



Enabling global identity
Protecting digital trust

Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Australian Treasury’s consultation on Scams Prevention Framework – exposure draft legislation

October 4th, 2024

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide feedback to the Australian Treasury’s consultation on the effectiveness of the exposure draft of the Scams Prevention Framework (SPF). GLEIF welcomes the opportunity to comment on the Framework and will focus its comments on how incorporating the Legal Entity Identifier (LEI) into the Framework can help effectively combat scam in the Australian economy, in alignment with the Framework’s guiding principles.

GLEIF fully supports the Australian Treasury’s initiative to introduce the SPF as part of a broader effort to modernise Australia’s legislative landscape for the digital age, including updates to privacy, anti-money-laundering and cybersecurity laws, as well as payment system reforms. GLEIF would like to highlight the significant role the ISO 17442 [Legal Entity Identifier](#) (LEI) could play in supporting these efforts.

In particular, GLEIF would like to propose that the LEI be incorporated in the SPF to ensure the effective and unique identification of service providers to combat scams across multiple sectors in the economy, such as telecommunications, banks, digital platform services.

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). It connects to key reference information that enables clear and unique identification of legal entities participating primarily in financial transactions and answers the questions of ‘who is who’ and ‘who owns whom’. Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace.

As such, the LEI would bring direct benefits in terms of the machine-readability, interoperability, and usability of the collected data to help all entities within the scope of the SPF (‘regulated entities’) to address the scams risk and residual risk, in alignment with the SPF principle of ‘governance’.

When service providers, are defined and tracked using different identifiers, it becomes exceedingly challenging for consumers or regulators to track services, detect the volume of scams or address emerging scam threats. Using the globally recognized LEI for all service provider license schemes or registers would reduce fragmentation and enhance consumer protection by providing global transparency on the involved service providers and their corporate hierarchies. Additionally, such an approach would strengthen the service provider ecosystem by leveraging the LEI for key functions, such as verification of payee, sanctions screening and payment processing, while streamlining monitoring and investigation processes to more efficiently ‘prevent’ and ‘detect’ scams.

In addition, GLEIF would like to highlight to the Australian Treasury the key role the LEI can play in enhancing customer-due-diligence (CDD) and know-your-customer (KYC) procedures, particularly in the identification of counterparties during fund transfers and onboarding legal entities, thereby aiding in the improvement of the anti-money laundering practices.

Such considerations are reflected in the most recent (2023) draft revisions to the Financial Action Task Force's (FATF) Recommendation 161 of the 'Travel Rule', which propose that for both originators and beneficiaries 'information accompanying all qualifying payments or value transfers should always contain [...] their Business Information Code (BIC), Legal Entity Identifier (LEI), or the unique official identifier of the originator/beneficiary.' Furthermore, the proposed revisions suggest that beneficiary financial institution should check that the beneficiary information in the payment messages aligns with the information held by the beneficiary financial institution. This represents a significant opportunity to introduce the LEI, a precise and digital identifier for the beneficiary, to streamline the beneficiary bank confirmation process.

Also, the LEI is recognized in the BIS' Committee on Payments and Market Infrastructures (CPMI) '[Harmonized ISO 20022 data requirements for enhancing cross-border payments](#)' as an equivalent identifier to the Business Identifier Code (BIC) for identifying financial institutions and legal entities within a payment message in cross-border payments. This publication is in line with Wolfsberg Group's updated [Payment Transparency Standards](#).

At an EU level, the new AML Regulation (AMLR), which is part of the recently finalized AML package², references the LEI as part of the identity and verification of customers and beneficial owners for legal persons. Additionally, as part of the EU AML package, the EU Transfer of Funds Rule (TFR) was recast to ensure that transfers are accompanied by various data points on the originator and beneficiary (for non-individuals)³. Lastly, the regulation on instant credit transfers in Euros enables PSPs to allow users to use the LEI for the verification of payee⁴.

Additionally, the Bank of England published its 'Policy Statement: Implementing ISO 20022 Enhanced Data in CHAPS' which confirmed the introduction of the LEI into the CHAPS payment message standard when migrating to ISO 20022.⁵

¹ FATF, 2023, Public Consultation on Recommendation 16 on Payment Transparency, available at:

<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html>

² https://www.europarl.europa.eu/doceo/document/A-9-2023-0151-AM-329-329_EN.pdf

³ European Council, Digital finance: Council adopts new rules on markets in crypto-assets (MiCA), available at:

<https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/>

⁴ REGULATION (EU) 2024/886 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202400886

⁵ Bank of England, 2023, Policy Statement: Implementing ISO 20022 Enhanced Data in CHAPS, available at:

<https://www.bankofengland.co.uk/-/media/boe/files/payments/rtgs-renewal-programme/iso-20022/policy-statement-implementing-iso-20022-enhanced-data-in-chaps-january-2022.pdf>

Further, the Reserve Bank of India (RBI) issued a mandate for the LEI in all payment transactions totalling ₹ 50 crore and more undertaken by entities for Real-Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT). From October 2022, this requirement was extended to cross-border capital or current account transactions.⁶

Last but not least, in Australia, commencing on 21 October 2024, the [ASIC Derivative Transaction Rules \(Reporting\) 2024](#) will repeal and replace the current 2022 rules to align with international reporting standards. The updated rules aim to consolidate transitional provisions and exemptions while ensuring that reporting requirements are fit for purpose. Under these rules, the use of the LEI will become mandatory, replacing AVID or BIC codes. Reporting entities, counterparties, central counterparties, brokers, and other relevant entities will be required to use the LEI for identification purposes.

The Australian Treasury is also actively combating SMS scams through the implementation of a new **SMS Sender ID Registry**. Here are the key strategies and initiatives involved:

1. **Sender ID Registry:** The government has launched a pilot program for the SMS Sender ID Registry, which requires organizations that send SMS messages using alphanumeric sender IDs to register their IDs. This registry helps prevent scammers from using fraudulent sender IDs to impersonate legitimate brands, such as banks and government agencies.
2. **Blocking Suspicious Messages:** Participating telecommunications companies are mandated to block any SMS messages that use non-registered sender IDs or do not match the approved numbers in the registry. This measure aims to protect consumers from being scammed by ensuring that only verified entities can send messages under specific brand names

For foreign legal entities providing services to domestic consumers or business, Australia Treasury can consider asking them to register their IDs with SMS Sender ID Registry using local business registry or LEI.

GLEIF also suggests that the Australian Treasury explore implementing solutions for digital organizational identity, such as the verifiable LEI (vLEI), the LEI's digital counterpart, to support its efforts in preventing and detecting scam. The vLEI is a digitally signed credential that allows an LEI to be instantly and securely verified when presented in digital form. This enables digital interactions using the vLEI to maintain a high level of assurance about the identity of the actors (both official and functional representatives) and the organizations they represent, while also fulfilling zero trust architecture requirements.

⁶ GLEIF, 2022, #7 in the LEI Lightbulb Blog Series - Spotlight on India: A Rise in LEI Mandates Offers MSMEs a Springboard for Growth, available at: <https://www.gleif.org/en/newsroom/blog/number-7-in-the-lei-lightbulb-blog-series-spotlight-on-india-a-rise-in-lei-mandates-offers-msmes-a-springboard-for-growth>



The vLEI can support the Australian Treasury’s efforts to combat scam by providing robust identity management solutions for submissions. This would address critical needs such as the identification, authentication, authorization, security and management of users responsible for submitting information. The vLEI can also provide a standardized, verifiable identity layer that can reduce the manual processes involved in reporting frameworks, thereby simplifying the overall data collection ecosystem. As an example, GLEIF is participating in a proof of concept with the European Banking Authority (EBA) for Pillar 3 reporting, in which 17 banks have agreed to participate using the vLEI for private sector reporting to the EBA.

EBA assessed the vLEI in collaboration with Gartner. Based on a first preliminary assessment, the EBA concluded that the vLEI could serve as a scalable and secure solution to authenticate and bind cryptographically the legal entity, an authorized representative, and this representative’s authority to submit EBA Pillar 3 Data on the EUCLID platform efficiently. The key points from Gartner’s analysis, after scanning the market, have been that there are no comparably efficient alternative solutions globally. For more information, please see section 6 in the document [PILLAR 3 DATA HUB PROCESSES AND POSSIBLE PRACTICAL IMPLICATIONS](#).

In a similar fashion, GLEIF encourages the Australian Treasury explore implementing the vLEI for the identification of the origins of calls. In particular, digital organizational identity tools, such as the vLEI, could be leveraged to identify the originators of robocalls and robotexts, while at the same time, legitimate enterprises struggle to have their calls and messages answered. Numerous entities, from the enterprises that originate communications, to the service providers that deliver these communications to end-users, would all benefit from vLEIs which could be used as the basis for identifying legitimate enterprises and their communications.

GLEIF remains at the Australian Treasury’s disposal to discuss and support its work. Please do not hesitate to engage us in discussions and questions related to the LEI and/or the vLEI in current and future consultations. We are also available to provide further assistance to ensure the LEI is leveraged in the most efficient manner, benefiting both consumers and regulators.

Submitted by:

Alexandre Kech, GLEIF CEO

Alexandre.Kech@GLEIF.org