

## Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Financial Crimes Enforcement Network (FinCEN), Treasury, on Anti-Money Laundering Program Effectiveness Advance Notice of Proposed Rulemaking (ANPRM)

### November 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the Financial Crimes Enforcement Network (FinCEN), Department of Treasury, on questions pertaining to potential regulatory amendments under the Bank Secrecy Act (BSA).

GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) as a response to the Question 3. *“Are the changes to the AML regulations under consideration in the [Advance Notice of Proposed Rulemaking \(ANPRM\)](#) an appropriate mechanism to achieve the objective of increasing the effectiveness of AML programs? If not, what different or additional mechanisms should FinCEN consider?”*.

First some background on the LEI.

The development of a system to uniquely identify legal entities globally had its beginnings in the 2008 financial crisis. Regulators worldwide acknowledged their inability to identify parties to transactions across markets, products, and regions for regulatory reporting and supervision. This hindered the ability to evaluate systemic and emerging risk, to identify trends, and to take corrective steps. Recognizing this gap, authorities, working with the private sector, have developed the Global LEI System with a global governance framework representing the public interest that will, through the issuance of unique LEIs, unambiguously identify legal entities engaged in financial transactions. Although the initial introduction of the LEI was for financial regulatory purposes, the usefulness of the LEI can be leveraged for any purpose. The LEI is use case agnostic and can be used in any process of entity identification, from finance to healthcare to verifying all counterparties of businesses supply chain.

The LEI is the only global standard for legal entity identification. It is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It 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 and thus answers the questions of ‘who is who’ and ‘who owns whom’. Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace.

The drivers of the LEI initiative, i.e. the Group of 20, the Financial Stability Board and many regulators around the world, have emphasized the need to make the LEI a broad public good. As such, the LEI and its associated reference data are accessible to all as open, public data. It is registered and regularly verified according to protocols and procedures established by the LEI Regulatory Oversight Committee.

The value proposition of LEI has already been recognized by several U.S. regulators such as the Federal Reserve, Consumer Financial Protection Bureau, Municipal Securities Rulemaking Board, National Association of Insurance Commissioners, U.S. Treasury, which utilize the LEI. U.S. Customs and Border Protection is working on the Global Business Identifier (GBI) Initiative, in which the Bureau will test the LEI as part of an evaluative proof of concept to determine the optimal GBI solution.

### **Potential use of the LEI in Suspicious Activity Reports (SARs) and information sharing**

An effective anti-money laundering (AML) programs is key in tackling money laundering and illicit finance flows. A consistent, high quality, and globally recognized identifier for clients is absolutely essential to AML programs in today's digital world. The LEI is the essential building block for legal entity "client identification" in AML programs. GLEIF suggests the LEI should be required for all SARs reports and its use should be encouraged for all industries that have AML program requirements under FinCEN's regulations. Regarding the receipt and processing of SARs, the inclusion of the LEI would streamline report processing and analysis. The inclusion of the LEI would guarantee a unique and unambiguous identifier is associated with the entity. This identifier also links to the direct and ultimate parents of the legal entity. FinCEN could avoid name matching and the associated manual reconciliations of client identity and instead focus on the substantive details of the report. This would dramatically improve monitoring and record keeping for SARs and more broadly in FinCEN's own database of tracking legal entities. Data lineage is a key component to tracking entities over time. As such, the LEI could be used as the primary entity identifier for tracking legal entities reported to FinCEN thus creating an historical record of repeated entities over time. The LEI could also be used to track all reports from each reporting financial institution (FI) historically. Aggregation of reported content could be achieved by associating the LEI of the entity to the LEI of the reporting FI.

FinCEN could go even further in their classification schemes of high-risk legal entities. For example, FinCEN could set guidelines based on the corroboration status of the LEI (the ability to corroborate the LEI reference data with a local authoritative source like a business registry), the last refresh of the LEI data, or the status of parent data reporting associated with the LEI. FinCEN could leverage the open LEI data as the authoritative source for legal entity identity as intended by the founders of the system – the leaders of the G20 and the Financial Stability Board.

FIs have already begun utilizing the LEI within client onboarding, Know Your Customer (KYC) and customer due diligence processes. Today, FIs require LEIs for the identification of counterparties and trading partners, based on certain regulatory mandates, in both the initial on-boarding of a new entity record or through periodic refreshes of existing entities. However, most of the times, the LEI is collected at the end of the onboarding process for fulfilling the regulatory requirements. With its new [Validation Agent operating model](#), GLEIF encourages financial institutions to issue LEIs for their clients in cooperation with accredited LEI Issuer Organizations by leveraging their business as usual client identification procedures in KYC and client onboarding processes. This model, triggering LEI growth beyond regulatory mandates, would help to make the financial ecosystem more transparent and accessible for all parties.

Collection and use of the LEI in a consistent and standardized way would help FIs to streamline their internal data management processes and comply with regulatory requirements that require collection of the LEI. Furthermore, there exists more than 115 regulations globally that mandate the use of the LEI, most of which is required for financial reporting purposes. Point being, the LEI is no stranger to the financial marketplace and is a logical tool for FinCEN as well. In a recent [report](#) published by the Bank of International Settlements, the Global LEI Repository is mentioned as a "non-documentary verification" source under the "Verification of identity of legal persons". The LEI was also added under the "potential additional information" column, next to "at a minimum" (basic requirements), and in the footnote, it is

stated that subject to developments in the LEI project, this information may become required in the future.

Furthermore, inclusion of the LEI by FinCEN 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. 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 “Main Street Trading Inc” causes a tremendous number of false positives. 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.

Another area that the LEI can help to streamline is information sharing. Information sharing across US law enforcement organizations as well as other nations’ intelligence agencies is critical for ongoing surveillance. The LEI is an ISO (International Organization for Standardization) standard as well as an adopted U.S. standard. The Global LEI System meets all the requirements for international and national information sharing:

1. Identifier is based on an international open global standard
2. Identifier is truly globally unique
3. System produces open data
4. Data model and data quality measures are open and clear
5. System is governed by public entities and is not subject to private sector dominance

Even within the US, the LEI could enable better information sharing across different government entities. Today, the US government utilizes more than 50 different identifiers for legal entity identification<sup>1</sup>; which causes manual reconciliation of data and drain of resources. Instead of using/accepting a plethora of identifiers, FinCEN could leverage the LEI, as an established open source, to harmonize and sharing of critical data both at home and abroad. The current use of multiple identification schemes hampers both national and global interoperability and increases opportunities for illicit behavior to occur. Given, one of the recommendations in the ANPRM is to leverage existing information sharing initiatives between the public and private sectors and sharing with foreign affiliates and global institutions, leveraging the LEI, a global identifier, in information sharing could create a common language between different parties regardless of where they are located and increase the efficiency, speed and transparency of existing information sharing mechanisms.

### **European and global support for the LEI in AML and payments landscapes**

In the European Union, the European Commission considers making the LEI a required data element in client identification its upcoming AML Rulebook. The European Systemic Risk Board (ESRB) in its recently published [Recommendation](#) highlighted that clear identification of the legal entities and the connections between them with the LEI is a key requirement for drawing a reliable map of the global economic and

---

<sup>1</sup> See Envisioning Comprehensive Entity Identification for the U.S. Federal Government, <https://www.gleif.org/en/lei-solutions/regulatory-use-of-the-lei/gleif-and-data-foundation-comprehensive-entity-id-for-u-s-federal-government>

financial landscape and called for action all relevant parties to close the LEI gap in the EU. Specifically, it recommends the introduction of a Union framework on the use of the LEI by June 2023.

As already highlighted in the [Financial Stability Board's Enhancing Cross-border Payments Stage 1 report to the G20](#), greater use of the Legal Entity Identifier (LEI) for firms in cross border payment arrangements can reduce unnecessary barriers to cross-border data sharing when implementing the Financial Action Task Force (FATF) standards and other regulatory and supervisory requirements. The use of the LEI consistently as a common data standard would ensure interoperability among different payment system operators or providers regardless of their jurisdiction. Payment is the last step of B2B transactions. Therefore, ensuring quality control in counterparty verification and validation by using the LEI in previous steps such as the selection of providers, agreeing on a contract, confirming orders, and agreeing on delivery ensures that payment is made from a legitimate business to a legitimate counterparty.

In the [Stage 2 Report published by the FSB](#), the LEI is suggested as a unique identifier for precisely identifying the beneficiary and originator in payment messages. As part of the "Focus area D: Increase data quality and straight-through processing by enhancing data and market practices", the Report highlighted that poor data quality and limited standardization of data exchange make cross-border payments more complex to process, in turn affecting their speed, price and transparency. Promoting the adoption of common message formats directly mitigates the friction around fragmented and truncated data.

As set out in building block 14, adopting common message formats can play an important role in interlinking payment systems and addressing data quality and quantity restrictions in cross-border payments. It can also enhance automated straight-through processing functionalities, supporting quicker and more efficient payments. Standardization of the payer, payee, payment service providers, and other actors in the payment network with the LEI can bring efficiencies in other building blocks, such as building block 8: Information sharing and know your customer efficiencies.

And in the [recently published Stage 3 Report](#), the FSB provided indicative timelines for achieving the previous reports' objectives. Starting from June 2021, the FSB will explore options to improve adoption of the LEI with GLEIF, LEI Regulatory Oversight Committee, and national authorities. Beginning in October 2020, FSB, in Consultation with Committee on Payments and Market Infrastructure, International Monetary Fund, World Bank, GLEIF, ISO and other stakeholders, will explore the scope for, and obstacles to develop, a global digital Unique Identifier for cross-border payments, and potentially other financial transactions, that takes into account existing identifiers, including the LEI for legal entities and identifiers for natural persons.

Wider usage of the LEI in cross border payments and other areas could help to fulfill AML Expert Working Group's recommendation that the AML monitoring and reporting practices be modernized and streamlined to maximize efficiency, quality, and speed of providing data to government authorities with due consideration for privacy and data security. The LEI data is publicly available and therefore does not come up with any data privacy issues.

### **The role of the LEI in new technologies**

For the identification of senior managing officials and beneficial owners, as it relates to Customer Due

Diligence Rules for Financial Institutions (CDD Rule), 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.

The LEI also has been adopted in messaging pertaining to AML. Regarding new potential money laundering threats along with technological innovation, GLEIF would like to provide an update on its cooperation and collaboration with relevant parties in identification of virtual assets service providers (VASPs). 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.

Lastly, GLEIF would like to reiterate that the Global LEI Repository is a source of truth and validation for more than 1.7 million entities. Every LEI is validated by Local Operating Units (LOUs), issuers of LEIs, that have been approved through a formal accreditation process. GLEIF offers a free API service that permits users to validate the LEI and data that is a part of an LEI record, such as address or legal name. FinCEN, following a possible mandate of the LEI, could leverage the API to validate entities and supplement data coverage of entities.