. The leaked FinCEN papers revealed the inherent problems regarding SARs. According to media coverage, FinCEN received 2 million SARs in 2020. This is an extraordinary volume of data meaning FinCEN must rely on automated processing if it desires to identify initial trends and highlight outliers. Adding the LEI instead of or in addition to the entity name would improve the SARs processing by reducing time wasted, eliminating incorrect identification using name matching and focusing the involved parties on value-added tasks of aggregating and analyzing transactions.

Imagine the LEI is added to a SAR subsequently when the user selects "legal entity" as the Main Subject. Adding the LEI would make "Legal entity name", "country of registration", "house number", "street", "city/town", "country", "postcode" and other address details unnecessary. The LEI reference data already includes the legal entity name, business registry ID of the entity and the ISO compliant address field. Connecting to the powerful and free-to-use GLEIF API could even return entities where there is a match against a former name. This is a powerful tool for increasing transparency for the National Competent Authority.

This idea can be extrapolated to any supervisory authority involved in receiving SARs reports. Not only would the supervisory authority render its own work more efficiently, it could also share feedback with financial institutions and enable financial institutions to create better, data-driven risk profiles of their clients.

GLEIF would like to comment on the Question 3. "*In your view, what does a 'public-private partnership' mean in the context of preventing and fighting against money laundering and the financing of terrorism?*".

Both the private and public sectors benefit from a safe and transparent financial system with measures in place to curb the bad actors. In order to develop this ecosystem, compliance needs to be a proactive rather than a defensive "box-checking" exercises. However, compliance comes with costs and over the past decade the regulatory burden on financial institutions has accelerated dramatically. Fragmentation of the KYC landscape globally adds up cost and burden for financial institutions. Different financial institutions may hold information on the same customer, which may overlap, but which may also be inconsistent and incomplete, a weakness that criminals can navigate and exploit. If the LEI was used to tag all financial institutions' legal entity clients, then all financial institutions and supervisory agencies would speak the same language. For example, if an entity is identified as associated with politically exposed persons, the data vendors providing monitoring products for customer due diligence would flag the associated LEI record and the information would flow seamlessly to financial institutions and from financial institutions to the supervisory agencies.

The value of the LEI in AML is already recognized by the European Commission. In the recent anti-money laundering and countering the financing of terrorism legislative package of the European Commission, it is stated in Article 18 that "*Identification and verification of the customer's identity - the LEI is required, where available, for the identification of a legal entity; for a trustee of an express trust or a person holding an equivalent position in a similar legal arrangement and for other organizations that have legal capacity under national law*".

GLEIF suggests that the identification of the legal entity customer via the LEI be required. This would significantly enable an ecosystem for communicating information between involved parties, thereby supporting public private partnership efforts to build up a broader risk management approach and away from an event-driven system.

GLEIF would like to respond to Question 11. "*In your opinion, what should be the main objectives of a public private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism?*".

GLEIF suggest that "*improve the quality of suspicious transaction and activity reporting by obliged entities*" and "*Preparation of risk indicators and red flags in order to improve the detection by private sector entities of suspicious financial flows*" are the primary objectives of a public private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism.

As highlighted in GLEIF's response to Question 1, tagging all relevant entities with their LEI in SARs is particularly important for automation and data efficiency in SARs processing. Data consistency is key to increasing efficiency and reducing the time and costs of data processing. Use of the LEI more broadly would help achieve this. Cleaning and reconciling identity data is one of the most significant inefficiencies in AML/ CFT data processing across both public and private sector. The LEI offers an independent, robust standard to ensure data insights can be more readily attributed to entities, avoiding much of the current re-checking and discovery processes. Linking national standards to a global LEI will allow more efficient and consistent data sharing across boundaries. A global approach to entity identification is a key element of ensuring more effective AML processes.

The Guiding principles for screening ISO 20022 payments report highlights that unstructured data is a barrier to building effective transaction screening and monitoring tools that mitigate sanction and AML risks. As the payments industry prepares to adopt ISO 20022, banks are revisiting their screening environments to identify the impact of this move and opportunities for change. BIC and LEI codes of Entities published on sanctions lists are listed as the relevant information that should be screened against. The targeted screening approach allows financial institutions to avoid false positives linked to mismatches between information types (e.g. debtor name hitting against vessel names, street name information hitting against embargo data). Unlike other identifiers, BICs and LEIs are global in nature which make them particularly effective to identify sanctioned entities or discard potential hits.

Another report published by the Payment Market Practice Group, Global adoption of the LEI (Legal Entity Identifier) in ISO 20022 Payment Messages – 2021, suggests that the LEI can be used in the sanctions screening space with even more potential improvements once the regulators come on board and add the LEI into the sanctions screening lists.

Additionally, in the Cross Border Payments Survey Report published by the Financial Action Task Force (FATF), many respondents asked for increasing uniformity in the list entries and greater use of structured identifiers such as Legal Entity Identifiers (LEIs). Respondents also indicated that using the LEI to identify the beneficiary and originator in payment messages would support widespread interoperability between systems and reduce costs and increase precision and transparency.

All these examples and recent reports show the value of using standardized data and structured identifiers in public private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism.

Lastly, GLEIF would like to respond to Question 14. "*In your opinion, in relation to the application of which rules is the issuing of guidance with respect to public-private partnerships for the exchange of strategic information most needed?*".

GLEIF suggests that provision of feedback on suspicious transaction reports by the FIU to the obliged entity is quite important with respect to public-private partnerships for the exchange of strategic information. The flow of information and processing data should be two-way. Financial institutions spend considerable time and money to file these suspicion transaction reports and these reports are one of the main tools of compliance regimes. However, regulators rarely provide feedback to banks on how they use these reports, or whether the information is useful.

There are problems of data volume and the manual processing of SARs in supervisory agencies which either reduce effectiveness, raise costs, or both.

The better, clearer, and standardized requirements that promote good practices will help fight crime and improve the system. GLEIF suggests that a consistent and standardized application of the LEI and reflection of LEIs in suspicion activity reports would reduce the regulatory burden on obliged entities and simultaneously enhance information gathering and sharing practices between supervisory authorities and other relevant institutions. The supervisory agencies would be able to process data in a more efficient way and provide feedback to the financial institutions accordingly.