

**Finance and Economics Discussion Series
Divisions of Research & Statistics and Monetary Affairs
Federal Reserve Board, Washington, D.C.**

**Identity, Identification and Identifiers: The Global Legal Entity
Identifier System**

Arthur B. Kennickell

2016-103

Please cite this paper as:

Kennickell, Arthur B. (2016). "Identity, Identification and Identifiers: The Global Legal Entity Identifier System," Finance and Economics Discussion Series 2016-103. Washington: Board of Governors of the Federal Reserve System, <https://doi.org/10.17016/FEDS.2016.103>.

NOTE: Staff working papers in the Finance and Economics Discussion Series (FEDS) are preliminary materials circulated to stimulate discussion and critical comment. The analysis and conclusions set forth are those of the authors and do not indicate concurrence by other members of the research staff or the Board of Governors. References in publications to the Finance and Economics Discussion Series (other than acknowledgement) should be cleared with the author(s) to protect the tentative character of these papers.

**Identity, Identification and Identifiers:
The Global Legal Entity Identifier System**

November 8, 2016

Arthur B. Kennickell
Advisor
Board of Governors of the Federal Reserve System
Washington, DC 20551
Arthur.Kennickell@frb.gov

The views expressed in this paper are the views of the author alone and they do not necessarily reflect the views of the Board of Governors of the Federal Reserve System or its staff, or any part of the Global LEI System. I am grateful to my colleagues on the LEI Regulatory Oversight Committee and its predecessors, the board members and staff of the Global LEI Foundation, as well as numerous other public spirited people who contributed their time to develop and guide the Global LEI System. I am particularly grateful to Stephan Wolf for comments. I am solely responsible for any errors or omissions.

Identity is a critical concept in the rational interactions of any set of objects involving subject-object relationships. The objects must be distinguished according to some framework in order for such relationships to have meaning. In the world of economic systems, relationships such as ownership and responsibility require specific parties to be fixed with a high degree of certainty. This need is particularly strong in financial markets, where transactions can take place in nanoseconds. This paper discusses a particular framework for defining economic actors, the Global Legal Entity Identifier System (GLEIS), which was initiated for the purpose of creating greater transparency about participants in financial markets and transactions. The views expressed in this paper are mine and do not necessarily reflect those of the Federal Reserve Board or its staff.

As discussed in more detail below, the GLEIS follows from a G20 initiative to address fundamental problems related to identification that arose during the recent financial crisis. This system was constructed in stages, starting from an investigation under the leadership of the Financial Stability Board (FSB) of the relevant theoretical, practical and political constraints. Following from that start came the development of an international charter of cooperating authorities, the elaboration of operational principles, and ultimately the unfolding and elaboration of an operational structure under a Swiss foundation created for that purpose.

As background for the discussion of the GLEIS, the paper addresses the most important conceptual issues related to identity, identification and identifiers. At a high level, these concepts are equally applicable to both natural persons and non-personal entities, though there are also fundamental differences.¹ To support intuition, the paper begins with a discussion of the case of natural persons and then develops more details in the context of non-personal entities. The ideas highlighted provide a framework for understanding the choices made in creating the GLEIS as a practical system of identity management for entities. The discussion also probes points where any such system might have weaknesses.

There is no pretense here that the discussion covers every aspect of identify, identification and identifiers. From John Locke [1690] onward, a large literature has developed on issues around identity, some of which reaches into very rarefied questions of existence or interpretation of

¹ Identifiers for other types of objects are not considered here, but many of the same issues are involved.

reality. This paper purposely glosses over such fine elemental points, except where relevant to the goals of the paper.

I. Natural persons

As applied to a natural person, the broad concept of *identity* is potentially very complicated, involving the subjective views of the person about their distinct existence and their connections to ideas, groups and various other attributes—as well the views of other persons, systems or mechanical processes that may classify the person or distinguish the person from other persons. The process of *identification*, as the term is used here, classifies a person according to a set of criteria appropriate to a given context, and often at the most atomic level as a person distinct from all others. The identification may be determined at a given point in time, or for many points in time, given an underlying concept of what it means for a person to be “the same” at different times. It is such specific and persistent identification that is relevant for this paper.

Specific identification assumes first that there is an appropriate distinction between a person and not-a-person, as well as a distinction among persons. For purposes of this paper, it is most relevant to concentrate here on the inherent physical reality of a person. Outside of exceptional situations, an individual living person is easily distinguishable by observation as separate from other living persons. Thus, in principle it is possible to think of a persistent virtual envelope around the physical body of a given person and thereby formally distinguish the person from all others, even if parts of the person become separated (or parts are added) or the person otherwise changes size or condition over time. Such a distinction identifies the elements of the relevant set of persons in a persistent way. But it does not specifically distinguish among persons, outside the moment of observation.

A more specific and persistent identification requires matching attributes of a distinct physical person with a set of recorded information taken to be sufficient to define a person uniquely in a given context. Such information might be defined in terms of attributes directly connected to the physical reality of the person or attributes that reflect choice (e.g., “I see he is a distinct person, he says his name is Leif Xanthophyll and he lives in Philadelphia; because I believe he is telling the truth and there is only one Leif Xanthophyll recorded as living in Philadelphia, I conclude he is the specific person identified by the record.”).

Problems in such identification may arise for three principal reasons. First, scope limitations in the set of attributes recorded for matching may lead to incorrect or ambiguous identification (e.g., “One Leif Xanthophyll lives on Lombard Street in Philadelphia and another lives on Luzerne Street, but the recorded attributes do not include the street name.”). Where it is known that the entire population of individuals has been subjected to a common framework of identification, it is a theoretical possibility to verify the uniqueness of each set of values of the recorded attributes. In the common situation where the entire population is not recorded, there may be a risk of non-uniqueness of identification.

Second, the attributes of a person to be identified may be observed from the person with error (e.g., “He says he is the unique Leif Xanthophyll recorded as living in Philadelphia, but he is lying.”). Careful observation and quality management as well as legal or similar compulsion to reveal the truth about some attributes may reduce the potential for such error. Where there is no constraint on implementation, attributes that have a minimal error rate in their association with a unique person, such as iris scans, could be used. However, privacy concerns, legal constraints, costs and other practical considerations may limit what can be collected or maintained as attributes or that may be applied in practice.

Third, the relevant set of reference attributes may be recorded or maintained with error, so that an incorrect match or no match is made (e.g., “There is a Leif Xanthophyll recorded as living in Philadelphia, but the only Leif Xanthophyll actually lives in Yellow Leaf, not Philadelphia.”). Systematic revalidation of recorded attributes, perhaps by periodic direct comparison with the attributes of the person, may reduce the level of such error. Depending on the relevant institutional structure, some identifying attributes may change, yet the identification process may still remain informative about the correspondence of the person and a record of attributes (e.g., “Leif Xanthophyll, always a joker, changed his name to Godzilla Xanthophyll; the record for the former Lief Xanthophyll needs to be updated.”). The validity of the concept of updating for addressing incorrect or stale information depends on support in the institutional structure for a concept of ownership or responsibility (such as an official record of a change of name), supported as necessary by an acceptable method of authentication (perhaps by a certification process or via access control using an alternative private code, such as a password). It may also be that the available attributes contain more than one subset of information that could be

considered independently sufficient for identification (again for example, iris scans, in addition to other demographic information, such as an address), thus allowing a logical support for updating the incorrect attributes.² Such subsets of the identifying information might be virtually absolute in their connection with a specific person, or the connection might be true with a level of probability. If the more nearly absolute attributes are relatively costly or difficult to evaluate, it may be sensible to include an array of less rigorous attributes that are almost always sufficient and to save use of the relatively absolute attributes for situations where the identification is otherwise ambiguous or where updating is necessary.

Normally, it would be considered very inefficient if detailed comparison of the entire set of relevant attribute information were necessary to achieve identification every time it might be required. An alternative is to undertake identification once, and to assign a unique and persistent label to a person. For example, a U.S. social security number is assigned based on an array of identifying information and it is (intended to be) unique to a particular person). A unique *identifier* is a type of formal label or pointer for which a value or code of some sort is assigned uniquely and exclusively (one and only one assignment) to a person specified by a unique combination of values of the relevant underlying identifying information.³ The identifier itself may be considered as a special type of attribute. In some cases it may contain specific information about the person identified (e.g., in most cases, the first three digits of a U.S. social security number reflect the location where the person was born.).

Generally, the most important use of an identifier is in connecting multiple sources of information that do not necessarily contain all the information required for primary identification, and doing so without direct intervening reference to the relevant physical person. If all the sources contain a common identifier, it may provide a more straightforward or efficient means of identifying sets of information about a specific person than separately collecting and maintaining identifying attributes, filtering across them in all sources to be connected and validating their applicability in each instance. For example, the U.S. Internal Revenue Service connects all income and tax information for a person through the use of a social security

² For example, multi-factor authentication, such as tokens in addition to passwords, might be appropriate in some situations for sufficiently reducing the probability of error.

³ For example, for the Aadhaar code for personal identification in India, the identifying information includes finger prints, iris scans, photographs and other demographic information. See <https://uidai.gov.in/>.

number.⁴ Obviously, for such linking to be meaningful, it is critically important that the initial association of the identifier with each record of information be reliable and that it be subsequently maintained through a chain of control.

The virtual envelope around a person is persistent, but over time the association of an identifier with a specific individual may become corrupted to some degree, lost or otherwise untrusted, either because the underlying identification process fails or because the identifier itself becomes corrupted in some way. In principle, it must always be possible to validate that the recorded attributes underlying an identifier continue to correspond to a specific person. The persistence of an identifier as a reliable mode of identification rests on the supporting institutional structure, the extent of redundancy in the identifying information, and the possibilities for other types of error. The possibilities for accidental or deliberate error are discussed further below for the case of entities.

In practical applications, there are many questions to be answered about when a degree of error or probability of error may overwhelm the usefulness of a set of attributes in identifying a person uniquely; often a perfect solution is not possible, so minimizing error within the existing constraints becomes important.⁵ For practical purposes, an identifier will not be used if there is insufficient confidence in the reliability of its association with a specific person. Confidence is supported by two factors. First, there must actually be an acceptable minimization of error within the domain of intended use. Second, transparency is needed about the limits of a given

⁴ There may be intermediate approaches, such as in the case of a passport, which can be taken as a sort of portable identification system. To obtain a passport in the past, the applicant was required to provide documentation of eligibility (leaving aside the question of how the legitimacy of that material might be assessed) and to supply a photograph. Passports are designed to be difficult to fabricate, thus tightening the connection between the photograph included and the chain of documentation supporting the issuance of the document. In direct personal use of the passport, visual inspection of the photograph and the person holding the passport was judged sufficient for the purpose of identifying the holder. Subsequent incorporation of nearly unique biomarkers, such as finger prints and iris scans, makes fabrication more difficult, but if the biomarkers of the passport holder are assessed only relative to the information contained in the passport, for example in a chip, there is no logical difference from use of a photograph alone, because either might be forged in the physical document. A passport also contains a unique number which may be used as an identifier in data on instances of direct personal use of the passport.

⁵ There may be errors of a “minor” sort that do not fundamentally affect the interpretation of the identifying information. For example, “111 E. Luzerne Street” would not normally be taken to be meaningfully different from “111 East Luzerne Street”, even though one of those versions may be considered the “official” version by some standard. In contrast, “111 East Luzerne Street” and “111 West Luzerne Street” might be expected to be considered meaningfully different. The level of acceptable ambiguity depends on the background against which the information is viewed and the sensitivity of the purpose for which it is used.

approach, in order to allow users to judge for themselves whether their specific uses might require additional effort to identify a particular individual to a higher degree of certainty.⁶

II. Non-personal entities

Non-personal entities (referred to here as simply “entities”) are artificial objects socially constructed according to law, regulation, or convention to perform some function.⁷ The process of identification for entities raises most of the same general issues as the identification of persons. A significant difference is the range of possibility or difficulty in defining a persistent virtual envelope to contain a distinct entity. Direct physical reality does not necessarily offer a straightforward means of distinguishing an entity (for example, a fund). Sometimes the essence of an entity may have very little extent in the physical world, other than a notation of its existence or the traces of its actions. Legal personhood or similar legal, regulatory, administrative or other formal constructions may serve to define the identifiable essence of a particular entity at a given point in time.

Unlike the case of physical persons, the temporal persistence of the resulting virtual envelope, also may be more questionable for entities. This impermanence has implications for the definition of a consistent set of entities across time as well as the continuity of individual entities. An entity may change fundamental composition over time via corporate actions such as mergers and spin-offs or undertake basic changes of internal structure or function, leading to complex questions about what it means to be “the same entity” at various points in time. Moreover, in some jurisdictions a simple change of ownership of an entity that remains otherwise exactly the same is treated legally as a new entity, thus further calling into question the connection between even the physical reality of an entity and its legal embodiment. For some purposes, it may be possible to define specific information or a framework to track the composition of an entity sufficiently over time. As an extreme example, an entity might be pre-programmed by contract or other form of obligation to disintegrate in some way; there are many possible definitions of the relevant entity in this case, including one that encompasses a reference to the contractual

⁶ Even when the tolerance level is not always met for a very sensitive use, such as identifying blacklisted individuals, the identification may still be helpful if the association of the person and the identification process is sufficiently tight that it is only additional information (such as knowledge of a person’s association with a specific group), not a different and more rigorous core process, which would be required.

⁷ Such entities could range from the arrangement whereby an individual engages in a business activity to more complex forms, such as publicly traded corporations or state-owned enterprises.

nature of the disintegration from a specific initial state. In some cases, it might be sufficient to use data to track complete or fractional antecedents and successors of entities up to a level of materiality appropriate for a given set of uses.

Ideally, the identifying characteristics of an entity should be as closely connected as feasible to the legal, regulatory or other administrative construction that specifies the existence and extent of the entity. In some jurisdictions or situations, an entry in a business register may serve this function. In other situations, such information may be unavailable or unreliable and other identifying information would be required.⁸ The question of the sufficiency of identifying information for entities is addressed further below.

As in the case for natural persons, a unique identifier for an entity requires an unambiguous and exclusive assignment of an identifier to a single entity, based on a reliable process of identification. To be more than a trivially useful decoration, it should be either the sole sufficient information, within the tolerance of a given use, to make unique connections among different sources of information. For that reason, it is important to consider how an identifier, once assigned to an entity, might become associated with a given process or set of information and what limitations may apply.

An identifier in sets of information to be matched might have been provided originally by the authority of the entity itself, or it might follow from an earlier “chain of control” of other information that includes the identifier. It might also be “derived” by identifying a set of attributes associated with one identifier with comparable attributes in another source associated containing a different (or no) identifier; this approach is commonly referred to as “mapping.” Such mapping is commonly performed once and revised only if there is a conflict in terms of the definition of an entity or its survival in the separate systems (e.g., two data systems might differ in standards for determining when an entity becomes a new entity, following its sale). Note that mapping is a type of identification and thus it is subject to the same sorts of qualifications as identification in general.

⁸ An additional means of identifying an entity might be via its relationship to other entities in an organizational structure or its connection to corporate officers or other individuals. In that sense, identification of larger organizational structures, rather than just entities, might provide more precise identification as well as supporting broader understanding of actions taken by or performed on entities.

If the process for including an identifier in a given process or information set were perfectly controlled, the supporting identifying information for the entities associated with the identifier would not even need to be available. The usefulness of a reported identifier in practice turns on how close the practical situation is to this ideal, the possibilities for fast and inexpensive partial checking (for example, the identifier in conjunction with some other set of shared information), and the costs or risks from using or maintaining an erroneous identifier in the context of a specific set of uses.

Errors may occur in reports of an identifier for either accidental or intentional reasons. Accidental errors fall into three general types: chain-of-control errors, transcription errors and association errors. Chain-of-control errors may occur when procedures for assigning or propagating an identifier unintentionally contain an error (or where an error or other defect in associated security arrangements allows for corruption of the identifier); systematic testing (and security analysis) may minimize the likelihood of such errors.

Transcription errors in reports of an identifier may be controlled at a formal level through the use of check digits (e.g., ISO 7064). It is also possible that use of long and seemingly meaningless alphanumeric identifiers might increase the likelihood that reporters would use a mechanical process to refer to the identifier, rather than manually specifying the identifier. In this way, the possibility of multiple transcription errors could in principle be reduced to the possibility of a single error in the reference source, to which quality assurance procedures might more economically be applied.

Association errors occur as a result of misunderstanding which is the relevant identifier for an entity in a situation where its identity must be represented by an identifier. Where the data or process involving the reported identifier results in a transaction or other definitive action directly affecting an entity erroneously associated with the identifier, there would often be a built-in incentive to correct the information, if only at a point after the action has taken place—such as in the resolution of market trades that fail due to improper identification. Some such errors may be a result of confusion created by errors or by actual or perceived insufficiencies in the underlying identifying information associated with the identifier.

Intentional errors in the reporting of an identifier may occur when there is a deliberate effort to disguise the true identity of an entity or where a supposed entity does not in fact exist.

Deliberate reporting of a nonexistent value of an identifier is, in principle, straightforward to detect by searching the universe of the given identifier. Much more difficult to detect are situations where such errors occur by the masquerading of an entity under the identifier of another existing entity or by exploiting an identifier associated with a fabricated identity for a nonexistent entity. As in the case of accidental association errors, errors through masquerading at least can be expected to be detected at the point where an action affects the entity truly associated with the identifier, though this resolution may be much too late to be of practical use in cases of fraud. Masquerading may be limited by requiring multiple sources of authentication. Fabrication may be minimized by a rigorously enforced process to require proof of existence when an identifier is assigned, and by regular monitoring to ensure that the entity continues to exist and the identifying information remains sufficiently correct.

III. The Global Legal Entity Identifier (LEI) System

Following the financial crisis beginning in 2008, the G20 pointed to a variety of defects in existing systems for the identification of entities and called for the creation of new and globally oriented identification system.⁹ Responding to the request, the Financial Stability Board assembled a global set of financial regulators, international organizations and other experts to develop a set of principles and requirements necessary for a new identification system. From that work came a rigorous conceptual framework and an implementation plan, supported by a governance model designed to ensure the highest quality of information feasible globally, promote transparency, and secure the broad public interest for the long term.¹⁰ This system became the GLEIS. The organizational structure of the GLEIS consists of a federated group of registrars, Local Operating Units (LOUs); a central operational body, the Global LEI Foundation (GLEIF); and a regulatory body charged with oversight of the GLEIS, the Regulatory Oversight

⁹ “We support the creation of a global legal entity identifier (LEI) which uniquely identifies parties to financial transactions. We call on the FSB to take the lead in helping coordinate work among the regulatory community to prepare recommendations for the appropriate governance framework, representing the public interest, for such a global LEI by our next Summit.” Declaration of the 2011 G20 Cannes Summit, <http://www.g20.utoronto.ca/2011/2011-cannes-declaration-111104-en.html>.

¹⁰ See Financial Stability Board [2012]. This report was endorsed by the G20 at its 2012 Los Cabos Summit (“We endorse the FSB recommendations regarding the framework for development of a global legal entity identifier (LEI) system for parties to financial transactions, with a global governance framework representing the public interest. The LEI system will be launched by March 2013 and we ask the FSB to report on implementation progress by the November 2012 Finance Ministers and Central Bank Governors’ meeting. We encourage global adoption of the LEI to support authorities and market participants in identifying and managing financial risks.” See <http://www.g20.utoronto.ca/2012/2012-0619-loscabos.html>.)

Committee (ROC). The governance model is described in more detail in the annex. For a more detailed discussion of governance and its importance, particularly for acceptance of the GLEIS in a regulatory context, see [Couillault, Mizuguchi and Reed [2016]].

Virtually any practical system of identification faces a variety of limitations, particularly if the objects to be identified may be difficult to make entirely (and permanently) unambiguous and if the system must operate within the finite resources of a business model that supports it. Ideally, precision should be maximized according to criteria appropriate to a set of motivating use cases, subject to the relevant constraints. Where ultimate precision is not feasible, transparency about any general limitations or limitations specific to particular entities is highly desirable. Where such a system is created without an exact pattern to copy, careful account must be made for the possibilities of overwhelming complexity, and the implementation path should be structured to support learning-by-doing and resilience in the face of unanticipated disruption. Finally, there must be a practical means of including the objects to be identified by the system. These are some of the most pressing practical complications against which the GLEIS unfolds.

As discussed above in general, the degree of abstraction involved in defining the identity of an entity may raise questions beyond those that apply in the case of a person. The problem is further complicated in practice by the variation globally in relevant legal, regulatory and administrative structures that might give definition to an entity, as well as the available type and quality of information associated with such a definition that might be used to confirm the existence of the entity and the validity of reports of its identifying attributes.

In developing the LEI, a broad consultation took place with experts from academia, the financial industry, regulators and others to consider the information necessary for unique identification of an entity in a global context. The International Organization for Standardization (ISO) 17442 standard developed in this process was adopted as the core identification framework for the LEI.¹¹ The standard specifies the high-level definition of the identifier code, an indication of the scope of coverage, and the information required for identification. The standard does not provide further specific guidance on implementation; for that reason, the governance structure for the implementation is particularly important.

¹¹ See International Organization for Standardization [2012].

The LEI code required by the standard is a 20-character alphanumeric string embedding no persistent information about the entity associated with it.¹² To support avoidance of transcription errors or other corruptions, the LEI incorporates two terminal check digits.¹³ Once issued, a given value of an LEI should never be issued to another entity, thus supporting the uniqueness of an LEI. No given entity is permitted to obtain more than one LEI, thus supporting exclusivity of assignment of the LEI. The LEI code and supporting data are persistent in the sense that the underlying entity may expire or it may allow its registration to lapse, but the LEI and the most recently obtained information should, in principle, be available in perpetuity.

In its discussion of the scope for the LEI, the language in the ISO 17442 standard does not restrict eligibility to entities with legal personality. For example, among the illustrations of eligible entity types given in the standard are umbrella structures and their sub-fund components, the latter of which are a type of quasi-entity.¹⁴ The standard focuses on parties that have responsibility for financial transactions or the ability to enter independently into contracts, but it also notes that coverage is not necessarily restricted even to such parties. Only natural persons are explicitly excluded under the standard.¹⁵

In considering a more specific practical definition of entities eligible to receive an LEI, there are three important considerations. First, to maintain the logical coherence of the GLEIS, an eligible entity must have a physical, legal or administrative definition that distinguishes the entity sufficiently clearly, distinctly and persistently as long as it continues to exist. Second, to avoid ambiguity of reference, any eligible sub-entity element within another type of entity eligible to obtain an LEI (for example, a sub-fund and an associated umbrella fund) must also have a similarly unambiguous way of defining the place of the sub-entity within the containing entity,

¹² In general, the first four digits of an LEI generally represent a prefix associated with the initially issuing LOU. The prefix is used only for operational convenience. Because the maintenance of the data for any LEI may be transferred across LOUs, there is no necessary connection between the prefix and the issuer subsequent to issuance of the LEI.

¹³ The two LEI check digits are determined by applying the MOD 97-10 method given in ISO 7064 to a concatenation of the first 18 component numbers and letters mapped to numbers (as given in ISO 17442).

¹⁴ Most typically, the umbrella entity would have legal personality, while its component the sub-funds would not. However, the sub-funds would generally have ring-fenced assets and liabilities. Protected cell companies are a similar type of organizational structure.

¹⁵ As noted earlier in the paper, identification of natural persons and of entities raise different issues. Generally, the relevant identifying information would be substantially different. Thus, it might be more straightforward to treat each under a separate standard. However, there is a gray area between entities and natural persons that is addressed by the LEI, as described in the text.

as well as a means of associating the entity and the sub-entity. Third, to be feasible, there must be an acceptable means of validating the existence and attributes of the entity, which can be supported by the underlying business model.

Clearly a wide variety of legal forms, such as public corporations, fall within this scope of eligibility. Following additional analysis, the ROC determined that two types of entities in the gray area left by the standard should be considered in scope for LEI eligibility. First, the ROC recognized that natural persons may act in a business capacity distinct from their personal capacity; in some cases, regulations specifically characterize such actions within the definition of reportable business activity. Under conditions aimed at ensuring that there is sufficiently clear evidence of business activity, as distinct from purely personal activity, the ROC explicitly allowed the possibility for such individuals to receive an LEI.¹⁶ This limited extension allows for accumulating experience in coping with potential privacy issues for such individuals, particularly in situations where a registered individual may subsequently cease to act in a business capacity.¹⁷

Second, the ROC recognized that there is a spectrum of potential sub-entities beneath a given legal entity (such as branches or other organizational units defined internally on an administrative basis) that may have relevance for regulatory or other practical purposes. International branches or a legal entity sometimes may be taken to be an edge case between strictly defined legal entities and a broader set of possible sub-entities. In particular, under some legal or regulatory structures, an international branch of a legal entity may be subject to constraints or regulatory requirements independently of its containing legal entity that are similar or identical to requirements imposed on domestic legal entities. Moreover, such branches may have a “contingent legal entity” aspect, in that certain types of bankruptcy situations would require jurisdiction-specific ring fencing of international branches. In order to address compelling regulatory needs, the ROC explicitly recognized international branches as being eligible to receive an LEI, subject to conditions to ensure the quasi-entity nature of the branch

¹⁶ Eligibility in this case turns critically on the presence of such an individual in a type of business register.

¹⁷ The LEI and its reference data should persist indefinitely, but there is some question about whether the historical data on an individual acting in a business capacity might become personal data when the person ceased such activity under some jurisdictional frameworks.

and to support its linkage with the containing legal entity.¹⁸ Because the number of international branches potentially relevant appears to be relatively small, this step allows for the exploration of potential issues surrounding the inclusion of sub-entities, while limiting the risks to the GLEIS.

Part of the mission of the GLEIS is to remain flexible in identifying entities that are relevant for regulatory purposes, a potentially very broad range of possibilities.¹⁹ However, unrestricted extension of scope to include additional classes of individuals might heighten fears about privacy and possibly even evoke political reactions. Unrestricted extension of the LEI scope to additional types of sub-entities could raise both the possibility of introducing logical or operational complexity (not least because definitions of such sub-entities are often idiosyncratic and the persistence of such objects over time may be unclear) and questions about the business model to support such an extension (particularly the effort that might be necessary to validate information about structures with idiosyncratic or unclear definition). It is important that any further extensions bear in mind these and other potential risks.

The information deemed necessary and sufficient for identification depends on the types of entities to be identified, as well as the intended uses.²⁰ The broad discussion that led to the adoption of the ISO 17442 standard considered the minimal set of information necessary in a global context to identify an entity, against a background of intended general use for market transactions and regulatory reporting.²¹ As the standard was implemented, the informational requirements were further elaborated and extended.²² For example, the name and address of the entity are required to be provided in the local character set relevant for the entity and additional provision is made for including transliterated names given in non-Latin character sets and for names used for other purposes. When it is implemented, the new ISO 20275 standard on entity

¹⁸ As with the case of individuals acting in a business capacity, a critical constraint on eligibility for an international branch is that it must be recorded in a type of business register.

¹⁹ Among other things, Recommendation 5 of FSB [2012] requires that “Flexibility must be built into the global LEI system to provide the capability for the system to expand, evolve and adapt to accommodate innovations in financial markets. It must also allow the seamless introduction of new participants.”

²⁰ In a world where perfect identification is either impossible or unmanageably costly, some degree of approximation is necessary. As noted earlier, the approximations should be optimized for the motivating use cases, as was done for the LEI. In general, other uses might require additional information or a different process for the chain of control of information.

²¹ The resulting core set of “business card information” includes the official name of the entity, the legal address, the headquarters address, and, where relevant, the business register where the entity is recorded. The information specified under the standard also includes the date of assignment of the LEI, the most recent update of the information, and, where relevant, the reason the entity has ceased to exist and its legal successor.

²² The ISO Standards Advisory Group with oversight of ISO 17442 provided very helpful comments at this stage.

legal form, developed at the behest of the ROC, will provide a standardized expression of entity legal form in the LEI records.²³

Unique identification of some types of entities eligible for an LEI may require additional or different information.²⁴ For example, in the initial implementation of the LEI for funds, it was recognized that owing to ambiguous naming conventions common in some jurisdictions, a given fund might be difficult to distinguish from others, without an indication of the entity managing the fund or the name of the fund family; to address this limitation until a more refined solution could be developed, an additional element was added to the basic LEI data. Any extension of LEI scope, such as to include additional types of individuals, sub-entities or other currently unrecognized types of entities would also require a corresponding examination of the information required for identification and a consideration of what systematic linkage with eligible entities related in a relevant sense might be required, as discussed below.

An entity enters the GLEIS by contacting an LOU to register for an LEI, generally through an online portal. The entity is responsible for providing the required identifying information, along with evidence that the person submitting the registration is authorized to do so on behalf of the entity. Only an official of the entity or a specifically designated third party may provide the information.²⁵ Acquiring information in this way is believed to result in higher quality information than alternatives relying on less formal and transparent methods that do not systematically involve the entity itself.

LEI issuance has an associated validation process intended to ensure there is evidence that an applicant actually exists as an entity and that the attributes captured correctly reflect the situation of the entity. The LOUs perform the validation, using authoritative public sources, such as business registers, when they are available and of sufficient quality. When only authoritative private sources (such as an official record of incorporation or a fund prospectus not available for reference from local public authorities) are available, the information may still be acceptable.²⁶

²³ The LEI record also contains a variety of status indicators and operational flags.

²⁴ Note that LOUs may use information beyond the data published in an LEI record to verify the existence of an entity and its complete alignment with the information collected at the point of registration.

²⁵ Payment for registration is viewed as traceable and contributing evidence supporting the identification of the person registering to the entity.

²⁶ To be accredited under in the GLEIS, LOUs are required to have expertise in local conventions sufficient for them to be able to judge what information is meaningful and to use the information appropriately in validation.

In the interest of transparency, the level of identification is explicitly flagged in the published data. Following an upcoming revision, the specific official sources used will be listed, using a standardized list of sources. If a supposedly authoritative source and the entity disagree about any aspect of the reported information, it is the responsibility of the LOU to reconcile the differences with the entity. This rigorous and explicit approach to the chain of responsibility for the information and the transparency in reporting for the LEI stands in strong contrast to many commercial approaches to identification.

The GLEIF maintains an evolving set of quality assurance techniques to ensure the initial and on-going quality of LEI data. Quality standard may be seen as more difficult to uphold uniformly in a federated system of registrars. To address this potential problem, the GLEIF is in the process of negotiating contracts with each of the LOUs, specifying required service levels and specific quality standards, and retaining the right to conduct a more intensive audit. In the steps leading to the signing of the contract, each LOU must go through a process of accreditation, in which it reveals the details of its approach to the GLEIF. Requirements for transparency about validation sources noted earlier also serve to increase the level of certainty that appropriate validation has been conducted.

The GLEIF itself operates under the ISO 20000 standard, which includes requirements for a focus on continuous improvement.²⁷ The continuous improvement model is particularly relevant in complex systems, such as the GLEIS, where the implications of decisions often can only be seen clearly through learning-by-doing.

Given the required validation process for LEI issuance, the level of error in the initially published LEI reference data should be minimal, but facts may change over time.²⁸ Publication of the LEI data as open data allows for review by any interested party. Users of the data discovering an error may file a “challenge” to the information provided about an entity, either on the website of the relevant LOU or centrally on the GLEIF website. The LOU managing the information for the entity is obliged to investigate and resolve the claim. Experience in open data systems suggests that a challenge system can be a very important tool for maintaining data

²⁷ The GLEIF publishes regular reports on the quality of the GLEIS data at <https://www.gleif.org/en/lei-data/gleif-data-quality-management>.

²⁸ The GLEIS itself does not yet monitor information such as corporate action feeds to detect relevant probable changes in the status of an entity or its reference data. Such review may be expected as the system continues.

quality. In addition, entities are expected to update their information as relevant changes occur, and once a year they should formally recertify the accuracy of their information. The registration of an entity that fails to recertify its data is marked as “lapsed”.²⁹

To this level of definition of the GLEIS, it is simply a logical model for implementation that respects key theoretical principles outlined earlier in this paper, incorporates means of controlling error and provides a transparent means of assessing the quality of the data, all under a governance model designed to guard the broad public interest. However, actual implementation requires a mechanism for achieving registration and a business model to support that process.

Many private systems of entity identification cost an entity nothing to be included (and often do not even require its permission to be included), while consumers of the data are charged for use. In contrast, in the GLEIS an entity must pay an initial registration charge as well as a subsequent annual maintenance fee, thus assuming implicitly that identification has positive value to the entity. Use of the information, however, is completely free and unconstrained. Freely available identifiers provide an important public benefit in supporting truly open data, which is not generally feasible if otherwise open data contain proprietary identifiers. They also offer potential advantages in terms of reducing the strength of informational silos that depend on proprietary or other more limited identifiers. If those silos contain the LEI or there is an external mapping of the silo identifiers to the LEI, it is possible to bridge the best information from a variety of sources.

An identification system has no practical value unless it covers some useful set of entities. But the business model for the LEI also seems likely to have some effects on the level of its coverage of entities. Registration costs as of June 2016 were approximately \$180 for an initial registration and \$90 for the annual maintenance. Because the GLEIS operates on nonprofit, cost-recovery principles, the fees are expected only to cover the actual costs of operation and a sufficient amount to fund prudent reserves. To the extent that fixed costs are a significant factor in the GLEIS (for example, costs of developing systems of expertise for validation and IT systems to support operation), the charges for obtaining and maintaining an LEI should be expected to fall

²⁹ At least some entities that are marked as lapsed appear to be no longer in existence. Absent external motivation, LOUs appear to have little incentive to research such entities, and generally users of LEI data should tend to have fewer interactions with data on defunct entities that might lead to a formal challenge to the data. Additional work is needed to determine the most efficient means of addressing this problem.

as registration advances. Increased use of automation in the process of validation or other efficiencies may also reduce variable costs over time. While the current fees may be a minor practical barrier compared with other routine costs of doing business for most entities, its effect may still be noticeably negative. Large organizations may have thousands of entities, implying hundreds of thousands of dollars in fees. In addition, the existence of any fee may serve to crystallize a psychological perception of the burden an entity would have to bear in taking the effort to register for an LEI; if that argument holds in an appreciable way, a lower fee might have a smaller than expected effect.

The practical birth of the GLEIS came with requirements from the U.S. Commodities Futures Trading Commission and the European Securities and Market Authority for counterparties to over-the-counter derivatives trades to register for and report an LEI. As of July 2016, approximately 450,000 entities had received an LEI, mainly as a result of those requirements and a number of others that have followed. Obviously, this figure is far short of the unknown millions of entities that potentially could be covered by the LEI.

This shortfall is driven by a set of issues, aside from cost, each of which contributes to the implicit cost-benefit calculation a potential registrant faces. One large factor concerns the value of an LEI when coverage is low. In structures with network features, such as the GLEIS, the potential value of broad coverage is high, but when coverage is low the potential value is disproportionately low. In the initial stage, the value of LEI registration to an individual entity is simply the value for its private purposes, such as fulfilling a regulatory reporting requirement. Each registration also generates an externality in terms of the potential benefits for others' recordkeeping, in terms social benefits of a more transparent and stable financial system, or in facilitating unambiguous linking of information across sources. But at very low levels of coverage, such benefits are generally diffuse and of relatively low value. Such low benefits stand in strong contrast to the substantial costs users would face in altering their data systems to take advantage of the LEI. Thus, to an extent, there may be a self-reinforcing equilibrium of low coverage, in the absence of other incentives or special conditions. With low or only slowly growing coverage, the value of the LEI as it might be with higher participation may appear to be mainly theoretical or be sufficiently distant to be very sharply discounted.

Both costs and benefits may vary across users and entities, but *a priori*, benefits appear to have the most potential variation, both in the short run and to a lesser extent in the long run. In part, the short run variation in benefits turns on the level of coverage in specific areas, as noted generally above. For example, for a data user specialized in OTC derivatives markets, the LEI would have a relatively great appeal as an identifier, given its near universal coverage of counterparties as a result of broad regulatory requirements for reporting LEIs for such trades. Whereas someone interested in tracking entities black-listed for terrorism would be unlikely to find that any significant number of such entities would see an incentive to register.³⁰ However, even given complete coverage, the benefits of the LEI could still be expected to differ across entities, unless the set of applications also expands. For example, a small firm that only occasionally needed an LEI in order to hedge currency risk in overseas transactions would have a lower level of use (and presumably a lower subjective value) than a firm actively engaged in financial markets and including LEIs in regulatory reports and financial messages, such as ISO 20022, for generating and supporting its trades. But both might benefit from a movement to use the LEI more broadly in shared information systems. While practical situations may emerge where an LEI might not be ideal for representing every relevant type of entity even in the long run, currently the most important obstacle appears to be one of creating appropriate incentives for LEI registration, rather than any fundamental conceptual flaw in the LEI design or implementation.

Analogously to the case of many other dispersed networks of potential participants, the expectation for the GLEIS is that the inherent structural and informational advantages of the LEI determine a threshold point from which the value would so broadly exceed the cost that coverage would expand to a nearly universal level at least within the class of entities engaging in financial markets in any significant degree. To this end, some have argued that the public sector could act with coordination difficult to achieve in the private sector in order to jump to such a threshold point through the broad use of regulatory requirements to report an LEI as an identifier. Given the G20 mandate underlying the GLEIS and the spoken support of high officials of many important public institutions, there was even a presumption on the part of many that the public sector would quickly move in this direction. During the development of the GLEIS,

³⁰ For limited areas such as this, an exception to allow third-party registration by authorities or to allow a space for interoperability with an external system created for this purpose might be a way forward.

representatives of large financial organizations argued repeatedly that the envisioned system has the potential to reduce costs in the financial sector in a dramatic way, while improving the ability to monitor and control risks. Some even went so far as to ask regulators to require them to register, arguing that this step would empower them to ask the same of their customers.

Often it is argued that public authorities should take a longer-term perspective in evaluating costs and benefits than private parties and should attempt to recognize collective gains from positive externalities that are too weak to be motivating at the level of individual behavior. While many regulatory requirements for LEIs are now in place, more are already scheduled to follow, and a number of significant possibilities are under discussion, the regulatory response has been far less than universal. In some jurisdictions, it would require a legislative act to mandate the LEI.

Other arguments for regulatory restraint have been varied, but they appear generally to turn on cost-benefit arguments that existing systems, perhaps supplemented by vendor data, are good enough for now and it is costly and inconvenient to transition to a new system with such a low rate of coverage. In some cases, the framework for required cost-benefit analysis may discount or ignore positive externalities of substantial and coordinated expansion of registration requirements or it may view the risks at the current stage of development of the GLEIS as still too high. Some also appear to argue that the current relatively low level of voluntary coverage should be taken as a negative verdict of the virtues of the LEI.

Some initial regulatory reluctance to mandate the LEI turned on instances where the GLEIS was not able or not yet able to capture certain entities or types of information, as was the case for individuals acting in a business capacity at the beginning of the implementation of the GLEIS. Because it is a core principle of the GLEIS that it should respond flexibly to identification needs, however, it seems unlikely that such problems would persist, unless the solutions are very costly or disruptive. Overall, there appear to be few publicly expressed opinions questioning the long-run desirability of the GLEIS from a regulatory perspective, if sufficient coverage could be achieved and quality could be broadly assured.

Although there are still substantial mandates being contemplated in various jurisdictions, near-term practical progress may depend more on focusing attention on constructing or marketing incentives for registration around specific purposes or groups of entities. Engagement with market participants may help to identify specific areas where the LEI would add sufficient value

to motivate significant collective action within these areas. If enough such small expansions of coverage were successful, there might also be a higher likelihood that entities in areas interconnected with such entities would see more tangible value in the externalities of those registrations and encourage other entities to register or even to register themselves. Any such proof of value might also be additionally motivating to regulators considering mandates.

Increased coverage by the LEI would decrease the cost per LEI, because the fixed costs would be divided by a larger number of entities. However, the direct monetary cost of an LEI appears unlikely to be the most seriously inhibiting factor for large entities, the group most relevant for the systemic stability arguments that were a core motivation of the LEI effort. Seemingly more plausible is the potential cost of reworking existing information systems to include the LEI. Existing systems may employ a variety of other entity identifiers.

Introducing the LEI as an additional (or potentially a replacement) identifier would require another identification step to map the LEI to the relevant existing identifier(s) in order to be of any systematic use. Some identifiers do not have the uniqueness and exclusivity features of the LEI and they may also have different rules about the persistence of identifiers over time. Such mapping is a technically challenging identification exercise. If it could be performed reliably once, rather than separately in every situation, this could substantially reduce the costs of use, thus tilting the cost-benefit trade-off more toward the LEI. Some private data vendors already provide the LEI as a part of their entity-specific data files. The GLEIF might be the ideal neutral party to consider working to establish a formal certification program to support such mappings. A reliable system of mapping would reduce one important cost of implementing the LEI, but a focus on maximizing benefits and making them clearer is also needed.

Starting in 2017, an important additional value of the GLEIS will be the addition of information on entities' direct and ultimate organizational parents, as defined under accounting consolidation principles.³¹ This step fulfills one of the critical requirements for the GLEIS set out in the FSB Recommendations. During the financial crisis, there was a lack of comprehensive and

³¹ In the initial phase, the parent definitions will be based on the type of accounting consolidation relevant for an entity or jurisdiction. For example, it can be expected that most U.S. entities would report parents according to US GAAP principles, whereas in Europe IFRS principles would generally apply. Preparatory work for this work indicated that differences in accounting principles are unlikely to lead to seriously inconsistent outcomes for this purpose. For details, see "Collecting data on direct and ultimate parents of legal entities in the Global LEI System – Phase 1" (http://www.lei.org/publications/gls/lou_20161003-1.pdf).

transparently reliable data on organizational structure that could be used to aggregate risks faced by individual entities in order to understand the risks faced by an organization as a whole. The classic example is the lack of information on the holding company structure of Lehman Brothers at the time it failed. One of the motivations for establishing the GLEIS was to fill this gap. With complete coverage of entities within an organization by the LEI, the relationship information would be sufficient to characterize the entire organizational tree.³² With the current rate of LEI coverage, however, it is unlikely that a large number of organizations will be completely covered in this framework. Nonetheless, the information on ultimate parent would at least support aggregation of risks or other responsibilities to a top-level parent level for activities where an LEI is required.

It is important to recognize that while the addition of these organizational relationships are an important first step, there are other ways of viewing organizational relationships that may lead to different hierarchical structures. Control and beneficial ownership are two other common perspectives. The Federal Reserve's National Information Center database, which largely addresses the composition of bank holding companies, several different types of organizational relationships are available and sometimes they imply notably different organizational structures.

Other types of relationship beyond traditional hierarchical organizational relationships may be of interest in the longer run. For example, some have even foreseen the possibility of relationships defined in terms of "financial exposures". In addition, there may be other types of relationship specialized to particular sectors, uses or jurisdictions, such as the relationships that govern the connection of participants in U.S. electricity transmission markets.³³ Where relationships are relatively narrowly applicable or where the GLEIS otherwise cannot support a broader approach, smooth interoperability with external satellite information systems is likely to be very important.

There is an important indirect benefit from adding relationship data to the GLEIS. Such information places a given entity in the context of other entities that are also subjected to independent identification and validation of their identity and their other relationships. In

³² Note that there are a variety of alternative relationship types (such as one based on control or other aspect of responsibility) and each type could lead to the identification of a different organizational structure, potentially having different entities at the top of the resulting hierarchy. Connection of off-balance-sheet entities, such as special purpose vehicles, might be linked to an entity with yet another type of relationship.

³³ See <https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-7.pdf>.

general, the more relationships that are defined for given an entity, the less room there is for error in terms of its identification. This refinement may ultimately help to extend the set of applicable use cases for the LEI to include ones where there are more stringent requirements, such as “know your customer” rules.

Development of a detailed framework to contain the historical data of the GLEIS should also add to its use value. In the early stages of the GLEIS, the approach to managing historical information has been minimal. LOUs have been required to maintain data on the history of any changes to the LEI reference data, and that information is reflected in “delta files” showing changes from one file to the next. In addition, if an entity ceases to exist, either by going out of business or by being merged into another entity, the fact of expiration is recorded in the reference data of the entity, along with the reason for expiration and the LEI of a successor entity where relevant. As noted in the more abstract discussion of entity identification above, the question of the survivor following a corporate action, such as a merger or sale, is not always straightforward, and there are many views and even legal frameworks about the relevant survivor. The GLEIS cannot hope to impose a uniform global definition of survivor, but it should be able to collect and report sufficient information for users of the GLEIS to be able to construct or sufficiently approximate a consistent history of all individual entities. Work is ongoing in this area.

IV. . Conclusions

We have reached a stage of human history where there is a strong likelihood that machines will have an increasingly deep role in running the great majority of the manageable processes in the world that support life, and they will operate with minimal human intervention. If the relevant quanta for management—an action, the subject and the object of the action, and the relevant initial state description—are not defined and identified to a sufficiently high degree of precision in such a world, unintended actions could arise and systemic stability may be threatened by resulting turbulence. A taste of such breakdown was experienced in the financial crisis—or in fantasy in the film “Brazil”. Highly reliable identification will also be necessary to support the level of transparency necessary to support trust in such systems. Identification needs in finance are likely to remain especially strong.

This paper has reviewed a range of conceptual issues relevant for identity, identification and identifiers. Identity raises fundamental questions about what an entity of any sort is, as distinct from all other possible arrangements of matter or logic, and the extent to which it is persistent over time and space. Identification operates at a more concrete level by associating observable attributes with an entity, as defined against the background of specific types of formal organization. By serving as a unique label, an identifier is a shorthand way of referencing an identification process for a particular entity. An advantage of an identifier is that it may be taken to signify a particular identified entity, regardless of whether the entity is present in a meaningful sense.

Although the paper explores a variety of areas of abstraction around the terms identity, identification and identifier, many others are silently passed over. Virtually any aspect has the possibility to regress to the point of metaphysics. The paper attempts to remain at a practical level, where the most pressing problems are ones associated with costs and the possibilities for information for identification, process control, error and risk, in the context of a given use or set of uses. The appropriate trade-off between costs and the other factors must be determined as appropriate for use.

Finance may be currently in the forefront in terms of the level of interaction of massive amounts of data with broader aspects of human behavior. Given the numerous, disparate and dispersed participants involved and the necessity for automation, standardization is critical for such a system to operate at all. The elements communicated must be as clear as possible. Among those elements, nothing is more important than the identity of actors in any exchange. The construction of the GLEIS described in this paper is practical example of a standardized system of identification that has considered the practical trade-offs against a foundational set of use cases.

The GLEIS is intended to provide an identifier, the LEI, associated with a level of identification appropriate for a wide variety of areas where the identification process underlying the LEI is viewed as sufficiently trusted and the propagation of the LEI in use is either unquestioned or separately controllable to a sufficient degree. For example, because the LEI serves as the primary regulatory identifier in OTC derivative trades, it is unambiguously associated with a

trade; propagation of the LEI beyond that point through clearing and settlement relies on the integrity of the supporting information systems.

In some very sensitive applications, even the rigorous identification process underlying the LEI may not be sufficient, or its attachment to a given body of data may not be sufficiently trusted. For example, some anti-terrorism uses may require extraordinarily high precision for selected cases that would not be feasible to uphold for every entity. Nonetheless, the LEI framework might still serve as a core around which an even more rigorous process of this sort could be built, and errors in identification for the LEI could be passed back to the GLEIS for correction through the open challenge process.

Interoperability of data organized around the LEI with other sources of data is also critically important. The GLEIS is not designed to contain all relevant information about entities, but only to serve as a “hub” for identification of entities across other systems of information. Sometimes the LEI may not be present in a relevant body of data where there is a need to connect the data with other data containing the LEI as the identifier. Where the data without an LEI contain an alternative identifier, the problem becomes one of mapping, as discussed in this paper. Where the data contain no relevant identifier, a process is required to identify the entities present to an appropriate level of rigor for the intended use and to map those identities to the appropriate LEIs in the other source of data. Because mapping is itself another form of identification, complications may arise when the sources mapped rest on incompatible information or frameworks. Interoperability of the GLEIS with relationship structures organized and maintained outside the GLEIS is likely to be particularly important even in the long run. The GLEIS has the possibility of being the foundation for many other such complex systems.

Going forward, the rigor of control of LEI validation and the steps to ease mapping for the LEI should spur progress. The underlying quality processes supporting identification with an LEI can be expected to become increasingly rigorous as the ability of the GLEIF to enforce standards becomes more firm and as evaluation of past performance leads to continuous improvement. Addition of information on organizational structures to the GLEIS will provide greater clarity about both the identity of individual entities and the collective effect of the organizations of which they are a part. Such organizational information, together with potential additions of information on relationships with corporate officers or beneficial ownership, could serve to

further sharpen the level of identification for uses with more critical needs for precision in identification. For the long run, the GLEIS can be expected to evolve further around its original structure to support, or even prompt, a variety of new needs where identification has a key role.

Bibliography

Couillault, Bertrand, Jun Mizuguchi, and Matthew Reed, “Collective Action: Creative Use of Soft Law, Local Law, and Private Law to Build a Global Infrastructure” (forthcoming).

Financial Stability Board [2012]. “A Global Legal Entity Identifier for Financial Markets”, http://www.fsb.org/wp-content/uploads/r_120608.pdf.

International Organization for Standardization [2012]. “ISO 17442: Financial services — Legal Entity Identifier (LEI)”, http://www.iso.org/iso/catalogue_detail?csnumber=59771.

Locke, John [1690]. *An Essay on Human Understanding*, Prometheus Books.

Annex: Governance of the GLEIS

The GLEIS was designed to serve a public-interest mission, by creating an identification system centered on the LEI in order to support the missions of regulators, facilitate improved information management in the private sector, serve as a tool for research and provide information for the public in general. In contrast to many of the existing proprietary identification systems, the LEI and its supporting data are freely available without intellectual property restrictions. The costs of the GLEIS are paid by registration and maintenance fees imposed on entities that register in the system.

The governance structure of the GLEIS operates at three levels: the Regulatory Oversight Committee (ROC), the Global LEI Foundation (GLEIF), and Local Operating Units (LOUs). The ROC, the highest-level governance body of the GLEIS, came into existence in January 2013 under a charter developed by a working group of the Financial Stability Board, which was endorsed by the G20 and then acceded to by over 70 public authorities from a wide range

of jurisdictions globally.³⁴ Those authorities became members of the ROC. The ROC is responsible for setting policies under which the system operates and for overseeing the operation of the system in a variety of ways.

The Global LEI Foundation (GLEIF) was established in Switzerland in June 2014 to serve as the central operational unit of the GLEIS, with key operational responsibilities, including, among other things, overseeing the quality of the assignment of the LEI to entities, setting operational standards and coordinating the federated registrars of the GLEIS. The constitutional document of the GLEIF (its “statutes”) establishes its formal relationship with the ROC; among other things the statutes require the GLEIF to accept standards and protocols put forward by the ROC to define the nature of the GLEIS.³⁵ A memorandum of understanding between the two parties further clarifies the relationship in practice.³⁶

Local Operating Units (LOUs) provide registration services to entities and perform validation of the data. An LOU may be a public or private body, but each is required to operate in this capacity on a nonprofit cost-recovery basis. An LOU may operate in a single jurisdiction or market or it may operate much more broadly—even globally. However, an LOU must have sufficient institutional knowledge about the markets in which it operates to be able to select and use documentation to establish the existence of registering entities and to validate the information provided by the entity about itself.

From the time in 2013 when the ROC came into existence, the GLEIS operated in an interim manner, with the ROC assuming the minimal necessary operational responsibilities for the GLEIS to operate, until the GLEIF could be established and it could assume operational control and oversight. At this time this paper was written, all aspects of transition from this interim state had been completed except one: Initially, the LOUs were brought into the GLEIS under the sponsorship of a ROC sponsor, which had responsibility for ensuring that their sponsored LOU was compliant with ROC principles; by the middle of 2017, all LOUs are expected to have completed a formal accreditation process with the GLEIF, resulting in a set of bilateral contracts between the GLEIS and the LOUs that will empower the GLEIF to

³⁴ See https://www.leiroc.org/publications/gls/roc_20121105.pdf for the ROC Charter.

³⁵ See <https://www.gleif.org/content/1-about/5-governance/8-statutes/gleif-20140824-3.pdf> for the GLEIF Statutes.

³⁶ See <https://www.gleif.org/content/1-about/5-governance/3-mou-between-gleif-and-lei-roc/20150923-ROC-GLEIF-MOU-final-signed.pdf> for the memorandum of understanding between the ROC and the GLEIF.

enforce common standards and data quality. ³⁷ Any LOUs failing to complete this process by the end of 2017 will be excluded from the GLEIS.	
--	--

³⁷ See <https://www.gleif.org/en/lei-system/gleif-accreditation-of-lei-issuers/required-documents> for the Master Agreement governing the relationship between the GLEIF and each LOU.