Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission Public Consultation VAT in the Digital Age

May 2022

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the European Commission Public Consultation VAT in the Digital Age. GLEIF will concentrate its comments on the use of the Legal Entity Identifier (LEI), a machine-readable, global standard for unique and unambiguous entity identification that can be leveraged in digital reporting /e-invoicing requirements. GLEIF will clarify how the addition of the LEI in VAT reporting obligations can help to reduce fragmentation in digital reporting and unnecessary costs for EU companies operating across borders.

GLEIF would like to respond to the Question: "*Would you like to add any comments or suggestions on reporting / e-invoicing requirements*?".

First, GLEIF would like to provide some background on the LEI.

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. GLEIF was established by the FSB in 2014 to support the implementation and use of the LEI. 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. GLEIF, a supra-national not-for-profit organization, is overseen by more than 65 public authorities and 19 observers participating in the Regulatory Oversight Committee (ROC). The European Supervisory Agencies (ESAs), ESMA, EBA and EIOPA, as well as the ECB and the European Commission, are represented in the ROC. In total there are more than 20 member states or EU organizations represented in the ROC.

The LEI is already required extensively in financial markets regulation in the EU. All EU corporates listed and traded at any marketplace already have an LEI due to the Regulation (EU) 2017/1129 (Prospectus Regulation). Moreover, many other large corporates or financial institutions have already obtained an LEI due to different EU regulatory requirements such as EMIR, MIFID II, MAR, CRR, Solvency II, AIFMD, CRAR, CSDR, Transparency Directive, Securitization Regulation and the proposed AML Regulation and Transfer of Funds Regulation (recast 2015).

GLEIF suggests that the mandatory inclusion of the LEI in digital reporting requirements, including e-Invoicing and EC sales listing (ESL) can substantially reduce fragmentary implementation across various Members States, reporting and compliance costs for EU businesses and fraud attempts.

For example, the ESL provides details of sales or transfers of goods and services to other VAT registered companies in other EU countries. GLEIF suggests that if the legal entity customer information reported in the ESL were based on the LEI, instead of the customer's name, data aggregation, verification and reporting would be easier, precise, and more transparent. It would also provide the foundation needed to evolve ESL to a digitally enabled reporting environment.

GLEIF also understands that with the introduction of its Central Electronic System of Payment information (CESOP), the EU Commission aims to combat cross-border VAT fraud caused by the fraudulent behavior of some businesses in the area of cross-border e-commerce. For fulfilling this aim, it is essential that the payment service providers uniquely identify the payee and the payer with a global identifier. It is stated in the Council Directive (EU) 2020/284 that a payment service provider holds specific information to identify the recipient, or payee, of the payment together with details of the date, the amount and the Member State of origin of the payment as well as of whether the payment was initiated at the physical premises of the merchant. That specific information is particularly important in the context of a cross-border payment where the payer is located in one Member State and the payee is located in another Member State, in a third territory or in a third country. Such information is necessary for the tax authorities of the Member States (the 'tax authorities') to carry out their basic tasks of detecting fraudulent businesses and controlling VAT liabilities. It is therefore necessary that payment service providers make that information available to the tax authorities to help them detect and combat cross-border VAT fraud.

For payment service providers to report this information into national tax authorities, they first would need to uniquely identify the merchant and the location information of the legal entity. Given cross-border e-commerce goes beyond the borders of the European Union, any identification solution should be global in nature. Therefore, GLEIF suggests the EU Commission explicitly require payment service providers to report the LEI of the payee and payer in all payment transactions where a legal entity is an originator and/or beneficiary. The LEI is an international standard that connects to key reference information that enables clear and unique identification of legal entities including their status as active and operating,

headquarters/legal address and ownership structure. The complete database of LEIs and the associated LEI reference data is available free of any charge or barrier to anyone on the web. GLEIF operates under the Open Data Charter terms, which means the data can be used by all users without limitations.

Cnsistent and mandatory use of the LEI in e-invoices and payments lifecycle would provide verified, authoritative information about the entities involved in payment transactions and guarantee security. The LEI is included on the EU Electronic Address Scheme (EAS) code list meaning the LEI can be used in EU eInvoicing.

GLEIF would like to share a real-life example provided by one of its partner firms. This particular EU based firm received an invoice for services provided. The invoice included the name of the firm providing the services, the expected address, the VAT number and the agreed upon amount. The invoice passed the internal review and payment was executed. A month later, the firm received a phone call from the supplier notifying that the payment was past due. To its surprise the firm learned the original invoice had been intercepted and a fraudulent account had taken the place of the account of the supplier. The firm then had to pay the invoice a second time – a considerable loss for an SME. Our partner firm pointed out that if the invoice had contained the LEI plus the account information then the fraudulent payment would never have been made. Instead, the reliance on manual verification and proprietary data, such as the account number, did not allow for an appropriate review. Should the invoice have had the LEI, the VAT and the account number, the bank could have leveraged the open public LEI data to confirm the identity of the recipient of the payment by cross referencing the LEI of the service provider and the account number on the invoice before proceeding with the payment. The sending bank would not have executed the payment unless the two pieces of information were confirmed.

The Payment Market Practice Group's (PMPG) recent publication on the use of the LEI in ISO20022 Payment messages confirms corporate invoice reconciliation as one of the use cases. The PMPG highlights that use of eInvoices (e.g., in UBL format) signed with debtor's LEI embedded digital certificates enables data to be automatically parsed and match the person authorizing the payment with the entity. The Debtor can verify the supplier by a single call using the supplier's LEI and verify the supplier's identity via the GLEIF API within milliseconds. The Debtor can then decide if verified to proceed with the payment order and if not to stop the payment order. If the LEI is included in the payment order from vendor to the bank and bank checks the IBAN and LEI, the fraud can be totally avoided. The net result would be ensuring full automation, trust, authenticity, and reliability of documents. It would also improve the ability to flag possible fraud attempts by ensuring full transparency of parties to the transaction from start to end.

The European Systemic Risk Board (ESRB) recommends the use of the LEI in fighting VAT evasion in e-commerce. The ESRB highlights that while the LEI would only be the first step in this regard, it would be a necessary one in order for further progress to be made. Furthermore,

in addition to the identification of individual entities, the intragroup relationships present in the LEI database could make it possible to track parents and subsidiaries located in offshore centres. The location and legal form of these related entities could help tax authorities to identify possible tax evasion cases.

Therefore, GLEIF suggests the Commission be more prescriptive in setting requirements for digital reporting and eInvoice templates. If the Commission requires that all companies add/require the counterparty LEI (where the counterparty is a legal entity) in their eInvoicing and digital reporting templates (e.g., ESL), the data collection capabilities would increase substantially at the EU company-level. Once the data collection enabling digital reporting and data analysis is achieved, Member States collectively would have the opportunity to close the loopholes that fraudsters exploit today.