Response of the Global Legal Entity Identifier Foundation (GLEIF) to the European Commission's Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)

November 2021

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the European Commission for the "Proposal for preventing money laundering and terrorist financing – traceability of crypto-asset transfers."

First, GLEIF applauds the Commission for creating a harmonized rule-setting across the internal market to prevent fragmentation in the AML/CFT regimes. It is essential to set granular and standardized requirements across the Union, as demonstrated by the Commission's proposal for customer due diligence in the new AML Regulation, to adequately protect the internal market and reduce additional costs and burdens for operators providing cross-border services.

GLEIF agrees that the transfer of virtual assets, which have remained outside of the scope of Union legislation on financial services until now, poses money laundering and financing of terrorism risks. The flows of illicit money can be done through transfers of crypto-assets; hence it could damage the integrity, stability, and reputation of the financial sector and threaten the internal market of the Union. Therefore, GLEIF welcomes the inclusion of crypto-assets and crypto-asset service providers under the proposed recast of Regulation (EU) 2015/847.

However, GLEIF suggests that the applicability of the LEI should be extended to the originator and beneficiary of the crypto-asset transfer when these parties are legal entities. Article 14 "*Information accompanying transfers of crypto-assets*" of the proposed recast of Regulation (EU) 2015/847 states that "*The crypto-asset service provider of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the originator:*
(a) the name of the originator;
(b) the account number of the originator, where an account is used to process the transaction;
(c) the originator's address, official personal document number, customer identification number or date and place of birth.
2. The crypto-asset service provider of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the beneficiary:
(a) the name of the beneficiary;
(b) the beneficiary's account number, where such an account exists and is used to process the transaction."

The Regulation (EU) 2019/1937 requires that crypto-asset service providers shall report their LEI before they apply for authorization as a crypto-asset service provider to the competent authority of the Member State where they have their registered office (Article 57). Additionally, the same Regulation requires that the ESMA register contains the LEI of the issuer of asset referenced tokens.

Extending the LEI requirement to the originator and beneficiary in the crypto-asset transfer would enable traceability and transparency of the parties. The LEI, a global standard, could be leveraged by all

regulators, as well as participants in a crypto-asset transaction, across jurisdictions for uniquely identifying entities involved in creation of crypto-assets. In particular, parties involved in crypto-asset transactions could easily exchange information in a protected and private manner; but leverage the LEI to access the publicly available LEI data pool in order to identify precisely who is involved in a particular transaction when a transacting party is a legal entity.

The LEI is a more comprehensive due diligence tool than static name and address information collection. As the financial industry moves to digitalized processes and machine-readable formats, the need for international data standards and structured data formats for identifying parties is increasing. Without the LEI, originator/beneficiary information will remain siloed publications with very limited ability to communicate across FIUs within the Union and across borders. They also perpetuate the shortfalls of the existing financial ecosystem, such as lack of interoperability, the minimal ability for financial markets participants and authorities to communicate with each other, and reliance on non-standardized, non-digital formats. These are the exact shortfalls that criminals exploit in today's financial markets to carry out illicit transactions.

GLEIF welcomes the inclusion of the LEI for payer and payee under Article 4 "*Information accompanying transfers of funds*" where provided by the payer to the payer's payment service provider for transfers of funds or transfer of crypto-assets from the Union to outside the Union as part of the complete information on the payer and the payee. First, GLEIF suggests that Article 4 could also make reference to the originator and beneficiary in the case of transfer of crypto-assets. Second GLEIF suggests the Commission extend the LEI requirement to include transfers from third countries to the EU (two-way traffic). This will enhance EU authorities and EU based financial institutions ability to combat money laundering or terrorist financing sourcing from third countries by enabling precise identification of the legal entities involved in fund transfers into the EU. The consistent use of the LEI for the beneficiary and originator would better enable tracing of the source of funds.

The European Systemic Risk Board (ESRB) recognized the value of the LEI in fighting against money laundering in its recent report. The ESRB highlighted that "the extensive use of the LEI could also make anti-money laundering measures work more effectively, for instance by helping to identify (chains of) legal entities involved in financial transactions (payments). The detection and analysis of certain patterns (with the help of algorithms and artificial intelligence) would enable signs of potential money laundering to be flagged. Similarly, it could contribute to fighting VAT evasion in e-commerce. 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. **The LEI could also be required in information accompanying transfers of funds for the purpose of fighting money laundering and combating terrorist financing**, e.g. in the case of international wire transfer messages."

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 that should be screened against. This 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.