# Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Berlin Group's Open Finance API Framework Implementation Guidelines for Extended Services Push Account Information Services

November 2021

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to comment on the Berlin Group's Open Finance API Framework Implementation Guidelines for Extended Services Push Account Information Services. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) in "*Push Account Information Message Flows*" and "*Transactions*" in the consultation. GLEIF suggests that the technical standardization of the payer and beneficiary information with the LEI for Third Party Providers (TPPs) and corporates in the openFinance API will enable interoperability, thereby reduce data reconciliation costs, time, and uncertainties for all involved parties.

GLEIF understands that with the new *Push Account Information Service*, ASPSPs will be able to inform PSUs via API Client systems about account information into the openFinance API Framework. GLEIF welcomes direct access for Corporates when the API Client is a direct corporate customer of the ASPSP and potentially gets Account Information directly pushed to the API Client's IT systems via this service. GLEIF suggests that unique and standardized identification of all parties involved via the LEI can enhance interoperability, usability and consistency of the openFinance API framework, which has paramount importance for all users in this network.

Specifically, under "Section 6 Push Account Information", GLEIF suggests that the "creditorLEI" and "debtorLEI" for business clients are added in the push account entries request, in addition to the already existing "creditorName" and "debtorName". The LEI enables precise identification of the creditor and debtor. This is an additional layer of security and also enables numerous downstream business processes (see Global adoption of the LEI (Legal Entity Identifier) in ISO 20022 Payment Messages – 2021 which provides examples of how the LEI can be used in sanctions screening, reducing fraud for Corporate Treasurers, account to account owner validation and also improvements across the industry for Know your Customer (KYC) processes). Moreover, since the LEI is machine-readable, its use will enable automatic account aggregation. GLEIF would like to remind that the Global LEI System is free to use, open, and easily accessible database that all parties would be able to connect with 24/7 operating hours. The System is overseen by the Regulatory Oversight Committee, a group of more than 65 financial markets regulators and other public authorities. The LEI connects to key reference data that provides the information on a legal entity identifiable with an LEI: the official name of the legal entity as recorded in the official registers, the registered address of that legal entity, the jurisdiction of formation. The Global LEI System links with the local business registries that might be proprietary and in different character sets. Instead of navigating through various access points and languages, the Global LEI System allows any party to a transaction to conduct quick due diligence in a trusted way.

Similarly, under "7.10 Transactions", GLEIF suggests that the LEI is adopted to uniquely identify creditor, debtor, ultimate creditor, and ultimate debtor, respectively. In the current public consultation, GLEIF understands that the text field (with a maximum of 70 characters) is allowed to identify all these parties, which would cause manual intervention for data reconciliation and hinder straight through processing.

 

Recently, SWIFT published its **Guiding principles for screening ISO 20022 payments**. The report highlights that unstructured data is a barrier to building effective transaction screening and monitoring tools that mitigate sanctions and AML risks. As the payments industry prepares to adopt ISO 20022, banks are revisiting their screening environments. The report advises that BIC and LEI codes of Entities published on sanctions lists are listed as the relevant information 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). SWIFT's Guidelines have been endorsed by the Wolfsberg Group, who develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

 