Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Payments Systems Regulator Authorized Push Payment Scams Consultation Paper

January 2022

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the UK Payments Systems Regulator (PSR) Authorized Push Payment (APP) Scams Consultation Paper. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) in the consultation and would like to respond to Question 17: "*Do you agree with our position on improving intelligence against fraud? We welcome any further comments from stakeholders about this work.*".

GLEIF agrees that taking measures to prevent APP scams are of great importance. As highlighted in the consultation paper, reported losses from APP scams have risen rapidly, particularly in parallel to the growth in online banking or payment platforms. A recent UK Finance report confirms that 70% of APP scams originated via an online platform.

The PSR highlights in the consultation paper that there is evidence that Confirmation of Payee (CoP), has helped prevent some types of APP scams. However, CoP has its shortcomings - specifically the reliance on name-checking rather than a precise digital identifier. Although all three measures suggested in the Consultation Paper are significant to bring transparency to the PSP market, still the foundational question - how to prevent fraudsters and APP scams from the very beginning - is yet to be responded.

GLEIF suggests that particularly for Consumer-to-Business (C2B), Business-to-Business (B2B), Consumer-to-Government (C2G), or Government-to-Business (G2B) transactions, the LEI can be leveraged to set the first foundational step for a transparent payment chain. If all parties in the payment chain verify the LEI of the recipient business/government entity, the receiving PSP would have complete transparency before allocating funds. A recent Payment Market Practice Group (PMPG) report explains how the LEI can help enable more transparent, efficient and secure payments. In particular the use case on corporate invoice reconciliation and fraud detection are relevant.

Scenario 1- - Fraud detection and fight against vendor scams just in 4 steps

- **Step#1**. The supplier generates a machine-readable document (according to the format expected by the vendor's Enterprise Resource Program (ERP)) containing the bank account number for payments. The supplier signs the document by using a digital certificate with its LEI embedded.
- **Step#2.** The vendor received the document from the supplier. The vendor's ERP parses the document, extracting the certificate information, including the LEI code and IBAN.

- **Step#3.** The vendor's ERP using extracted LEI code checks (using GLEIF's API) that this LEI matches with the supplier's LEI. Suppose the LEI code matches the provider's data. In that case, the supplier's bank account number is considered correct as it is contained in a digitally signed document, and it is added to the ERP's valid records for further payments.
- **Step#4**. When Bank receives the payment order, it checks if the IBAN of the supplier matches with its LEI. If yes, it continues with the allocation of funds; if not, it creates a red flag in the system that it can be fraudulent.

All these four steps above can be performed in an automated fashion and without any manual intervention.

Additionally, the PMPG paper highlights that matching a name of a client to an account on an incoming payment or as part of CoP is an imprecise exercise as there are so many permutations for how a name can be written. The CoP matching criteria must allow for a certain level of mismatch meaning the validation between the name and account number can take longer than necessary and often require manual intervention. If LEI is provided, then this is an exact identifier that can provide a 100% match and validation in milliseconds. This can also reduce fraudulent payments or money laundering by ensuring that the credited account matches the LEI provided for the creditor.

Imagine the following C2B scenario. Jane Smith, a UK citizen, initiates a payment from Bank A to pay Amazon Services Europe S.à r.l. (LEI 549300OW58AHTDBJQX90) in Bank B. Amazon Services Europe S.à r.l is based in Luxembourg. If Bank A asks the LEI of the creditor from Jane Smith within the payment instruction, there would be no doubt or ambiguity that the funds would not be transferred to another company with the name "Amazon" (E.g., another Luxembourg based Amazon Oil Ventures S.à r.l. (LEI 549300QJIT3TQ2HS2I38)) but to the e-commerce platform provider Amazon for Jane's purchases. Moreover, Jane can easily verify the LEI and associated reference data of Services Europe S.à r.l. via the open, publicly available GLEIF API.

GLEIF suggests that adding the LEI, a machine-readable globally recognized common data standard, as a mandatory data field in payment transactions can prevent APP scams and fraudulent transactions. Another PMPG paper published and then endorsed by the Wolfsberg Group states that with large market infrastructures migrating to the ISO 20022 messaging standard starting from 2022, it is time for all financial institutions to revisit their risk screening. 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). Therefore, GLEIF proposes that when financial institutions add the LEI of the client and link it with the client's IBAN in their databases, they can use this combination of information for multiple purposes, from sanctions screening to the prevention of APP scams.

The LEI reference data does not contain any personal information and can be easily shared among PSPs for transaction risk information sharing.

The LEI has already been incorporated to several Pay.UK and Bank of England proposals in payments. The Pay.UK Standards Authority made the LEI one of the pillars of the data enhancement building blocks in its New Payments Architecture. The Bank of England, with its transition to the CHAPS, required the LEI for all financial institutions by 2024 with a possibility to extend this requirement for all legal entities, depending on the growth of the Global LEI System. Therefore, GLEIF invites the PSR to consider the LEI as a foundational standard to be implemented to prevent APP scams in parallel to other existing payments initiatives in the UK.

Payments are global in nature and hence need global standards. Only global standards such as the LEI can respond to the challenges in cross-border payments. Therefore, the Financial Stability Board (FSB), in its Stage 2 Report, suggested the LEI as the 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. And in its concluding Stage 3 report of the FSB the LEI features prominently as part of the solution for making cross-border payments cheaper, more accessible, and transparent for all parties.

Lastly, GLEIF suggests the addition of the LEI in the CoP as an extension of the service. The account name and type (consumer/business) are currently used as the match criteria. Given that some business names might be similar to each other (as our example above with "Amazon"), a manual reconciliation is often still required because the account name might not match the entity's legal name (although it is the correct entity). What if a global unique identifier, the LEI, were used instead of imprecise name matching? Since an entity can only have 1 LEI, even if the entity has a similar name with 100 other entities, its LEI can give the exact result without any doubt. Precision in CoP service should be considered as one of the main objectives for a faster payments environment. As the precision level increases, the number of APP scams will drop significantly.