

## **Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission on its Roadmap titled Towards a New Comprehensive Approach to Preventing and Combating Money Laundering and Terrorism Financing**

**March 2020**

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the European Commission on its Roadmap titled Towards a New Comprehensive Approach to Preventing and Combating Money Laundering and Terrorism Financing. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) in the Roadmap.

The LEI is a 20-character, alphanumeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). The LEI connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure, answering the questions of 'who is who' and 'who owns whom'. It provides a universally recognized identifier paired with essential entity data, rigorous verification processes and high data quality.

The LEI initiative is driven by the Financial Stability Board (FSB) on behalf of the finance ministers and governors of central banks represented in the Group of Twenty (G20). In 2011, the G20 called on the FSB to take the lead in developing recommendations for a global LEI and a supporting governance structure. The related FSB recommendations endorsed by the G20 in 2012 led to the development of the Global LEI System as a broad public good that provides unique identification of legal entities participating in financial transactions across the globe and the subsequent establishment of the GLEIF by the FSB in 2014. As outlined in the GLEIF's Statutes, the Global LEI System is designed and developed to be used by the (i) public authorities and (ii) by the private sector to support improved risk management, increased operational efficiency, more accurate calculation of exposures and other needs. The GLEIF, a supra-national not-for-profit organization, is overseen by a committee of currently 71 global regulators and 18 observers, known as the LEI Regulatory Oversight Committee (LEI ROC). The European Supervisory Agencies (ESAs), ESMA, EBA and EIOPA, as well as the ECB and the European Commission, are represented in the LEI ROC.

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 put in place effective surveillance processes.

It is stated in the July 2019 [Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions](#) that in some instances, it appears that the parent company had difficulties in forming an accurate and complete overview of the existing risks in the group. Some of the cases involved banking activities undertaken in different parts of a group, through branches established in different Member States or third countries,

or through subsidiaries located in Member States other than where the headquarters are established. The Report confirms that supervision of such entities is also rather fragmented and inefficient. Information sharing within the EU and with third countries are uneven and often established on an ad hoc basis without a consistent and standardized approach.

GLEIF therefore argues that mandating the use of the LEI under the EU's AML framework could prove beneficial to protect the EU internal market from criminals attempting to launder money and finance terrorism for the following reasons:

**(1) Strengthen entity identification and verification processes in the EU financial ecosystem:** One of the biggest challenges confronting the world's financial ecosystem is how to complete its transformation to a fully digital environment. Success here will be determined, in part, by the new digital system's ability to identify participants in financial markets and track, predict and mitigate criminal activity. GLEIF proposes that the target model needed to capture and articulate the spirit of digitally-enabled financial regulation must have at its core strong legal entity identification. Specifically, the financial ecosystem should enable that all endpoints are identified and verified at the point of transaction, and privacy and security benefit the entire community.

GLEIF proposes that improving Customer Due Diligence (CDD) processes and results for legal entity clients starts with the mandated use of the LEI, a global standard to uniquely identify legal entity clients. This would enable a financial ecosystem based on strong identity and verification processes rather than estimation and human intervention.

Here is an example:

- To combat fraud and other illicit transactions, publicly available sanctions and watch lists are maintained by a variety of supervisory authorities around the world. These lists typically comprise the names of persons and legal entities whose transactions are deemed to warrant further investigation. Financial institutions responsible for enabling financial flows must ensure compliance with these lists by checking, sometimes manually, that the names published do not correspond with the names displayed on the transactions they perform with clients. Even though 'natural persons' typically represent two thirds of the entries on sanctions and watch lists, a high proportion of financial crimes involve the use of a company name. This is why identification of the legal entities that appear on these lists is so crucial to successfully curbing financial crime.

Currently, the compliance process requires financial institutions to match names only; it does not require the identities of the transacting parties to be confirmed, limiting its effectiveness. Additionally, in a global economy names exist in multiple character sets whereas most watch lists, and the financial system in general, works with basic Latin characters. The transformation of names between different character sets further adds to the ambiguity. Given that the current processes are also both expensive and inefficient, a significant opportunity exists to replace the name-based system with one based on identity, thereby making it faster, more effective and less expensive to administer for all stakeholders.

Furthermore, several international institutions have identified the LEI as an important tool in combatting criminal activity. For example, the International Finance Corporation (IFC) of the World Bank's publication, ['Navigating Essential Anti-Money Laundering and Combating the Financing of Terrorism'](#)

[Requirements in Trade Finance: A Guide for Respondent Banks](#) identifies the LEI as one of the emerging innovations for efficiency and effectiveness of a bank's efforts in AML/CFT compliance. Further, to bring transparency on entities and their transactions, the LEI is being recommended for conducting due diligence on borrowers, on-boarding clients in securities and fixed-income markets and for verifying buyers and sellers in cross-border trade in the [T20 Argentina Report, 'A global framework for tracing Beneficial Ownership.'](#)

Another area where the LEI can have substantial contribution in tackling against fraud and strengthening risk management is the customs. As the e-Customs environment in the EU continues to develop and assumes greater complexity, tackling against fraud becomes more challenging. Given the importance of improving data for collaborative risk management is required not only within the EU but also across borders, incorporation of the LEI, along with the EIORI number, for shipper, consignee, notify party in the Entry Summary Declaration (ENS) would be beneficial.

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 to the Latin Alphabet. This avoids inaccuracies and is value-add for customers in countries using non-Latin characters. The LEI removes the ambiguity associated with names and helps avoid 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.

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.

Additionally, the 5<sup>th</sup> AML Directive sets out a series of requirements for Member States and their obliged entities as part of the "Chapter 6: Enhanced Due Diligence" (EDD). GLEIF would like to emphasize that customer LEI would also be useful as part of EDD if the customer is a legal entity in designated high-risk countries. Currently, the Global LEI System covers more than 200 countries, which means coverage already exists for legal entities to apply for an LEI in high-risk countries and coverage in additional jurisdictions could be added.

**(2) Futureproof AML/CFT efforts vis-à-vis digital revolution:** Reliable, independent, digital ID systems are a necessary foundation for Customer Due Diligence (CDD) functions. In our interconnected world, information overload risks eroding trust, so stakeholders must work harder than ever to mitigate doubt when verifying each other's identity. One piece of this information overload is the plethora of identifiers applied to legal entities engaged in financial transactions.

As regards creating trust and transparency across EU financial markets, some market observers have suggested that rules, regulations and supervisory institutions cause more problems than they solve and

that ‘technology will soon make them redundant’. At the same time, these critical voices also frequently fear that financial regulation may hinder innovation; a showstopper for the digital economy: *“The main drag on implementing innovation in financial services is regulation.”* (CoinDesk).

In our view, regulation, however, is the representation of shared ethical norms that underpin trust: *“Trust is the expectation that arises within a community of regular, honest, and collaborative behavior, based on commonly shared norms, on the part of other members of that community... Communities depend on mutual trust and the shared ethical norms that underlie it. Trust is not reducible to information.”* (Trust, *The Social Virtues and the Creation of Prosperity*, Francis Fukuyama).

Technology itself does not define ethical norms, however. It is purely the means through which shared norms can be expressed and enforced. In this way technology can’t make rules, regulations and institutions redundant, it can only facilitate or hinder them.

To this end, GLEIF suggests the Commission should examine its CDD requirements in light of emerging technology solutions for CDD processes. One such area is decentralized identity management systems. 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. Typical roles include corporate officers, corporate insiders, board members, shareholders and beneficiary owners. GLEIF would be pleased to demonstrate, along with its EU partners such as the Banque de France, the results of its DVC proof of concepts.

Within the eIDAS Regulation the LEI is already accepted as an optional attribute for legal entities’ data sets in transactions between eIDAS nodes, i.e. interfaces between national eID infrastructures. The LEI can be used within eIDAS-compliant digital certificates as the eIDAS Regulation includes a tag (ETSI technical standard available) for digital identification tools such as the LEI to be embedded within certificates and seals to support identity validation and management.

Within [GLEIF’s 2018 annual report](#), GLEIF’s LEI is embedded within the digital certificates of GLEIF’s signing executive officers, which are compliant with the eIDAS Regulation. 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 regardless of the access point to the document. 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.

Lastly, it is interesting to note that some prominent data vendors, such as Refinitiv, support mandated use of the LEI in the Europe. The LEI can be used within eIDAS-compliant digital certificates as the eIDAS Regulation includes a tag (ETSI technical standard available) for digital identification tools such as the LEI to be embedded within certificates and seals to support identity validation and management. As a global

identifier, the LEI can serve as a bridge between EU Member States connecting their national eID schemes, and therefore facilitating cross-border identification processes within the EU and with third party states. Following analogy might help to understand better the difference between the LEI and the eID. The LEI is the passport of a legal entity, whereas the eID is the national electronic identifier. Similar to information contained in a passport, the LEI contains the national ID, registration authority, jurisdiction of formation of a legal entity. Therefore, the LEI system provides a harmonized, standardized, global and open representation of identity.

**(3) Enable Faster, better and more cost-effective compliance:** Today, banks spend around EUR 35 billion on client onboarding annually, presenting a clear opportunity for increasing efficiency and reducing costs. By widely adopting the LEI, banks could unlock an estimated EUR 1.75-3.5 billion per annum by improving full time employee (FTE) productivity in client onboarding alone to focus on the fight against financial crime.

Systems are now in place across the financial sector to catch financial crime however it is estimated that only 1% of the total of financial crime proceeds is caught. One of the main reasons cited is the lack of efficiency of the current system notably due to the very large number of reports. Among these reports, there are a number of false positives which could be avoided by having a common standard in place.

The LEI, supported by G20, is a global standard for uniquely identifying legal entities and already anchored into several EU regulatory requirements such as EMIR, MIFID II, MAR, CRR, Solvency II, AIFMD, CRAR, CSDR, Transparency Directive and Securitization Regulation. The LEI is linked to a legal identity and issued by a GLEIF accredited organization. Such organizations are almost in all EU27 Member States accredited.

This means that when it is used in financial flows, compliance verification can be based on actual identities instead of just names. In reference to sanctions and watch lists, this means that transacting parties can be unambiguously identified, greatly reducing the number of false positives that the matching process generates today. By connecting multiple information sources at the European level and globally through the consistent use of a global entity identification standard, it would be possible to create large knowledge bases that can better support automated transaction surveillance.

GLEIF believes that this is also consistent with the [EU Commission's final report of the Expert Group on Regulatory Obstacles to Financial Innovation: 30 recommendations on regulation, innovation and finance](#). Below recommendations are particularly relevant for leveraging the LEI as a mandatory data element for identifying all legal entities in the EU and thereby increase supervisory efficiencies:

- The Commission, in co-operation with the ESAs and the ESCB, should facilitate initiatives that **promote standardization of legal terminology and digital standards-based common classifications** of actors, services, products and processes in the financial sector (*Recommendation 10*).
- The Commission recommended **full harmonization of AMLD identification & verification KYC processes** – notably for mandatory collected datasets (*Recommendation 15-17*).
- The Commission, in consultation with the EBA and relevant authorities, should investigate potential models (including decentralized models) for efficient, robust and **trusted digital identity verification** (*Recommendation 19*).

Lastly, GLEIF would like to highlight that 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.