Trusted and open corporate data: Why adoption of the LEI/vLEI is key to enhancing risk management practices in the face of rapid digital transformation

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

Stephan Wolf
CEO, Global Legal Entity Identifier Foundation, Switzerland

Stephan Wolf is the Chief Operating Officer of the Global Legal Entity Identifier Foundation (GLEIF). In 2023, he became a Board member of the International Chamber of Commerce (ICC) in Germany. In 2021, he was appointed to the Industry Advisory Board (IAB) of the global ICC Digital Standards Initiative (DSI). Between January 2017 and June 2020, he was Co-convener of the ISO Technical Committee 68 FinTech Technical Advisory Group. In January 2017, he was named a Top 100 Leader in Identity by One World Identity.

Global Legal Entity Identifier Foundation, St. Alban-Vorstadt 12, 4052 Basel, Switzerland
E-mail: stephan.wolf@gleif.org

Abstract As financial institutions increase their participation in the global digital economy, huge opportunities emerge: more efficient and accurate ways to fight fraud and crime through automated processes and real-time industry collaboration and action; the disinhibition of capital flows needed to fuel economic development; the growth of broader and trusted cross-border customer bases, partner networks and supply chains; and, as will be explored more fully through the presentation of a use case, the capability to advance environment stewardship. These are just some of many possibilities, yet new threats materialise as companies digitise and digitalise. Many are connected to the challenge of identity management and verifying the authenticity and integrity of associated entity reference data in digital environments. How do organisations verify the legitimacy of who they are interacting with online? Can they trust the origin and integrity of digital data associated with customers, partners and other stakeholders, and that the data they do have is current and accurate? Here, the Legal Entity Identifier (LEI) together with its digitally verifiable counterpart, the vLEI, can play a crucial enabling role. This paper examines the opportunities and risks that financial institutions face as they embark on digital transformation programmes. It explores the importance of high quality, verified and open legal entity data to enhanced risk management practices. An outline is given of how a universal ISO entity identification standard, the LEI and its digital counterpart, the vLEI, can be used to: verify the identity of companies, their corporate organisational structures and their authorised executives; and to connect an organisation to verified business data, other identifiers, company reports and multiple data sources. A risk management use case will be presented — the use of the LEI as an environmental, social and governance data connector — to show how the LEI and vLEI can be harnessed by financial institutions to inform better business decision making and create enhanced, even automated, risk management practices within increasingly digital corporate ecosystems.

Keywords: *digital identity, identity management, open data, digital transformation, ESG reporting*

DIGITAL TRANSFORMATION: THE OPPORTUNITIES AND RISKS FOR FINANCIAL INSTITUTIONS

Digital transformation is the practice of driving forward strategy-based change programmes that leverage digital technologies to enhance company operations and business value propositions.

Globally, this practice is changing customer behaviour and expectations. As a consequence, it is also changing the way in which financial institutions do business. Thanks to their corporate clients' growing participation in international digital supply chains and the broader global digital economy, significant opportunities are emerging for financial institutions to realise both commercial gain and competitive advantage today and in the future.

The extent to which financial institutions are able to harness digital technology to help them assess and mitigate client risk sits at the heart of many such opportunities. Due to the fact that digital engagement enables businesses to interact and transact across borders faster than ever before, the job of assessing and mitigating risk has become highly time-sensitive — particularly for financial institutions that support their business clients with trade finance. Yet, the integrity of a risk management professional's decision making cannot be compromised for the sake of speed. The evolution of healthy global supply chains and other relationships that contribute to a growing economy rely on robust, non-negotiable risk mitigation practices, particularly those related to counterparty operations and commercial transactions between entities.

The ability to accurately and reliably identify partners, customers and other commercial entities across borders and legal jurisdictions underpins this effort. This capability becomes more complex, time-consuming and operationally onerous as ecosystems grow and become digitised. Put simply, in today's global digital marketplace, it is harder than ever to establish and maintain trust.

Global Legal Entity Identifier Foundation (GLEIF) contends that the optimal way to overcome this challenge lies in the universal adoption of a globally standardised form of secure, reliable and interoperable digital organisational identity. Financial institutions that realise this can enable their risk managers who are responsible for operational and transaction-oriented risk to evolve their client risk management and risk profiling capabilities to address a whole basket of current challenges relating to, among others, payment fraud and other forms of cross-border criminality, supply chain transparency, sustainability and financial inclusion. It will also support broader risk assessments relating to newly emerging risk factors that are increasingly influencing finance and investment decisions across the globe, most notably relating to environmental, social and governance (ESG) stewardship.

There are many commercial challenges faced by financial institutions in the wake of increasing digitisation that can become opportunities with the application of a standardised digital entity identity solution that supports robust risk management decisions. These opportunities include the following points.

1) The creation of more efficient and accurate ways to fight fraud and crime through automated processes and real-time industry collaboration and action

Cross-border payments account validation

Payment fraud trends are changing at a rapid pace. With the acceleration of real-time payments around the globe, both the volumes and types of payment fraud have changed significantly in recent years. In parallel, the regulatory landscape governing payment markets continues to evolve. In the United States, corporate clients must comply with Nacha Operating Rules and rely on their payment service provider (PSP) to provide compliant services. In the United Kingdom, banks have been mandated to provide a Confirmation of Payee service. In Europe, anticipated amendments to existing instant payments regulations will mandate account validation.

Providing frictionless cross-border account validation services is a significant challenge due to the varying country-level regulations, standards, identifiers, currencies and payment schemes.

The inability to verify account information prior to cross-border payment processing not only

increases risk for the financial institution but can also result in higher payment returns, additional fees, payment delays, increased risk and poor customer experience.

Incorporating a universal form of entity identification into cross-border account validation messaging could increase match rates, reduce misdirected payments and enhance fraud prevention, detection and intelligence monitoring.

In July 2022, the Financial Stability Board (FSB) put its full weight behind a landmark recommendation that a universal legal entity identifier — the Legal Entity Identifier (LEI) made available by GLEIF — should be widely adopted across the global payments ecosystem. In a FSB report,[1] 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, published as part of the 'G20 Roadmap for Enhancing Cross-Border Payments'[2] is to stimulate LEI-use initially in cross-border payment transactions. By helping to make these transactions faster, cheaper, more transparent and more inclusive, while maintaining their safety and security, the LEI has been deemed by the FSB to support the goals of the G20 roadmap.

Sanctions screening

In 'PwC's Global Economic Crime and Fraud Survey 2022',[3] only 6 per cent of organisations surveyed had experienced anti-embargo fraud (attempts by businesses or countries to violate embargoes and/or sanctions) in the last 24 months. While that figure seems low, Price Waterhouse Coopers (PwC) observes within that report that the figure is likely to change within the next 24 months as global sanctions rise to the highest level in recent history.

To combat fraud and other illicit transactions, publicly available sanctions and watch lists are maintained by a variety of supervisory authorities around the world. These lists typically comprise the names of persons and legal entities whose transactions are deemed to warrant further investigation.

Financial institutions responsible for enabling financial flows must ensure compliance with these lists by checking, sometimes manually, that the names published do not correspond with the names displayed on the transactions they perform with clients.

If an international legal entity identification standard was adopted in financial flows, compliance verification could be based on actual identities instead of just names. In reference to sanctions and watch lists, this means that transacting parties could be unambiguously identified, greatly reducing the number of false positives that the matching process generates today.

By embracing a system where legal entity identification can be unequivocally assured, in an open, interoperable and instant digital format, risk would be reduced across all stakeholders, enabling financial institutions to facilitate client transactions with far greater confidence. Most importantly, however, the opportunities for financial criminals to cheat the system will be dramatically reduced on a global scale.

2) The disinhibition of capital flows needed to fuel economic development

Financial institutions in developing economies are grappling to balance their clients' need for trade finance with their own developing compliance requirements. Africa's heterogeneous economies, for example, suffer from a severe trade finance gap, which was estimated in 2019 to be more than US$81bn.[4] The limited availability of transparent key reference information for African businesses, together with the perceived risk of trading with them, is a major challenge both to banks seeking to expand trade finance portfolios on the continent and to international business partners seeking to engage this underutilised, nascent sector.

If such banks were to introduce a standardised form of business identity to their business clients, inclusion in the region would be greatly strengthened. Equipped with such a credential, African businesses could then apply for trade finance and establish contractual, regulated agreements with banks, payment networks and trading partners, leading to broader access to financial services and greater participation in both domestic and international

markets. Ultimately, this would strengthen these businesses on the global stage and increase the flow of inbound capital that is needed to fuel the development of the world's emerging economies.

3) The growth of broader, trusted cross-border customer bases, partner networks and supply chains

Supply chain fraud is an area of emerging fraud risk that PwC believes should be on every firm's radar. In its 'Global Economic Crime and Fraud Survey 2022'[5] PwC reports that one in eight organisations

> experienced new incidents of supply chain fraud as a result of the disruption caused by COVID-19. One in five sees supply chain fraud as an area of increased risk as a result of the pandemic. Few companies are aware of the fraud and misconduct risks within their supply chain, making this an area of exposure now and into the future.

According to a recent IDC Technology Spotlight[6] conducted on behalf of GLEIF, 'identity crime and fraud has soared, with digitization and globalization sometimes causing huge financial damage and destroying trust'. It is widely observed that the problem of identity verification is exacerbated between those operating across borders as there is no universal identity management solution that is recognised across legal jurisdictions worldwide.

At the end of 2021, about 50 per cent of companies interviewed by the International Data Corporation (IDC) worldwide said identity security is a source of operational savings, a linchpin for overall security or a technology they wanted to spend more on. Within the same report, some 79 per cent of organisations globally are prioritising 'trust programmes' this year, making investments in security, privacy and compliance to improve their risk posture.

IDC posits that three key success factors will determine the future of digital identity and trade digitalisation: interconnectivity, ease of access and a critical mass of participants. Moreover, the analyst firm also dangles a huge carrot: if trade ecosystems can become interoperable, standardised, technology-agnostic and easily accessible by 2028, it expects digital trade finance transactions to account for 30 per cent of all trade finance.

When participants in global supply chains can share a validated and universally recognised form of digital identity with clients, partners and suppliers, they can build the trust and transparency needed for stronger trading relationships that, in turn, reduces their risk profile for the financial institutions they engage with.

Put simply, global supply chains need a global identity solution and quickly. This makes the job of mitigating client risk via the availability of secure, reliable and globally recognised organisational identities a vital prerequisite for a prosperous future in global digital trade.

4) The capability to advance environment stewardship

To comply with evolving ESG regulations, financial institutions everywhere must increasingly be able to quickly identify their client entity and the entity's subsidiaries to which they are providing finance.

ESG reporting fraud is one of the biggest emerging fraud risks that has the potential to cause significant disruption in the next few years according to PwC. In its 'Global Economic Crime and Fraud Survey 2022'[7] it states:

> with ESG responsibility growing in importance to stakeholders, accuracy in ESG reporting is essential. Just 8% of organizations encountering fraud in the last 24 months experienced ESG reporting fraud, but the incentive to commit fraud in this area is only going to increase — as will the consequences.

A key challenge in ESG reporting, data collection and data exchanges today is the lack of standardisation for entity identification. This makes it difficult to find, compare and consume ESG data globally, leading to a lack of transparency and inefficiencies. Without a clear, standardised and global entity identification system, ESG reports lose value as it is not easy to evaluate performance indicators across different reporting regimes or jurisdictions.

Imagine, for example, that a Swedish fashion company applies for a sustainability-linked loan with its financial institution. Would the institution's financing decision change if the Swedish company's subsidiaries in Bangladesh do not consider supplier risks? How can the financial institution analyse the entity's eligibility for this type of loan quickly and

easily — a key part of which must be to perform an ESG risk assessment — to enable a fast decision and a positive client experience?

There are innumerable national and regional standards for entity identification across the world and, while different identifiers serve national needs, they create significant conflicts and inefficiencies when reconciling data across geographical borders. What is needed, again, is a single source of entity identification through which the financial institution can access relationship and ESG information on the client and its subsidiaries through an easily consumable and machine-readable format.

The four sections listed above are just some of many possibilities and are not meant to be an exhaustive list.

New threats also materialise as companies digitalise and harness digital technologies to enhance process and performance. Forty-six per cent of organisations surveyed by PwC for its 2022 survey[8] reported experiencing some form of fraud or other economic crime within the last 24 months. Of these organisations, 40 per cent experienced fraud connected to the digital platforms they rely on. Fraud types included know your customer (KYC) breaches, disinformation, money laundering, terrorism financing and anti-embargo activities. Within the financial services industry specifically, PwC reports that the three main types of fraud were customer fraud (44 per cent), cybercrime (38 per cent) and KYC failure (29 per cent).

It is clear that a number of these risks are connected to the challenge of identity management and the transparency, authenticity and integrity of associated entity reference data in digital environments. How do organisations know who they are interacting with online, let alone verify their legitimacy? Can they trust the origin and integrity of digital data associated with customers, partners and other stakeholders, and that the data they do have is current and accurate? What are the financial, reputational compliance, or even litigious risks of getting digital identity management wrong?

Once again, according to PwC:

> Systemic changes are helping to bolster organisation's against fraud and other economic crimes. [. . .] But the survey affirms that organizations are now doing the hard work of enhancing technical capabilities and implementing stronger internal controls and reporting measures.[9]

INTRODUCING THE GLOBAL LEI AND vLEI SYSTEM

Over two million legal entities around the world already identify themselves internationally using a LEI. This 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, free of charge. No two LEIs are ever the same. One LEI represents one legal entity. This means that any third party — from a curious consumer to a professional risk manager — 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, efficiencies and transparency to trade of all kinds.

Such broad expansion, of course, would not be possible without addressing some prevailing obstacles that, if unresolved, could inhibit wider LEI adoption. These principally relate to legacy integration issues, costs and the lack of perceived incentives for voluntary adoption of the LEI by market participants.

In its aforementioned report into available options to improve adoption of the LEI,[10] however, the FSB notes that market participants 'considered legacy systems less of an issue' and 'underscored the need to provide use cases to better inform market participants of the benefits of the LEI, which would help to explain why the cost of adapting legacy systems would be warranted.' To this end, GLEIF has been working with leading payments industry stakeholders to publish a variety of use cases that demonstrate the significant value the LEI brings to

non-financial corporates and financial institutions when transmitted in cross-border payment flows.[11]

The FSB report also observes that

> GLEIF, in cooperation with the ROC, has several initiatives to promote LEI adoption more broadly, including bulk LEI registration by intermediaries and business registries — which could both lead to a significant reduction of per capita fees and increase network effects — and additional LEI features that could incentivise voluntary adoption, such as the verifiable LEI (vLEI), i.e., a digitally verifiable credential containing the LEI.[12]

As the FSB noted, 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 identify themselves and verify the authenticity of counterparty organisations digitally. 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 cybersecurity industry. It provides a new, verifiable digital trust layer that sits beneath the conventional information exchanged between supply chain organisations.

GLEIF has designed the vLEI in the form of verifiable credentials, in accordance with the World Wide Web Consortium's open standard verifiable credentials data model. The process establishes GLEIF as the digital 'root of trust' and enables GLEIF to safeguard the integrity of the trust chain. Each vLEI must be issued by a GLEIF-certified vLEI issuer to a legal entity client that has an LEI. Once obtained, the vLEI can be used as a basis to issue additional credentials to members of the organisation.

As a secure digital attestation of a conventional LEI, vLEI credentials can be used in a wide variety of digitalised processes in which company identity verification is a prerequisite.

Prominent among these are digitally signing regulatory filings and reports, verifying business payments, counterparty due-diligence processes, accelerating business entity registrations and securing the remote execution of business contracts.

Together, the LEI and its digital counterpart, the vLEI, can be used to verify the identity of companies, their corporate organisational structures, and their authorised executives, to inform better business decision-making and create enhanced, even automated, risk management practices within increasingly digital corporate ecosystems.

USE CASES: HOW THE LEI/vLEI CAN MITIGATE RISK IN THE REAL WORLD

The opening sections of this paper illuminated the opportunities afforded by the adoption of a universal form of digital organisational identity in relation to enhanced risk management, as financial institutions serving corporate clients increasingly embark on their own journeys of digital transformation. Usefully, the LEI is already gaining recognition and advocacy among banks and financial institutions for the trust, transparency and efficiencies it can bring to existing due diligence processes, such as KYC, anti-money laundering and sanctions screening activities. Yet its potential to open up new opportunities for commercial growth and competitive advantage in a digital future is not yet widely understood, as no catalogue of future-gazing LEI applications has been curated. The use case below has been provided to help promote a better understanding of how the LEI and its digital counterpart, the vLEI, can be used to mitigate real world risk management scenarios that are emerging in line with increasing digitalisation. It sets out the value of the LEI in a digital future, where there is a growing requirement for ESG transparency in financial institutions.

LEI AS A DATA CONNECTOR: THE VALUE TO ESG REPORTING

There are significant variations in ESG reporting requirements from country to country, yet research undertaken by the Swiss Finance Institute[13] supports the notion that mandatory ESG disclosure around the world, enforced through regulation, improves the information environment and has beneficial capital market effects.

The research paper notes the following in respect to a particular challenge faced around the world by investors:

> Environmental, social, and governance (ESG) considerations have become increasingly important

> for investment decisions. Yet investors frequently complain that the availability and quality of firm-level ESG disclosures are insufficient to make informed investment decisions (Ilhan et al. [2022]). In response to the gap between the demand for ESG information by investors and the supply of such information by firms, several countries have initiated mandatory ESG disclosure regulations to force firms to disclose high-quality information on ESG issues either jointly with traditional financial disclosures or in specialized standalone reports. In addition to these country-level initiatives, there are significant efforts at the global level to design, harmonize, and eventually mandate international ESG disclosure standards.[14]

This latter point refers to the establishment of the International Sustainability Standards Board (ISSB) in 2021 by the International Financial Reporting Standards (IFRS) Foundation. According to the IFRS, the ISSB is developing 'standards that will result in a high-quality, comprehensive global baseline of sustainability disclosures focused on the needs of investors and the financial markets.'[15]

So where does the LEI fit in this scenario? Investors seeking responsible, sustainable investments that comply with ESG policies and financial institutions who need to check eligibility for sustainability-linked finance initiatives, are among those who can benefit from the LEI as an ESG data connector. A transparent, current and accurate view of the names, locations and legal forms of subsidiaries, parents and holdings of a company is imperative to fully understand the nature and systemic risks of an investment. As a standardised entity identifier that connects entities to key reference information, including ownership structure, the LEI tackles data reconciliation problems across borders and promotes an interoperable identity standard.

Inclusion of the LEI in ESG tagging makes it easier to find, compare and consume ESG globally for due diligence purposes and KYC processes. By tagging entities with the LEI and using it as an ESG data connector, transparency can be increased for the reporting entity, related companies and even for suppliers. This can mitigate against greenwashing — when, for example, a company claims strong environmental credentials yet fails to disclose a negative impact caused by the combined actions of itself and its supply chain partners — and other misleading practices such as the misallocation of assets, thanks to the 360 degree view afforded by a LEI. Machine readable and relevant across borders (thanks to its utilisation in over 200 jurisdictions), the LEI is a powerful tool for those conducting research on an entity's global strategies, assets, corporate structure and values.

The LEI can further instill trust in ESG reporting if it is embedded within the digital certificate when signing a report and/or the digital signatures or verifiable credentials (vLEIs) of its signing officers. This capability has been demonstrated by GLEIF on multiple occasions in recent years and most recently in the publication of GLEIF's 2021 annual report.[16]

In 2021, the Sustainability Accounting Standards Board (SASB) released its Standards XBRL (eXtensible Business Reporting Language) taxonomy[17] for companies which have reporting obligations under the european single electronic format (ESEF) reporting guidelines. This included the recommendation to use the LEI in its XBRL taxonomy — despite the taxonomy remaining identifier agnostic overall. While not binding, the recommendation to use the LEI in XBRL reporting supports the quest for standardisation and compatibility in global ESG reporting, as use of the LEI in XBRL reports will enhance machine readability as well as the comparability and useability of the collected data. It also provides a digital solution for tagging company information at a global level to help build a smooth and efficient ESG taxonomy value chain.

Other supervisors have already recognised the LEI's value in non-financial reporting. For example, the Eurosystem highlighted the importance of the LEI for linking financial and non-financial information and other data sources in its response to the European Commission's public consultations on the renewed sustainable finance strategy and the non-financial reporting directive review. Eurosystem also emphasised that the LEI would enable digital-age innovation and thus foster potential growth in new markets and reduce costs and operational risks of the reporting entities.

WHERE TO BEGIN: PRACTICAL STEPS TO INTEGRATE THE LEI INTO RISK MANAGEMENT PRACTICES

Risk managers in financial institutions keen to realise the value of integrating the LEI into their risk management practices can consider the following recommendations.

1) They should ensure that their headquartered financial institution, together with all their associated legal entities, are appropriately registered in the Global LEI System. This will enable clear and unambiguous verification of the institution's public footprint and its legal entity structure. The financial institution should also ensure that all related LEIs are conforming to Regulatory Oversight Committee (ROC) policy and consider managing their LEIs centrally to ensure that relationship structures (accounting consolidation parents, funds and branches) are accurately represented in the Global LEI System. This is important to the regulatory officials referencing the institution via its LEI in regulatory reporting. It is also important to private counterparties for trades and transactions which reference the institution via its related LEIs.
2) The financial institution should require the members of its client and supplier networks to obtain and maintain LEIs in accordance with ROC policy. This will provide transparency in reporting which, as has been explored, is important to ESG. If an institution is serious both about knowing its suppliers and about making this information available to the world, it should require its supplier to provide a conforming LEI and incorporate this information in public reporting and regulatory filings. These practices not only mitigate operational risk, but also reputational risk. Knowing precisely who your suppliers are and enabling full visible access to this information will shield the institution against negative misinterpretations regarding its operations globally.
3) Risk managers can also consider incorporating the LEI into their client onboarding practices. Ensuring that legal entity clients are 'tagged' with the LEI at the time of their account opening allows the institution to automate notifications of updates to important client information, like operating status and parent structure, ensuring it stays fully across the ever-changing nature of its client base.

A TRUSTED, OPEN AND GLOBALLY ESTABLISHED SYSTEM FOR MANAGING RISK IN THE DIGITAL AGE

Under GLEIF's stewardship, the Global LEI System has, for years, been providing open and reliable data, enabling the unambiguous identification of legal entities to financial institutions, regulators and other organisations around the world.

With well over two million LEIs now in use, GLEIF is building on its success by driving voluntary LEI adoption among legal entities across all industries globally, to establish the LEI as the world's *de facto* system of digital organisational identity.

A vital component in this mission is helping operational and transaction-oriented risk managers in financial institutions mitigate client risk so both their institutions and their clients may participate efficiently in the world's digital economy. Speed is a vital factor for all involved. New business models and newly automated processes are springing up all the time, fuelled by myriad advances in technology, from application programming interfaces, to blockchain, to Internet of Things.

Against this backdrop, it is easy to see why digital trust is in short supply, yet this is precisely what is needed. When legal entities digitally engage with their customers, partners and suppliers, they must be able to trust that these organisations are, indeed, who they claim to be, and when financial institutions onboard and engage with corporate clients operating digitally, they too must be able to assess the context in which they do business.

The creation of digitised trust, therefore, is central to GLEIF's ongoing work. GLEIF's belief is that each legal entity worldwide should have just one global identity capable of supporting its participation in the digital economy. Only then can everyone, inclusive of the world's financial institutions, work together in ways that can mitigate risk without curtailing momentum. Then the true potential of digitalisation/digitisation can

be unlocked: enabling innovation and collaboration to thrive unlimited by geography, and that finance, investment, goods and services may flow securely around the world faster, more efficiently and at a lower cost than ever before.

References

1 Financial Stability Board (7th July, 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 8th November, 2023).
2 Financial Stability Board (13th October, 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 8th November, 2023).
3 Price Waterhouse Coopers (2022) 'PwC's Global Economic Crime and Fraud Survey', available at https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (accessed 8th November, 2023).
4 African Development Bank Group (2020) 'Trade Finance in Africa: Trends Over the Past Decade and Opportunities Ahead — Policy Research Document 3', available at https://www.afdb.org/en/documents/trade-finance-africa-trends-over-past-decade-and-opportunities-ahead (accessed 8th November, 2023).
5 Price Waterhouse Coopers, ref 3 above.
6 IDC (2023) 'GLEIF & 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 8th November, 2023).
7 Price Waterhouse Coopers, ref 3 above.
8 *Ibid*.
9 *Ibid*.
10 Financial Stability Board, ref 1 above.
11 GLEIF (2023) 'LEI in Cross Border Payments', available at https://www.gleif.org/en/lei-solutions/featuring-the-lei/1-cross-border-payments (accessed 8th November, 2023).
12 Financial Stability Board, ref 1 above, p. 1.
13 Krueger, P. (2021) 'The Effects of Mandatory ESG Disclosure Around the World', *European Corporate Governance Institute – Finance Working Paper No. 754/2021, Swiss Finance Institute Research Paper No. 21-44, SSRN*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3832745 (accessed 8th November, 2023).
14 Ihan, E., Kreuger, P., Sautner, Z. and Starks, L. (2023) 'Climate Risk Disclosure and Institutional Investors', *The Review of Financial Studies*, Vol. 36, No. 7, pp. 2617–50, available at https://academic.oup.com/rfs/article/36/7/2617/6978207#408732790 (accessed 15th November, 2023).
15 International Financial Reporting Standards (IFRS) Foundation (2021) 'About the International Sustainability Standards Board', available at https://www.ifrs.org/groups/international-sustainability-standards-board/ (accessed 8th November, 2023).
16 GLEIF (2022) 'GLEIF Annual Report 2021', available at https://www.gleif.org/en/about/governance/annual-report (accessed 8th November, 2023).
17 SSAB Standards (2021) 'SASB XBRL Taxonomy', available at https://sasb.org/blog/sasb-standards-xbrl-taxonomy-now-available-for-public-use/ (accessed 8th November, 2023).