

Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Securities and Exchange Commission (SEC) Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security

November 2020

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the Securities and Exchange Commission (SEC) on proposed amendments pertaining to the National Market plan governing the Consolidated Audit Trail (CAT) to enhance data security. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI).

First, GLEIF would like to respond to Question 64. *“The proposed amendments define “Customer and Account Attributes” as meaning the data elements in Account Attributes and Customer Attributes. Do commenters believe these definitions should be modified to add or delete data elements? If so, what elements?”*

GLEIF supports the Commission’s proposal to clarify that the Industry Member will report “Employer Identification Number (“EIN”) **and** LEI, instead of the current wording EIN/LEI. Further, GLEIF also suggests that the SEC makes the LEI a mandatory data field for all legal entities instead of allowing *“other comparable common entity identifier, if applicable.”*

Adding the LEI as a mandatory data field would enable regulators to access and extract legal entity information for both domestic and foreign legal entities from CAT Data in a seamless and unambiguous way in order to achieve specific regulatory purposes.

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) and an adopted U.S. standard. It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. LEI data records also contain information about an entity’s ownership structure and thus answers the questions of ‘who is who’ and ‘who owns whom’. Further, usage of the LEI could eliminate the need to collect Name and Address for each legal entity, as this reference data also is part of the LEI data records. Reliance on the LEI as a structured code that points to legal entity reference data could substantially improve the data quality of the data collection for CAT. 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. The Global LEI System is overseen by the LEI Regulatory Oversight Committee which includes the Federal Deposit Insurance Corporation (FDIC), Federal Reserve, Department of Treasury, Office of the Comptroller of the Currency, Securities and Exchange Commission, and Consumer Financial Protection Bureau. Mr. Alan Deaton of the FDIC is currently vice-chair of the Regulatory Oversight Committee.

The LEI currently exists in 26 various U.S. laws and regulations. The LEI value proposition has already been recognized outside the financial industry by the U.S. Government with the Global Business Identifier Initiative. As part of this initiative The U.S. Customs and Border Protection and partner government agencies will test the LEI as part of an evaluative proof of concept to determine the optimal GBI solution.

Consistent use of the LEI in the US would greatly enhance information sharing across different government entities. Today, the US government utilizes [more than 50 different identifiers](#) for legal entity identification; which causes manual reconciliation of data and drain of resources. Instead of using/accepting a plethora of identifiers, the SEC could leverage the LEI, as an established open source, to harmonize and sharing of critical data both at home and abroad. The OPEN Data Act seeks to synchronize data across various agencies, inclusive of regulators. Consultations and amendments to existing requirements, like CAT, are an opportunity to re-consider existing identifier schemes with a long-term vision for broader use across US agencies.

The LEI is an open standard and therefore has no restrictions on use or redistribution. All LEI and associated LEI data can be found on GLEIF's public website and is made available to the public under a Creative Commons (CC0) license. As such, there should be reduced concerns about data security when using the LEI.

More importantly, by making the LEI a mandatory input the SEC would result in a more efficient system. The EIN was specifically built for tax reporting purposes and lacks certain features that make it more broadly applicable as an ID. Specifically, it was created for IRS use and, despite uptake among several other agencies, it is not consistently used across agencies and there is no way to clearly apply it outside of government. This means CAT data cannot be combined with additional financial reference data products to enable easy monitoring. Additionally, all users of CAT data would benefit from one standard being used for legal entity identification for domestic and foreign entities. The SEC would also benefit from data that accompanies a LEI record. For example, legal name and address, both of which are collected within CAT reporting today can be automatically retrieved from the LEI record. All LEI data is validated and verified by LEI issuers against authoritative sources which results in a trusted source of data. There are more than 1.7 million LEI's assigned globally.

GLEIF is aware of the cost concerns of the Commission and would like to provide an update on its work with financial institutions for reducing the cost of the LEI and shifting the responsibility of obtaining and maintaining an LEI from registrants to financial institutions, to the benefit of both parties. Under the [Validation Agent framework](#), GLEIF pilots the applicability of financial institutions issuing an LEI for each onboarded client through partnering with accredited LEI Issuing Organizations for a reduced LEI fee.

The Validation Agent Framework empowers banks to leverage their KYC, AML and other regulated business-as-usual onboarding processes, to obtain an LEI for their customers during initial onboarding or a standard client refresh update. In other words, banks acting as Validation Agents can liaise with the LEI Issuer on its client's behalf to 'validate' key identity data, such as the legal name and business registry information, confirming that these checks and processes have already been performed. GLEIF recently [announced](#) that the J.P. Morgan, one of the largest global banks of the United States, has become the first Validation Agent in the Global LEI System.

GLEIF also would like to provide its comments for Question 65. *The proposed amendments define the “CAIS” as the Customer and Account Information System within the CAT System that collects and links Customer-IDs to Customer and Account Attributes and other identifiers for queries by Regulatory Staff. Are there other data elements that should be included in CAIS, and if so, what are they and why would it be appropriate to include them? How would adding these data elements to the CAIS impact regulatory value? Please explain.*

According to GLEIF’s understanding, the Commission suggests the creation of a Customer-ID that uniquely identifies each Customer and would track orders from, or allocations to, any Customer or group of Customers over time via this Customer ID. For legal entities, the Commission suggests that the EIN is submitted to the CAT Customer ID (CCID) Transformation Logic for creating the unique Customer-ID.

Although GLEIF understands that the Commission’s proposal to create unique Customer-IDs could have some merits for natural persons with confidential data, this approach should be different for legal entities.

Given the LEI itself is a unique, global identifier which unambiguously identifies legal entities and the LEI is already proposed as one of the data elements under the definition of “Customer Attributes”, along with an EIN, to identify a customer, GLEIF believes the Commission’s proposal to introduce another internal unique identifier into the system is unnecessary.

Introducing new identifiers for legal entities creates additional reconciliation difficulties for users of the data. These reconciliation tasks would be avoided if a single and standardized approach based on a single unique identifier were instead adopted by the SEC. Therefore, GLEIF suggests that the Commission revisits this proposal and use the LEI as the unique Customer-ID for legal entities, instead of creating a new one.

Lastly, GLEIF would like to comment on the Question 93. *The existing CAT NMS Plan requires that the Chief Regulatory Officer or another such designated officer or employee at each Participant must at least annually review and certify that people with PII access have the appropriate level of access in light of their respective roles. The proposed amendments state that the review and certification must be made by the Chief Regulatory Officer or similarly designated head(s) of regulation, or his or her designee, at each Participant, and that the Chief Regulatory Officer or similarly designated head(s) of regulation, or his or her designee must, at least annually, review the list of people who have access to Customer Identifying Systems at their organization, the role of each person on the list and the level of access of each person. Based on that review, the Chief Regulatory Office must certify that people with Customer Identifying Systems access have the appropriate level of access for their role, in accordance with the Customer Identifying Systems Workflow. Is it appropriate to continue to facilitate oversight regarding who has access to the Customer Identifying Systems by applying these requirements to the Customer Identifying Systems Workflow? Why or why not? Please explain with specificity why such provisions should or should not apply.*

GLEIF agrees that who will access to Customer Identifying Systems at their organization is crucial.

First, GLEIF would like to provide an update on its work in digital certificates area. International Standardization Organization revised the ISO 17442 standard to define how LEIs are technically integrated within different types of digital certificates in a standard way. The qualified digital certificate by itself **guarantees the identity of the signer** and its signature guarantees document integrity and frames it into a precise timing, using qualified time stamps in combination. Therefore, by adding LEIs into digital certificates, these are included in the document signature process, which brings an additional trust proof, as the LEI is a globally secure mechanism that provides reliable data for company identity. Through LEI embedded digital certificates, legal entities can perform various corporate digital transactions, such as submitting e-invoicing, ordering goods and services, contracting with suppliers, or reporting tax statements to public authorities with an extra layer of trust. This company's data check can be automated, consistently regardless of the country where the company is allocated, in the same way, certificate validation is done. The result is a reliable and robust validation of the company's data and people's identity acting on behalf of the company.

Regarding cybersecurity, the use of the LEI allows for a persistent and reliable identification code to be present throughout successively issued digital certificates, thus enhancing trust in internet transactions and providing reliable and trustworthy information on the ownership and authenticity of electronic documents and, thereby transactions. Therefore, including the LEI within digital certificates establishes a verified link with the physical identity of a company thereby reducing cybersecurity threats.

As an example, GLEIF has published its [annual report](#) of 2019 in human and machine-readable Inline XBRL and HTML format, with its LEI embedded within both the annual report and the digital certificates of GLEIF's signing executive officers. This was delivered in partnership with XBRL International and Workiva, and in cooperation with the European Securities and Markets Authority (ESMA). GLEIF showcased how the LEIs should be included within digital, machine-readable financial documentation on the basis of [ESMA's European Single Electronic Form \(ESEF\) mandate](#), to enhance trust and ease data aggregation, and demonstrates how simple it is to incorporate the LEI into electronic signatures as an additional best practice.

For the identification of senior managing officials and their link with their organization, GLEIF also would like to provide an update on its latest work in Verifiable Credentials (VCs). 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 with GLEIF as the root of trust for the LEI. 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 ISO.

GLEIF would be pleased to further engage with the Commission on this topic and provide further information, if requested.