



Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Australian Treasury’s Inquiry for the Scams Prevention Framework Bill

January 8th, 2024

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to submit its response to the inquiry on the Scams Prevention Framework (SPF) Bill.

We welcome the introduction and enforcement of the SPF, as it represents a crucial step toward reducing scams and enhancing consumer protection.

GLEIF’s comments focus on the benefits of applying standardized identities to combat scams in the Australian economy, in line with the SPF’s guiding principles. We also recommend implementing technical measures to prevent the tampering of electronic data, further enhancing the effectiveness of the SPF.

The foundational step in preventing fraud in any communication or transaction is identifying and authentically verifying the counterparty with whom electronic data is exchanged. Identification and authentication are essential preconditions for ensuring the integrity of all six overarching guiding principles of the SPF. However, in many cases, reliably identifying the counterparty based solely on names and addresses—which are frequently exchanged in transactions—can be challenging.

This challenge is particularly pronounced in the Australian market, which involves numerous cross-border transactions, especially with Asian countries (as the SPF is extended to outside of Australia). The complexity is exacerbated by the use of different languages, formats, and the presence of duplicated or similar names, leading to frequent misidentification of counterparties.

For example, in past terrorist incidents in Europe, when a list of organizations suspected to be linked to terrorism was shared between countries, only names and addresses were exchanged. This resulted in significant time and effort required to properly identify these



organizations. To prevent similar issues, we recommend that the current draft framework mandate the use of globally standardized corporate identifiers (IDs).

Since the SPF extends beyond Australian borders to cover "acts, omissions, matters, and things outside Australia," it is essential to identify counterparties globally. Therefore, a globally recognized ID, in addition to national registration IDs, is necessary. Many jurisdictions have already implemented measures to facilitate the certification of foreign companies, and as cross-border transactions increase, adopting a standardized ID could help streamline this process and ensure a whitelist effect.

When considering the adoption of standardized IDs, it is important to focus not only on international standards such as ISO, but also on the quality of the data and the accessibility of information. The ID should reflect significant corporate actions such as mergers and acquisitions. This is particularly critical, as companies that do not have a legitimate presence are often used for fraudulent activities. Thus, maintaining high data quality is crucial. Moreover, it is important to ensure that necessary information is accessible to end users in a way that is both efficient and transparent. This principle is echoed in the Digital Product Passport Regulation under consideration in Europe, which aims to improve data accessibility and transparency.

While it has been noted above that the adoption of standard IDs can help prevent many frauds, GLEIF would also like to call for the framework to recommend the application of technical measures to further prevent counterfeiting and spoofing of the electronic data traded or exchanged. While the adoption of standardized IDs can significantly reduce fraud, GLEIF also advocates for the application of technical measures to further prevent counterfeiting and tampering of electronic data. While the standard ID ensures the authenticity of a counterparty, preventing fraud that exploits or alters electronic data—such as payments or orders—is equally important.

In recent years, several technologies have emerged to protect the integrity of electronic data throughout its lifecycle. Even if not made mandatory, recommending these technologies within the framework would further enhance safety. For example, there have been cases of fraud where only the amount or delivery address was altered while a legitimate ID was used. This type of fraud can be easily prevented by adding measures to safeguard the integrity of electronic data and prevent tampering or spoofing.

Specifically, technologies like digital certificates and Verifiable Credentials can help ensure the authenticity of exchanged electronic data. These technologies also provide



cryptographically secure authentication of individuals and their affiliations with specific organizations.

By applying standardized IDs and data tampering prevention measures to sectors like banking, telecommunications, and digital platforms, the following benefits can be realized:

Examples in the Banking sector:

- ✓ In addition to allowing the end user to determine the authenticity of the SMS message, it will also be possible to take measures to eliminate it from being delivered electronically.
- ✓ Assigning a standard ID to a transaction makes it easier to trace and aggregate information
- ✓ It prevents the payment data exchanged from being exploited and changed on the way.

Examples in the telecommunications sector:

- ✓ It makes it easier to detect abnormal High-Volume data, and to prevent and eliminate it.
- ✓ In the same way as the banking sector, payment data exchanged is prevented from being exploited and changed on the way.

Examples in the Digital platform sector:

- ✓ Additional account verification can be performed easily and efficiently by granting a standard ID.
- ✓ Suspicious accounts can be found more easily.
- ✓ Statistical information can be efficiently obtained at the time of reporting.

The Legal Entity Identifier (LEI) and the verifiable LEI (vLEI), both issued and operated by GLEIF, are ISO-standard global identity solutions that meet all the requirements outlined above. As noted in our response to the October 2024 consultation (attached), the adoption of the LEI and vLEI is being considered in other public initiatives in Australia. We believe that incorporating the LEI and vLEI into the SPF will ensure greater consistency with national policies.



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.

Submitted by:

Alexandre Kech, GLEIF CEO