

Leveraging the Legal Entity Identifier to mitigate the risk of financial crime and enhance fraud prevention in cross-border payments

Received (in revised form): 13th December, 2023

Clare Rowley

Head of Business Operations, Global Legal Entity Identifier Foundation, Switzerland

Clare Rowley is the Head of Business Operations at the Global Legal Entity Identifier Foundation (GLEIF). Prior to working with GLEIF, Ms Rowley worked at the United States Federal Deposit Insurance Corporation, where she led technology initiatives improving bank resolution programmes and contributed to research on subprime mortgages. Ms Rowley is a CFA® charter holder and holds an MS in predictive analytics from Northwestern University.

ABSTRACT

While today's global digital economy promises a new era of commerce, its sheer complexity also presents opportunities for malicious actors to perpetrate money laundering, terrorism financing, and other forms of financial crime. Despite the escalating compliance costs faced by financial institutions needing to meet increasingly rigorous anti-money laundering (AML), counter-terrorist financing (CTF) and sanction screening obligations, the lack of harmonisation within cross-border data flows inhibits the identification of suspicious actors and exposure of criminal networks. This contributes to a cross-border payments ecosystem that can be broadly characterised by limited trust, high costs, low speed and insufficient transparency. This is leading to increasing industry recognition of the need to promote unified, data-driven approaches to combating financial crime globally. In view of this growing consensus, the Legal Entity Identifier (LEI) is emerging as a key enabler. This paper examines the drivers of this consensus by: (1) detailing findings from key industry organisations, such as the Bank for International Settlements (BIS) and Financial Action Task Force (FATF),

outlining the need to increase data quality and standardisation of the data identifiers used within cross-border payment messages to counter complex global criminal enterprises; (2) outlining regulatory and industry momentum to leverage the unique benefits of the LEI within cross-border payment messages, to include an analysis of the implications and opportunities of ongoing initiatives to enhance payment market infrastructures; and (3) demonstrating how, by addressing inconsistencies in how legal entities are identified, connecting a greater range of datasets, and capturing entity relationships and ownership structures, the LEI mitigates AML–CFT risks, enhances fraud prevention, and supports more efficient sanction screening in cross-border payments. This is supported by examples of real-world industry initiatives.

Keywords: *cross-border payments, digital identity, financial crime, FSB cross-border roadmap, FATF principles, fraud management, AML–CFT management, counterparty risk management, management of sanction risks*

INTRODUCTION

Money laundering and the financing of terrorism present significant systemic challenges to the global financial system. The Bank for International Settlements (BIS) conservatively estimates that between US\$2–5tn is laundered globally each year, with less than 1 per cent recovered.¹

In a bid to stem the tide of dirty money across the global economy, financial



Clare Rowley

Global Legal Entity Identifier Foundation (GLEIF),
St. Alban-Vorstadt 12,
PO Box,
4002 Basel,
Switzerland

E-mail: clare.rowley@gleif.org

Journal of Payments Strategy & Systems
Vol. 18, No. 1 2024, pp. 39–50
© Henry Stewart Publications,
1750-1806

institutions are subject to increasingly stringent and intricate regulations to combat money laundering and the financing of terrorism (AML/CTF regulations), as well as various screening requirements against ‘watch-lists’ and international sanctions — the cost of which is spiralling. The increasing sophistication, technological capabilities and ingenuity of criminal networks compound the challenge, as do the considerable reputational risks associated with non-compliance.

The scale of the issue is laid bare in a recent study from LexisNexis,² which reports that global crime-related regulatory compliance cost financial institutions more than US\$206bn in 2023. Given this context, there is an understandable push within financial institutions to ‘identify and optimise the efficiency and efficacy of financial crime compliance concerning payments’, with 74 per cent of surveyed financial institutions emphasising this as a ‘critical or high priority endeavour’.³

This push has led to an increased focus on ‘trust programmes’ — namely, organisations making investments in security, privacy and compliance technologies to improve their risk posture. According to a recent IDC Technology Spotlight⁴ conducted on behalf of the Global Legal Entity Identifier Foundation (GLEIF), some 79 per cent of organisations globally prioritised ‘trust programmes’ in 2023. Given that all large-scale laundering operations involve at least some element of cross-border activity, the ability to build trust between counterparties across borders and legal jurisdictions is a must.

TACKLING GLOBAL FINANCIAL CRIME THROUGH DATA STANDARDISATION AND HARMONISATION

Fraudsters, terrorist financiers and other criminal enterprises exploit the inherent complexity and immediacy of today’s digitised global economy to wash illicit funds,

building elaborate networks that traverse borders and jurisdictions, and exploit multiple financial institutions and legal entities along the way.

Fragmentation largely inhibits a coherent and common response to this challenge. The datasets used by financial institutions (FIs) to detect and monitor suspicious financial flows are not standardised or readily consumable and shareable, which hinders collaboration and drastically limits the capacity to expose global criminal enterprises. As noted by the BIS, ‘most FIs rely on siloed data and isolated systems for their suspicious transaction monitoring, thus limiting their ability to detect complex cross-border and cross-institutional money laundering networks’.⁵

Consequently, harmonising cross-border data flows to overcome these ongoing challenges is an increasingly urgent priority. The Financial Action Task Force (FATF) has identified data-sharing, data standardisation and advanced analytics as underpinning effective AML and CTF initiatives across borders.⁶ More specifically, Project Aurora⁷ — an analysis by the BIS Innovation Hub — identifies ‘data quality and standardisation of the data identifiers and fields’ contained within the payment messages as important factors to improve data consistency and usability. This includes ‘greater use of the Legal Entity Identifier in data sets associated to legal entities’.

This has significant implications for the Legal Entity Identifier (LEI) within the context of cross-border payments. As the only established universal entity identifier globally, it is uniquely positioned to play a foundational role in the fight against financial crime.

THE LEGAL ENTITY IDENTIFIER AS A FOUNDATION FOR FIGHTING FINANCIAL CRIME

Over 2 million legal entities around the world already identify themselves internationally

using an LEI.⁸ This identifier is an ISO standardised 20-digit alpha-numeric code connected to a verified business registration and information record in the Global LEI Index — a data bank maintained by GLEIF and made available to everyone, everywhere, free of charge. No two LEIs are ever the same. One LEI represents one legal entity. This means that any third party anywhere in the world can cross-reference who an organisation claims to be, together with its ownership structure and subsidiary relationships, against a legitimate and verified data source.

In the fight to reduce financial risk globally by curbing money laundering, terrorism financing and other forms of financial crime, more than 200 financial regulators worldwide have already mandated the LEI among legal entities engaging in capital markets.

The system is now expanding beyond regulated use and re-focusing on helping organisations use the LEI to bring greater trust, efficiency and transparency to trade of all kinds. To support this expansive development, GLEIF has developed a new model of decentralised business identity — the verifiable LEI (vLEI) — that enables businesses everywhere to use the Global LEI System to automatically identify themselves and verify the authenticity of counterparty organisations in the digital world. The vLEI conforms to the popular ‘never trust, always verify’ mantra, embodied by the counterintuitively labelled ‘Zero Trust Architecture’ movement, which is rapidly growing within the cyber security industry. It provides a new, verifiable digital trust layer that sits beneath the conventional information exchanged between supply-chain organisations.

The LEI in cross-border payments

In October 2020, the G20 endorsed a roadmap⁹ to enhance cross-border payments developed by the Financial Stability Board (FSB) in coordination with the BIS Committee on Payments and Market

Infrastructures (CPMI) and other international organisations and standard-setting bodies.

In July 2022, the FSB¹⁰ put its full weight behind a landmark recommendation that the LEI should be widely adopted across the global payments ecosystem. Global standards-setting bodies and international organisations with authority in the financial, banking and payments space were encouraged to drive forward LEI references in their work.

A primary near-term goal of the FSB’s report is to stimulate LEI use initially in cross-border payment transactions. By helping to make these transactions faster, cheaper, more transparent, and inclusive, while maintaining their safety and security, the LEI has been deemed by the FSB as a key identifier that can support the strategic goals outlined in the G20 roadmap.

The FSB’s position echoes an earlier FATF industry survey,¹¹ in consultation with the Basel Committee on Banking Supervision (BCBS), where many respondents advocated the broader adoption of the LEI for cross-border payments to support widespread interoperability, reduced costs and increased transparency.

It also aligns with SWIFT’s ‘Guiding principles for screening ISO 20022 payments’,¹² endorsed by the PMPG and Wolfsberg Group, which highlighted how the LEI can support an effective, targeted approach to sanctions screening.

In view of these recommendations, there has already been movement to mandate the LEI on a national level:

- 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 20022.¹³
- The Chinese Cross-border Interbank Payment System (CIPS) has developed the ‘CIPS Connector’ to further the

use of the LEI in cross-border transactions and facilitate cross-border trade and investment. Every CIPS Connector user is assigned with an LEI, which is used for activating the tool as well as a mandatory business element in their business transaction.

- The Reserve Bank of India (RBI) issued a mandate for the LEI in all payment transactions totalling ₹500m or 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.¹⁴

GROWING REGULATORY MOMENTUM FOR THE LEI IN CROSS-BORDER PAYMENTS

The previous section outlined advocacy for, and implementations of, the LEI within today's cross-border payments ecosystem. This paper will now explore how ongoing initiatives to enhance payment market infrastructures, namely the planned review of FATF Recommendation 16 and the migration of payments systems to the ISO 20022 payment messaging standard, offer significant opportunities to extend the use of the LEI and promote data-driven approaches to combating financial crime globally.

FATF Recommendation 16

The FATF Recommendations¹⁵ set out a comprehensive and consistent framework of measures that countries should implement to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction. Recommendation 16, often referred to as the 'Travel Rule', specifically aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available.

While the interpretative note to Recommendation 16 references name,

address and national identifiers as important data elements for inclusion within the transaction message, it does not currently reference the LEI. This is a missed opportunity. National and local identifiers such as business codes play an important role within borders and legal jurisdictions but are, by their nature, inherently limited in their capacity to contend with the increased complexity and fragmentation associated with cross-border commerce.

In view of this, they should be complemented by a globally recognised identifier, like the LEI. As part of the upcoming review of Recommendation 16, GLEIF posits that where the originator or beneficiary is a legal entity, a trust, or any other organisation that has legal capacity under national law, the LEI should be included within the information accompanying the qualifying wire transfer.

The European Union's recent Markets in Crypto-Assets (MiCA) regulation also offers a compelling precedent for this position. MiCA addresses Recommendation 16 by extending the scope of the existing EU Transfer of Funds Rule (TFR) — first adopted in 2015 and applicable to traditional transfers of funds — to include transfers of crypto assets. Under the recast TFR, the crypto-asset service provider of the originator must ensure that transfers of crypto assets are accompanied by various data points on the originator and beneficiary (for non-individuals). Importantly, this includes the current LEI or, in its absence, any other available equivalent official identifier.¹⁶

ISO 20022 harmonisation

The CPMI has recently published its 'Harmonised ISO 20022 data requirements for enhancing cross-border payments'.¹⁷ The requirements, which were developed in collaboration with the Payment Market Practice Group (PMPG), establish a consistent minimum set of messaging data for more efficient processing of cross-border payments in support of G20 targets.

Following feedback from various industry stakeholders during the consultation phase, the CPMI recognised the LEI as an equivalent identifier to the business identifier code (BIC) for identifying financial institutions and legal entities within a payment message.

Specifically, the data-structuring requirements suggest the LEI and/or BIC for identifying all financial institutions involved in a cross-border payment in an internationally recognised and standardised manner. The LEI and/or the BIC may also substitute or complement name and postal address information to aid the identification of all legal entities involved in a cross-border payment in a standardised and structured way. (It should be noted that GLEIF and SWIFT have collaborated on an open source mapping file that enables market participants to link and cross-reference the LEI and BIC. This promotes consistency and facilitates the use of either or both identifiers by financial institutions.)¹⁸

The CPMI position reflects industry feedback that the LEI enables clear and unique identification of legal entities; is based on an international ISO standard; is globally accessible and open; offers high data quality; and is supported by a system subject to robust, international regulatory oversight.

In parallel, The Wolfsberg Group — an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks — has published its updated Payment Transparency Standards,¹⁹ which begin to identify how various capabilities within the ISO 20022 structure can be utilised to enhance payment transparency. The updated standards state that to the fullest extent permitted by the payment market infrastructure, the payment service provider of the payer (referred to within ISO 20022 as the ‘debtor agent’) should use the LEI or other equivalent reference codes to enhance the accuracy of identification information on relevant parties. Additionally, policies may set out

where a unique identifier code such as the LEI is sufficient to identify the debtor without full name and address information.

The Project Aurora initiative also highlights how the inclusion of the LEI in ISO 20022 payment messages, when combined with additional data fields available in the messages, could ‘help identify a greater range of money laundering activities involving legal entities’.²⁰

EXPLORING THE USE OF THE LEI TO MITIGATE AML–CFT RISKS

As the previous sections demonstrate, there is growing awareness and advocacy from regulators, industry bodies and standards development organisations on the potential for the LEI to address key challenges constraining the cross-border payments ecosystem.

By addressing inconsistencies in how entities are identified, connecting a greater range of datasets, and capturing entity relationships and ownership structures, the LEI can support improved risk management and enable enhanced monitoring, reporting and analytics. This can bolster efforts to tackle financial crime and promote greater trust and transparency; and mitigate and ameliorate the AML/CTF compliance burden for financial institutions, while supporting more effective and efficient screening against sanctions and watch-lists.

Addressing inconsistencies in entity identification

When the LEI — as a unique global identifier — is added as a data attribute in payment messages, any originator or beneficiary legal entity can be precisely, instantly and unambiguously identified across borders.

This solves the complexity associated with the use of national and local identifiers within cross-border payments. For example, there are over 1,000 legal entity registration authorities worldwide, and the format and

data quality of respective business registration numbers varies greatly across different countries and jurisdictions. This lack of standardisation in how entities are identified makes it difficult to exchange and integrate data on a global scale.

The LEI overcomes these issues by providing a common language and structure to facilitate holistic analysis. The Global LEI System links with the local business registries that might be proprietary and in different character sets. This means that instead of navigating through various access points and languages, the Global LEI System allows corporate payors, payments service providers and consumers to conduct quick due diligence in a trusted way, as all parties can easily know and verify with whom they are transacting. The system is also endorsed by the 65 public authorities that participate in the Regulatory Oversight Committee to provide an additional trust layer.²¹

In summary, and as noted by Beju Shah, Head of the BIS Innovation Nordic Centre:

‘Using the LEI for the identification of businesses involved in cross-border payments would significantly advance the ability to share information and overcome the inconsistencies in how entities are identified today in cross-border payments.’²²

Industry initiative: Bloomberg on using the LEI for sanctions screening²³

Through its extensive corporate hierarchy database, Bloomberg identifies explicitly stated sanctions as well as implicitly sanctioned entities and instruments. Bloomberg’s sanctions data provide the sanctioned status of tradable securities, legal entities and certain public funds in a timely and consistent manner, enabling pre-trade screening and post-trade compliance checks.

The challenge

Sanctions authorities publish lists of entities and natural persons to modify undesirable

behaviour. However, these authorities do not always provide details on the business registration ID, tax ID or other identifying information in their lists, making it difficult to validate targeted entities.

This is only part of the challenge. Financial institutions may also need to identify impacted subsidiaries and securities that are not explicitly listed, in a timely manner. Complicating matters are scenarios where convertible bonds or other securities may be impacted by sanctions even when the issuer is not.

As a result, data vendors like Bloomberg must complete a significant amount of research to establish relationships between companies and links to financial instruments to understand the scope of sanctions. Given that name-matching processes for sanctions are both arduous and time-consuming, a significant opportunity exists to promote broader adoption of the LEI.

The opportunity

LEIs play an important role in understanding the counterparties engaged in a financial transaction, which makes them very useful for sanctions compliance purposes; it means that transacting parties can be unambiguously identified, preventing the generation of false positives that may be created during name-matching processes. (Note: while criminal entities will likely avoid registering for an LEI where possible, the identification of all legitimate entities using the LEI will support automated whitelisting — enabling significant efficiencies by enabling resources to be focused on suspicious entities only.)

Wider adoption of LEIs could enhance identity-based screening systems, making sanctions compliance faster, more effective and less expensive to administer for all stakeholders. To correctly identify the legal entity affected by sanctions it would also be beneficial if sanctions authorities could add the LEI, where applicable, to the legal entities subject to sanctions. This should also

reduce the risk of false positives and add transparency.

By embracing an LEI-based system where legal entity identification can be unequivocally assured, in an open, interoperable and instant digital format, all stakeholders would be able to transact with far greater confidence and efficiency.

Looking ahead to the future value, Bloomberg utilises name-matching engines to compile an initial list of companies potentially impacted by sanctions. Entity names not found as part of the initial screening are manually reviewed against Bloomberg's database, and any entity that is not already included in the database is then added.

The LEI opens the possibility to greatly streamline the entity identification process and allow for straight-through processing. As a result, Bloomberg sees the value in sanctions authorities providing the LEI of sanctioned entities in their lists. The LEI is a unique and non-transferable validation point which would make the accurate identification of sanctioned entities faster, cheaper and simpler. (Note: this would address a key current implementation challenge, as the publicly available sanctions and watch-lists maintained by supervisory authorities around the world do not uniformly include the LEI as a standardised identifier).

The LEI can also help identify subsidiaries that are impacted as part of a corporate hierarchy. In addition, because the LEI dataset showcases the entity's country of operation, it would also make it easier to tag entities in sanctioned countries and regions. (For further information, see section on capturing entity relationships and ownership structures.)

Connecting different datasets

The LEI is a key data connector that enables critical data sets to be matched efficiently. The LEI can be directly mapped to myriad other identifiers to provide a comprehensive view of a legal entity, including the

OpenCorporates ID, S&P Global Company ID, SWIFT's Market Identifier Code (MIC) and BIC, and the Association of National Numbering Agencies' International Securities Identification Number (ISIN).

This 'ability to map' is the key to creating a holistic understanding of the complex networks built by criminal enterprises.

Industry initiative: The Transparency Fabric – using the LEI to enhance sanctions and AML screening²⁴

The Transparency Fabric is a joint initiative progressing between GLEIF, Open Ownership and OpenSanctions, which is set to revolutionise the screening process, by making it significantly easier to trace parties engaged in money laundering, terrorist financing and sanctions evasion.

The challenge

The initiative addresses the need for trusted international entity identifiers to be embedded within accurate and up-to-date data on the beneficial ownership and control of corporate vehicles, so it can be mapped to watch-lists, including politically exposed persons (PEP) lists, which also integrate the same entity identifiers. This would make it far easier to find direct and indirect connections between businesses and the person(s) exercising ultimate effective control over a company, thereby supporting AML, customer due diligence and sanctions enforcement efforts globally.

The opportunity

The Open Ownership database provides beneficial ownership transparency to help tackle corruption, reduce investment risk and improve governance. It currently provides over 26 million beneficial ownership records for 9.6 million companies globally. Its data are already reconciled with the OpenCorporates database, to ensure the highest-quality data sourced from national business registries in 140 jurisdictions. As a

result of the Transparency Fabric collaboration, Open Ownership is expanding the Open Corporates data fields it integrates to include the LEI where one is available. This will enhance the usability and mapping of Open Ownership data with other datasets globally.

Under the Transparency Fabric initiative, the Open Ownership database, including newly integrated LEI data, will be further mapped to the OpenSanctions database, which includes 80 government-published sanctions lists and multiple international databases of PEPs.

This three-way collaboration will result in the LEI becoming a common denominator across both beneficial ownership data and sanctions and watch-list publications. This will lead to the easier identification of direct and indirect connections between businesses that have an LEI and sanctioned persons and companies, using graph database solutions.

With LEIs embedded within Open Ownerships beneficial ownership data records and within Open Sanctions data, the potential exists for those data sets to be mapped to other data sets, from any data provider globally. The LEI opens the possibility to greatly streamline the entity identification process. It serves as the data connector starting with accurate identification of the involved entities and their direct and indirect connections with other corporate vehicles — all that means faster, cheaper and simpler compliance. Data users across governments, the public and private sectors will be available to quickly and easily identify people and companies that pose a compliance risk. This will deliver a more transparent and secure financial landscape for all.

Industry Initiative: ISO 20022 address field mapping

Addresses are foundational to the global economy. As noted by the Universal Postal Union, ‘addresses form an important part of the basic information needed to ensure

communication (both digital and physical) between individuals, governments, and organisations’.²⁵ Given the fundamental role in enabling legitimate access to global commerce, incorrect, incomplete, or incongruous address information is often seen as a ‘red flag’ signalling illegal activity within cross-border payments.

The challenge

The inclusion of address information within a payment message presents unique considerations. For example, address structures are wildly inconsistent across countries and jurisdictions, and can be inconceivably complex due to the vast array of potential combinations. Cross-border payments compound this complexity, as these transactions often involve organisations with addresses in different languages, formats and colloquial styles.

The ISO 20022 messaging standard aims to solve this problem through the introduction of highly structured, discrete, character-limited elements for specific address information. Nevertheless, the sheer complexity means that different organisations are simply not going to interpret addresses the same way.

Rather than add further structured fields in response to outliers (which only contributes to further complexity), overcoming this problem requires a common, globally consistent starting point. This is especially true for the creditor address data information in cross-border payment transactions. While debtor address information can be sourced from the debtor agent’s know-your-customer (KYC) master records, the debtor interpretation of the creditor address into the ISO 20022 format is recognised as being ‘problematic’.²⁶

The opportunity

In comparison to the highly structured ISO 20022 address format, the LEI is more streamlined and minimally structured to

account for the significant variability and flexibility. This is particularly important in the context of cross-border payments, where differences in address format are guaranteed. While this means that the format of the structured address within the LEI does not match exactly the format of the structured address within an ISO 20022 payment message, the LEI index can be used to map LEI address data into the ISO 20022 format.

Put simply, the LEI address information should be considered compliant with ISO 20022, and relevant address fields can be retrieved from the LEI reference data in an automated manner to reduce ambiguity and enable straight-through processing.

Capturing entity relationships and ownership structures

The core attributes of legal entities (such as directors, major shareholders and ownership structures) are subject to frequent updates and changes that demand ongoing data updates. Yet depending on the jurisdiction, business registration data update cycles vary widely, often resulting in outdated information that undermines the entire system. This demands solutions that accommodate regular updates, and LEI data can be updated proactively whenever there are changes or as part of the annual renewal process. Data consumers can also easily track the changes and, if required, challenge outdated information.

Similarly, company mergers and acquisitions can create complex and fragmented company structures that often span multiple jurisdictions. The LEI provides a simple and transparent historical view of a legal entity, as well as enabling the monitoring of ongoing mergers and acquisitions.

Industry initiative: Moody's Analytics on the power of the LEI in KYC and corporate onboarding²⁷

Most Moody's Analytics KYC customers choose its global business verification and

know-your-business solutions to manage ongoing risk and AML compliance. Using its solutions, customers can connect to the latest, most accurate official data sources to understand risks and make decisions with confidence about whom they work with.

The challenge

A core challenge for customers is to efficiently access the data they need for robust due diligence and ongoing risk monitoring. To this end, Moody's collates such data from disparate sources. Connectivity to business registries, for example, varies greatly from jurisdiction to jurisdiction. In some countries automated access is supported by the register. In others, data can only be retrieved via a user interface. The data availability itself also varies significantly. Some commercial registers offer access to fully structured and rich datasets, whereas others only make limited sets of data points available in an unstructured way within documents.

These variations shine a light on the inherent complexity of providing the data needed for entity verification and onboarding, together with the importance of accessing accurate, up-to-date, risk-relevant information.

In a typical onboarding process, customers search Moody's Analytics databases and real-time access network for relevant information and data on an entity, analyse it and then decide about onboarding. To assist this process, customers can set rules based on the information they retrieve, which provides further refinement on risk indicators to complete a profile.

Moody's customers report that onboarding times for corporate customers differ significantly depending on the information that needs to be collected. If it is a basic merchant, onboarding could take just a few minutes. For larger customers or suppliers who, for example, may have complex ownership hierarchies, onboarding can be more protracted.

The opportunity

Today, Moody's Analytics KYC uses the LEI in its real-time entity verification service for certain use cases. Where the LEI is assessed, customers are also typically keen to see if an onboarding entity's LEI renewal date is updated, so it can be factored into their risk assessments. Moody's offers customers the ability to search the Global LEI Index, and if the entity has an LEI, it ensures it is added to its reference table. As not all entities have an LEI, its use as a global identifier system is currently limited.

Looking ahead, so-called 'perpetual KYC' or pKYC is the key to ensuring onboarding data and risk profiles are kept up to date. If the LEI were mandated consistently across jurisdictions in onboarding and risk-monitoring processes, it could play a pivotal role in automating the KYC industry — saving time and money for all stakeholders, including financial institutions, supply chain organisations, large corporates and other regulated firms.

The LEI would provide significant efficiency gains when onboarding complex multinational companies as their ownership hierarchies are trackable via the Global LEI Index. This holds especially true for offshore entities for whom real-time access to data via business registries is not available in all jurisdictions, meaning it can take weeks to obtain the necessary entity information.

TOWARDS TRUSTED, TRANSPARENT CROSS-BORDER PAYMENTS

The pace of industry momentum behind the use of the LEI in financial flows is a clear testament to its vast potential to strengthen the world's defences against cross-border criminality and ease the compliance burden for financial institutions.

As payment market infrastructures across the world move to support instant payments, the ability to verify and validate the originator and beneficiary of a transaction

in near-real time is a foundational requirement to enable consumers, businesses and financial institutions to verify that funds are transferred across international borders to the correct entity.

The LEI can be directly mapped to other useful identifiers to provide a comprehensive view of a legal entity. It also provides a simple and transparent historical view of a legal entity, as well as enabling the monitoring of ongoing mergers and acquisitions, that penetrates the opacity of complex corporate structures.

Collectively, these benefits have various downstream impacts that mitigate the constraints of cross-border commerce to help tackle financial crime. Regulatory reporting, AML/CTF requirements and sanction screening can be streamlined with increased accuracy. Counterparty risk management and due diligence are improved as it is far easier to assess and verify the legitimacy of a legal entity involved in a transaction. In addition, the oversight of complicated corporate structures and supply chains is greatly simplified, leaving fraudsters and criminals with fewer places to hide.

The more widely the LEI is utilised in this manner, the more value it will deliver to the world's regulators, financial institutions and law-abiding legal entities. Ultimately, this can realise the promise of faster, cheaper, more transparent and inclusive cross-border transactions in support of the G20's ambitions.

For this reason, GLEIF continues to work with leading payments industry stakeholders to demonstrate the significant value the LEI brings to non-financial corporates and financial institutions when transmitted in cross-border payment flows. As part of this engagement, GLEIF reiterates the FSB's call for global standards-setting bodies and international organisations with authority in the financial, banking and payments space to drive forward LEI references in their work as part of the fight against financial crime.

REFERENCES

- (1) Bank for International Settlements (BIS) (2023) 'Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders', available at: <https://www.bis.org/publ/othp66.pdf> (accessed 12th December, 2023).
- (2) LexisNexis (2023) 'True cost of financial crime compliance study', available at: <https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report> (accessed 12th December, 2023).
- (3) *Ibid.*
- (4) IDC (2023) 'IDC Technology Spotlight: Driving business with trust — the sustaining role of digital identities', available at: <https://www.gleif.org/en/lei-solutions/gleifs-digital-strategy-for-the-lei/gleif-idc-research-creating-agile-resilient-global-trade-with-the-lei-and-vlei> (accessed 12th December, 2023).
- (5) Bank for International Settlements (BIS), ref. 1 above.
- (6) Financial Action Task Force (2021) 'Opportunities and Challenges of New Technologies for AML/CFT', available at: <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html> (accessed 12th December, 2023).
- (7) Bank for International Settlements (BIS), ref. 1 above.
- (8) Wolf, S. (2022) 'How the Legal Entity Identifier supports the digitisation of business transactions', *Journal of Payments Strategy & Systems*, Vol. 16, No. 2, pp. 148–159.
- (9) Financial Stability Board (2021) 'G20 Roadmap for Enhancing Cross-border Payments: First consolidated progress report', available at: <https://www.fsb.org/2021/10/g20-roadmap-for-enhancing-cross-border-payments-first-consolidated-progress-report/> (accessed 12th December, 2023).
- (10) Financial Stability Board (2022) 'Options to improve adoption of the LEI in particular for use in cross-border payments', available at: <https://www.fsb.org/wp-content/uploads/P070722.pdf> (accessed 12th December, 2023).
- (11) Financial Action Task Force (2021) 'Cross-border payments: Survey results on implementation of the FATF standards', available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cross-Border-Payments-Survey-Results.pdf> (accessed 12th December, 2023).
- (12) Swift (2021) 'Swift guiding principles for screening ISO 20022 endorsed by the Wolfsberg Group', available at: <https://www.swift.com/news-events/news/swift-guiding-principles-screening-iso-20022-endorsed-wolfsberg-group> (accessed 12th December, 2023).
- (13) Bank of England (2023) 'Policy Statement: Implementing ISO 20022 enhanced data in CHAPS', available at: <https://www.bankofengland.co.uk/-/media/boe/files/payments/rtps-renewal-programme/iso-20022-policy-statement-implementing-iso-20022-enhanced-data-in-chaps-january-2022.pdf> (accessed 12th December, 2023).
- (14) 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> (accessed 12th December, 2023).
- (15) Financial Action Task Force (2023) 'The FATF Recommendations', available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> (accessed 12th December, 2023).
- (16) European Council (May 2023) 'Digital finance: Council adopts new rules on markets in crypto-assets (MiCA)', press release, 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/> (accessed 12th December, 2023).
- (17) Committee on Payments and Market Infrastructures (2023) 'Harmonized ISO 20022 data requirements for enhancing cross-border payments — final report', available at: <https://www.bis.org/cpmi/publ/d218.htm> (accessed 12th December, 2023).
- (18) GLEIF (2023) 'Download BIC-to-LEI Relationship Files', available at: <https://www.gleif.org/en/lei-data/lei-mapping/download-bic-to-lei-relationship-files> (accessed 12th December, 2023).
- (19) Wolfsberg Group (2023) 'Wolfsberg Group Payment Transparency Standards', available at: <https://db.wolfsberg-group.org/assets/13422898-fba1-44b3-9679-a8c7406e9e78/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf> (accessed 12th December, 2023).
- (20) Bank for International Settlements (BIS), ref. 1 above.
- (21) Regulatory Oversight Committee (2023) 'About the ROC', available at: <https://www.leiroc.org/> (accessed 12th December, 2023).
- (22) GLEIF (2023) '#13 in the LEI Lightbulb Blog Series — Understanding the value of global identifiers in the fight against financial crime', available at: <https://www.gleif.org/en/newsroom/blog/number-13-in-the-lei-lightbulb-blog-series-understanding-the-value-of-global-identifiers-in-the-fight-against-financial-crime> (accessed 12th December, 2023).

- (23) GLEIF (2023) 'LEI in Cross Border Payments Pilot Engagements: Bloomberg on using the LEI for sanctions screening', available at: <https://www.gleif.org/en/lei-solutions/featuring-the-lei/1-cross-border-payments> (accessed 12th December, 2023).
- (24) GLEIF (2023) 'LEI in Cross Border Payments Pilot Engagements: The Transparency Fabric: Using the LEI to enhance sanctions and anti-money laundering screening', available at: <https://www.gleif.org/en/lei-solutions/featuring-the-lei/1-cross-border-payments> (accessed 12th December, 2023).
- (25) Universal Postal Union (2023) 'Addressing', available at: <https://www.upu.int/en/Universal-Postal-Union/Activities/Physical-Services/Addressing> (accessed 12th December, 2023).
- (26) Payments Market Practice Group (2019) 'Structured ordering and beneficiary customer data in payments', available at: <https://www.swift.com/swift-resource/234447/download?language=en> (accessed 12th December, 2023).
- (27) GLEIF (2023) 'LEI in Cross Border Payments Pilot Engagements: Moody's Analytics on the power of the LEI in KYC and corporate onboarding', available at: <https://www.gleif.org/en/lei-solutions/featuring-the-lei/1-cross-border-payments> (accessed 12th December, 2023).