GLOBAL iD (GiD)

BACKGROUND

Every person has a right, and a responsibility, to a secure, trusted, and private identity. The prevalence of electronic connections implies that we each must identify ourselves to prove our authorization for particular conduct -- without necessarily having to give up any more private details than necessary. For two parties to conduct their affairs in a trusted manner requires balancing reciprocal security and privacy concerns. Age-old concerns about "big brother" have chilled expectations about a corporation or government balancing these competing values. However, the advent of new technologies such as distributed ledgers suggests new possibilities for a universal and portable identity solution that does not require a centralized authority. The GID mission is to harness both new technical and governance possibilities to create a "little brother" identity helper rather than a "big brother" identity overlord. GID is initially focusing its efforts on digital financial identity, although we (or others) may pursue other use cases.

Many of the world's poorer individuals are unable to participate in the connected world, given they lack a digital identity to garner access to particular offerings in society. Nevertheless, even for those who have granted access, the status quo is friction-laden with redundant signups, as well as susceptible to abuse by bad actors. To date, no one has ever conceived of a central power to do all of this without veering into an Orwellian big brother reality. The alternative of distributed ledger technology and federated governance suggests there is a democratizing bottom-up identity architecture that could include and benefit every member of society.

The GID Framework describes the ability for individuals to control their assets, as well as permission-based conduct, rightly and responsibly and therefore in turn be trusted by others who do the same. This is only possible by reciprocally balancing the rights and responsibilities of a universal and portable identity framework.

OVERVIEW

Global ID (GID) enables each person or entity to own names that are a **secure, private, and trusted means** of controlling one's assets and permission based conduct. Specific names (or tokenized versions of those names) are unique across all use cases and legal jurisdictions in the world. The **"portability" of authorization** enabled by names, means that third parties **are no longer required to collect or store personally identifiable information (PII)** to interact safely with GID users.

The ideal GID framework is **governed by all its stakeholders under a federated structure**, rather than controlled by any single corporate or government authority. Access to **underlying data** about **individuals and entities is controlled** by those parties and is only shared and attested by the permission of the party that volunteered the data. While the underlying data is private and secure, **attestations about the veracity of the data are by default a *public* good**, which are openly and equally available to all for the creation of "trust scores" regarding GIDs. Unlike objective attestations about a GID holder, trust scores are subjective interpretations of the value of attestations by a third party who has to decide whether to interact with a particular GID holder.

Privacy rights of GID individuals and entities **are reciprocally balanced with societal compliance and risk controls within the legal and regulatory framework of the user's relevant jurisdictions**. The benefit for Global ID users is that once they create their Global Identity Name, they **only ever have to sign-in to participating services as their GID is embedded.** Furthermore, their PII is collected and safely stored once, instead of propagated and exposed across the internet and upon their interactions with service providers. For stakeholders, they also enjoy the benefit of removing friction of new/existing users to access their services, all with higher confidence that those users are compliant and risk appropriate for their offering. Additionally, regulators and law enforcement are provisioned with much more comprehensive and consistent tools. Consequently, they can uphold the law and oversee the risk at hand by **replacing the antiquated and ineffectual limits of silo-based PII data collection** that is the norm across different countries today.

ATTESTATIONS, AUTHENTICATION AND AUTHORIZATION

The greatest user benefit of the GID framework is that it grants users principal control over their digital personal information, thereby reducing friction without increasing risk when signing up or using existing services from third parties. The key mechanism behind enhanced access is a standardized process for identifying oneself when seeking authority to enjoy certain permissions and undertake certain actions.

Each GID identity includes **attestations from third parties who vouch for (1) the individual and (2) the authenticity of identity attributes.** (Attestation details found on pages 6 – 7). When the individual has created their GID, they **select vouchers** who would attest the individual in certain situations. Vouchers **perform a critical role** in the event an **individual loses their phone or becomes incapacitated.** Additionally, **presentation of some (secret) attributes associated with an identity** constitutes authorized access by the presenting party **to act on behalf of the identity in question**. Such action may **involve the transfer of virtual and material property and/or permissions to engage** in particular conduct. Conversely, others may transfer virtual or material property to, and conduct actions directed at particular identities, based on the belief that these destinations accurately represent the person or group behind the identity in question. Common **use case examples are sending funds or viewing documents with a security clearance**. Authorized access may be undertaken by the identified party directly or may be **pre-delegated via the issuance of tokens ahead of time and for a persistent period**, unless the original delegating authority revokes such permissions.

In situations where the individual has their phone stolen or lost their device, Global ID's **approach melds the new cryptographic notion of multi-sig with a conventional practice of democracy**. If a majority of the **individual has trusted peers who believe they are re-establishing themselves**, this is the best/final determinant of whether the individual should be allowed to proceed. Global ID expects the people who know them best will also be willing (and able in an automated fashion) to green light their need to re-establish their identity and phone token connection.[1]

It is worth noting that **restoring an account is designed to be completely built on a governance system of trust established by the Global ID holders themselves**, rather than reliant on a third party authority. One's ability to **restore their own compromised account is the foundational test of true portability of one's Global ID.** Dependence on an external authority to move/restore one's identity makes the ecosystem less portable. While minimum reliance on **public/private key pairs is just as**

[1] This same logic also applies when individuals become incapacitated and can no longer act rationally or responsibly on their own behalf. By **pre-stipulating a power-of-attorney advanced directive**, GID is setting up the means for overruling its own agency should a majority of their **trusted peers (previously approved by themselves) believes the time for authorization over the individual's permissions has succumbed to where someone else needs to take over**. All of us must face this eventual handover, and Global ID has anticipated such handovers for all individuals and even groups/entities that exist.

portable as trust based attestations, it is simply not practical to have users at **risk of losing all of their attestation history simply because a private key is lost or unrecoverable.**

Nor would it be acceptable if someone's private key was revealed publicly, that a particular Global ID would be forever compromised. While **private keys are a marvel of trustless solutions to privacy and security**, they fail as a practical mechanism where the preponderance of utility in identity is based on trusted attestations rather than mere possession of a secret. **Private keys ultimately suffer the same weakness as passwords given the vulnerability to being exposed**. They have more friction by being lengthier but fundamentally, they are no different in form than traditional password methods.

GID **incorporates a more secure authorization system that relies on something we as individuals have, rather than just something that we know**, and that can be compromised through a data breach or tricking us into handing a password over unknowingly. **Traditional OAuth solutions still depend on a username and password** combination; albeit one that is not to be shared with every application that defers its sign-up/sign-in process to a Facebook Connect like service. Unfortunately **passwords are vulnerable to phishing** attacks rendering these authorizations systems less secure.

Global ID anticipates **every named user having a mobile phone that acts as a physical token** for their identity (i.e. something that they have rather than a password that they know). Therefore**, one's phone (the combination of one's phone number, SIM card, and specific device) is connected to the Global ID** of the individual who has that device. The expectation is the device is present and once bound by attestations (and will be a method for confirming authorization) for all permissions executed on behalf of any Global ID holder. **Attestations about the holder** range from confirmation by the carrier as to the identity of user, to biometrics, and in a **novel and significant manner from the personal contact lists of other Global ID holders** who have a particular user (and that user's phone number) in their own private address books.

Global ID **introduces an important constraint** that actually significantly increases the privacy/security/trust of its ecosystem**: any Global ID name can only be associated with one-and-only-one phone (number/SIM card/device) at a time**. Thus one cannot associate their Global ID with multiple devices – meaning that there is always **only a single token of one's Global ID active** in the ecosystem at any point in time.

Furthermore, the expectation is this **device is not only what is signing, but also where a signing is occurring** (assuming built in GPS capabilities). This is a **significant risk mitigation capability**, as this binds the actual user with their device at any particular time when permissions are authorized. Payors and payees may be standing right next to one another (in a brick and mortar context), but even in an online context for commerce or other permissions, there are more and less natural expected locations where a user tends to initiate authorizations. While this information isn't intended for public consumption, the **location tags, when connected with phone number, SIM cards, and device IDs represent relatively highly trustable markers** for permissions to be granted.

If one's phone is lost or stolen, then one must disable one's existing phone token and seek authorization to establish a new phone to "carry the flag" and reattach to all the attestations associated with a particular Global ID.

IDENTITY VAULTS BY LEGAL JURISDICTION

GID is a ubiquitous alternative to silo based identity solutions that previously required each participating party to relinquish PII to each particular corporate or governmental entity with whom they were associated. Alternately, with Global ID, PII is entered by each participating individual or group and placed first in an encrypted local personal datastore – typically on a local browser or mobile phone under the control of the user. (Personal datastores details found on page 9) **Access to GID data by third parties is regulated by i) the wishes of the party providing those details, including selective access by attestation agents; and ii) by the law of the local jurisdiction in which the data resides due to the activity and location/residency status of the person or group concerned**.

Only data specifically tagged, as "searchable" via internet-based tools is available via IP based search methods. All other bulk PII **Meta data is unsearchable by design – except through locally running tools that can only be accessed within secure identity vault facilities residing within respective legal jurisdictions.**

GREEN ECOSYSTEM OF IDENTITY

The set of individuals and entities that are sufficiently attested to conduct **secure, trusted and private actions is termed the "green ecosystem"**. There are four states that can exist between two parties that reflect the topology of green versus less than green activity between individuals and entities. In the

case of sending and receiving money, the parties can be either rated green (sufficiently attested to) or not (lacking sufficient attestation), resulting in a two by two matrix of possible conduct:

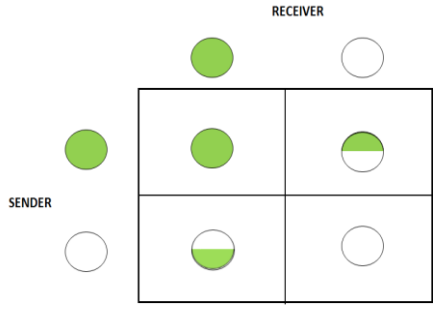


FIG. 1

In Fig. 1, the assumption is that there is a common definition of what attestations are required to be considered green or not green. **Common standards are set as a legal/regulatory standard within a jurisdiction, but also negotiated to a more acceptable international standard when jurisdictions agree to harmonize definitions (as might be the case through an entity like FATF-GAFI (Financial Action Task Force or Groupe d'action financiere))**. Regardless of whether standards for being green are intra- or inter-jurisdictional, the consideration is that the attestations regarding an individual or group are "pre-staged" prior to authorizing particular conduct by the concerned parties. Pre-staging authorizations is critical to ensure straight through processing for fully compliant and acceptable risk rated activity, but also for intervening with additional enhanced due diligence safeguards or when outright blocking is required.

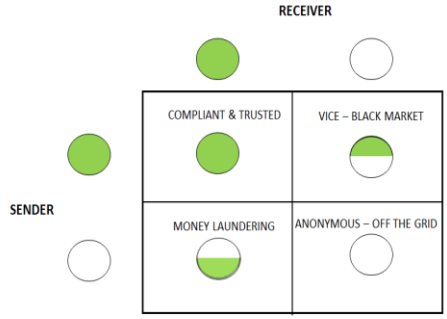


FIG. 2

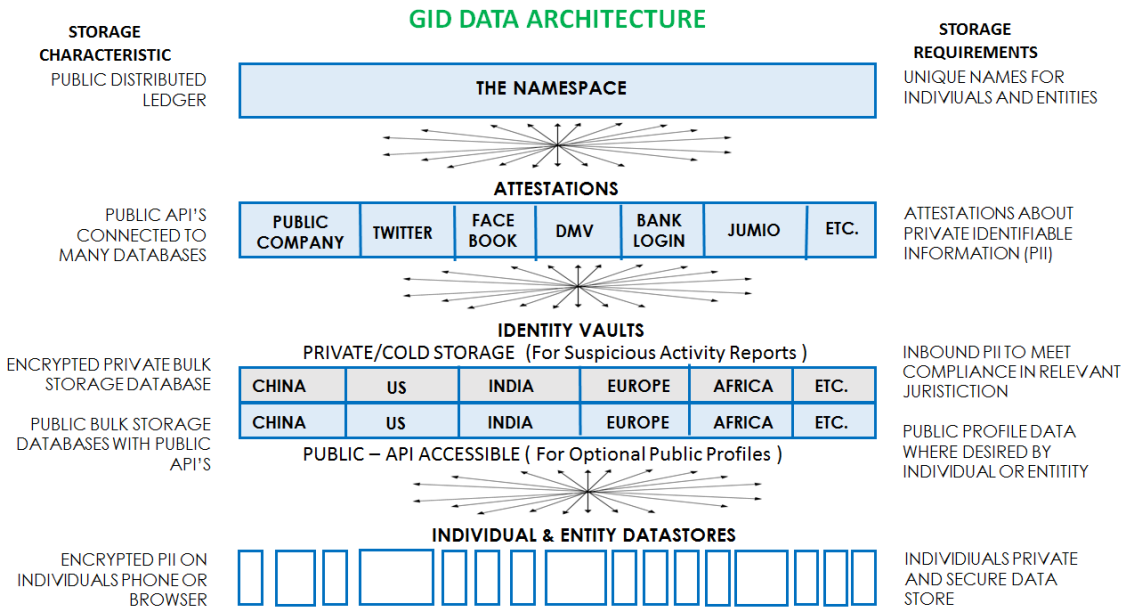
In contrast to **green-to-green activity that can be characterized as compliant and trusted**, the other combinations of activity that happen can also be labeled to reflect their potential meaning in society. **Green to non-green payments and conduct can be associated with vice or black markets**

whereby otherwise compliant individuals and entities seek out non-compliant parties for conduct that is not otherwise authorized in the mainstream of society or the law. Conversely, **non-green to green payments are associated with money laundering of proceeds from vice or black markets** moving back into the green ecosystem. Finally, non-green to non-green payments and conduct are anonymous or pseudo anonymous and operate “off-the-grid” from the green ecosystem of identity attestation.

THE GID ARCHITECTURE

The GID architecture is composed of **i) a namespace on a distributed public ledger; ii) attestations about those names via APIs; iii) compliant identity vaults for each legal jurisdiction served; and iv) user controlled personal datastores of personally identifiable information (PII)**.

FIG. 3



THE NAMESPACE

The namespace is where **individuals and entities unique names are displayed and “owned” using cryptographic signatures**. The list is a **public good** in which everyone has access – the **prime benefit** being assurance regarding **who owns a particular name at a particular point in time** (and secondarily for how long they have owned that name and any attestations that create a trusted reputation around that name).

Significantly, the existence of a name is not an indication that someone is a good rather than a bad actor. The **sole purpose of the namespace is unambiguously designate who has ownership** of a name, independent of any value judgment that can be reached about the owner.

Furthermore, the existence of a name is **not an assurance, in itself, of identity in a manner that "outs" the owner of that identity in a personally identifiable form to the public**. While a particular name may be purposely tied to other information that is shared to advertise a brand or personal reputation, the exact opposite use of the namespace as a privacy enhancing mechanism is also supported by the namespace. A name can purposely represent a level of indirection between a true identity and a privacy-enhancing alias under which someone operates in his or her daily life (but which could still be tracked back on a need-to-know basis if a crime has been committed).

The aspirational design is that **everyone and every group (and potentially everything in the internet of things) should want to have one or more names – some more public and some more private** – so that they can more easily prove (perhaps while maintaining privacy) themselves and their associated permissions when attempting to take action with others.

Distributed ledgers make equal, open, neutral, and permission-less access to this information **(in real time)** available to everyone and everything in the world. A decade ago, this method was impossible and therefore never contemplated as the foundation for a global identity framework. However, today **founding an identity framework on distributed technology and governance** is not only possible but an imperative in a **multilateral world** where there is no single authority on identity.

ATTESTATIONS

Attestations are **signed statements (by a user and a third party) about the objective state of some aspect of that user's PII**. Notably, **attestations are not the PII itself, but rather some verification or validation about that PII**. Thus an attestation can state that particular PII exists and/or is judged to be accurate **without i) giving up what that PII is, or ii) making a subjective judgment about whether the objective attestation means that the party concerned is a good or bad actor**. Attestations should not be confused with ratings, which are the subsequent (and subjective) ascription of good/bad absolute and relative scorings – which is beyond the scope of the GID Framework, but represents fruitful grounds for 3rd parties seeking to offer those value added services.

Attestations are about names written to the namespace. Attestations need not live in the namespace, providing they are cryptographically signed about a namespace entry and live in an API accessible database. As long as those attestations can be reached by 3rd parties in a timely fashion, then the need to support ratings and other on-demand issuance of permissions is met.

PERSONAL DATASTORES AND IDENTITY VAULTS

A personal datastore describes the practice of an individual securely and privately storing personally identifiable information (PII) about themselves in an encrypted form on their local browser or a mobile phone. As such, the information is retrievable and sharable by them only when they authorize such activity – and is otherwise private. Having entered and saved the data, the user in theory would not need to re-enter it other than to update or cope with a lost or new local device that holds the datastore. The user unplugging from the internet (cold storage) or erasing the datastore altogether could disconnect personal datastores from access to the outside world.

Personal datastores are privacy enhancing but fall short of meeting compliance requirements in various legal jurisdictions for conducting particular types of activity in society (sending and receiving money, boarding an airplane, etc.) that involve trust with third parties, or compliance with laws regarding illegal or terrorist activity. Thus, individuals and entities that wish to partake in societal activities inevitably have to give some PII to a third party. Historically, such PII would have to be given to each 3rd party service provider to store in a database controlled by that 3rd party. Such databases of PII become the target for hacking attacks given that such information can aid in identity theft and other malicious behavior. **Rather than multiplying the copies of PII every time a user interacts with a 3rd party service provider, a single or few carbon copies of PII could be kept in a purpose built "identity vault" accessible only on a need-to-know basis with due process of law and/or consent by the user in question**.

Identity vaults operate as a log of every piece of PII that is volunteered by the user about themselves (date stamped for any time changes). **No information in an identity vault is obtained from any place other than the user themselves**. In contrast to a credit bureau that is built from 3rd party sources about a user, an identity vault provides the opposite function – a store of data volunteered only by the user themselves. Furthermore, every user has a right to see (and edit) every piece of information about themselves – although an audit trail of all changes is always recorded to maintain present and past state of the identity data. Whereas credit bureaus are littered with erroneous and outdated

information about a user, an identity vault is completely managed by a user themselves – implying personal responsibility (and empowerment) for the provision of accurate and up to date data. The role of 3rd party attestations is segmented from the vault so there is a clear division between privately identifiable information and the verification of that data by 3rd parties.

All data in an identity vault is nothing more than what the user could/would have stored about themselves in their own personal datastore. The advantage and need for an identity vault (in addition to a personal datastore) can be summarized as:

i) **The identity vault is available 24/7** from an accessible (namespace directed), API so attestation agents can easily (and with user permission) access PII necessary to undertake a particular attestation on a timely basis. A personal datastore might (or might not) be available at a particular point in time to facilitate such a request and therefore is operationally inadequate for some situations

ii) The **identity vault ensures that particular data necessary to meet CIP/BSA/AML requirements is accessible by firms** for suspicious activity reporting requirements. Unless such data was guaranteed to be available, PII data would have to be collected and stored directly by firms providing services to users -- which would degrade privacy protections and increase security vulnerabilities

iii) **Users who want to promote a portion of their PII details in a public profile or brand can dynamically attach their profile, address book entry, web identities, etc. to the underlying data contained in the vault**. Additional third party registries can build (with permission) their own offerings based on the publicly designated data elements in the identity vaults. Thus Skype, Twitter instant message, mobile address books, and other profile based services can leverage public facing identity vault data to build out more trusted profiles of their users (when those users grant permission to do so)

GID OFFERINGS

GID **operates a dual issuance namespace** on **publicly accessible distributed ledgers**. Once names are issued on the **"raw" ledger**, the **recipient receives a private key that ensures that they, and only they, can allow attestations** about their name or transfer it to another party. In parallel to issuance of names on raw ledger, a parallel **"curated" ledger** entry is made for **which GID, rather than the name user, controls the secret key**. Under normal conditions, the curated version of the namespace will match the raw, but in the event of a proven claim that a raw name's access has been lost or stolen; **the curated version can denote the discrepancy**. GID can make a decision to

re-assign a disputed name on its version of the ledger, in response to due process of law. **Third parties can choose to rely on only the raw version of the namespace or reference GID** (or competing curated interpretations) **of what ownership should be if/when law overrides raw permissions state** of the ledger.

The GID Framework purposely anticipates the tension over a technically pure and permissions based view of the world where he/she who has a secret key trumps any other considerations about law (i.e. a view in which possession is 100% determinant). The GID counterbalance is that rules and law by various jurisdictions can determine who truly has authorized access to a name and attendant attestations, especially when the associated secret keys have been compromised or misappropriated by coercive and/or illegal means.

GID arbitrates disputes over namespace allocations when trademark or unauthorized conveyance is an issue. Because ownership of a name sits on a public ledger that states the duration of ownership of any particular name, it is easy for any and every one to determine which names (and their attendant attestations) have a long and durable track record versus those that have been hastily created or transferred. Names with longer and stable attestation histories are much more likely to be trusted than newly created or recently transferred names, which may enjoy little or no trust at all. Importantly, because the namespace registry is updated in near real time, there should never be ambiguity as to whom the actual holder is of a name that may be designated with particular permissions, including the receipt of funds being sent or spent.

GID names are issued free of charge and are renewable each year. Individual users are expected to **limit their collection and use of names to five per person (ten per group)** though a waiver of the limit can be applied for in special circumstances. Each GID name is attached to a mobile phone number at a minimum so that the maximum issuance thresholds can be observed and administrated. The **issuance of one time (disposable) names is available to established users** who have a track record of good behavior. These onetime names can automatically inherit a set of attestations that will signal that the holder is well attested to but seeks to use a one-time (privacy guaranteeing) token name for a particular transaction rather than a persistent name. Onetime names can be mapped back to the original persistent name holder only when suspicious activity has been detected with a particular person or transaction and due process dictates replacing the disposable name with the more persistent named party that asked for a one-time token name.

GID certifies which attestation providers are acceptable to participate in the GID framework. GID has no power to prevent non-certified parties from hosting their own attestations about namespace entries (which are publicly accessible to any or all). However, only certified attestation agents will be treated as GID constituents with full shareholding and governance rights. GID will actively resell attestation services of all constituent members and will ensure that access to an attestation agent's information is available through default API offerings for the GID ecosystem.

Individuals or groups who have been attested to can choose to notate those particular attestations as no longer (in their belief) accurate or relevant. GID will denote all user expired/revoked attestations as indicated, and compliant rating services will respect the request to not include user expunged attestations in any rating score calculation.

GID certifies identity vault providers that are deemed acceptable holders of PII in the various legal jurisdictions from which end users originate (essentially every country in the world). PII in certified identity vaults is accessible via GID specified APIs for access by certified attestation providers when combined with end user wishes that such data be accessed to obtain a particular attestation.

GID sets pricing for attestations requested by stakeholders seeking such attestations. **GID also sets pricing for access to identity vaults by stakeholders** needing to conduct suspicious activity reports. **GID provides identity vault services for the holding of PII to end users for free** and recoups the costs through marking up attestations about the PII held in identity vaults. All users are thus incentivized to utilize free identity vaults and to keep comprehensive and up-to-date PII. GID also offers optional interchange priced insurance and assurance services for stakeholders using GID OAuth services when conducting permission based activities where GID's risk and compliance controls are utilized.

DISPUTES BETWEEN INDIVIDUALS/GROUPS AND SERVICE PROVIDERS

Global ID anticipates that contingency of disputes through the implementation of a multi-sig +1 architecture that ensures that any whistle blower acting within the due process of their particular legal jurisdiction can petition to have a Global ID write an attestation calling for the suspension of further authorization privileges for a contested Global ID until the dispute is resolved. Global ID itself has no power to suspend authorizations given it is only a standard. But as a standard with the backing of its stakeholder community, Global ID can denote which Global IDs it attests are arguably "in dispute."

Parties that ignore the Global ID attestation about the recommendation to suspend do so as a rules violation of Global ID, and can expect to have a negative attestation written to their own attestation history. Note that all other attestations about Global ID holders are always positive attestations. Thus the decision to negatively attest by Global ID itself (and to "out" others who appear to ignore the attestations and continue as if the hold recommendation had not been made) exercise the nearest thing to "hard authority" that it can manage. While unable to block permissions due to the truly portable nature of Global ID, the ecosystem can nevertheless self-identify when its own members are operating outside of its own stakeholder-generated rule set.

Global ID will charge a commensurate fee to investigate a whistleblower claim to ensure avoidance of frivolous claims. Where the public interest is concerned, Global ID, via the guidance of its Dispute Committee, can chose to waive the whistleblower claim fee if doing so serves the public good. A meritorious whistleblower claim should never fail merely because the petitioner lacks the means to fund a worthy notification of a dispute that is failing to be equitably resolved by the automated Global ID capabilities.

The impact of a valid Global ID whistleblower claim is the equivalent in traditional law of filing an interpleader:

> Interpleader is a civil procedure that allows a plaintiff (Global ID) to initiate a lawsuit to compel two or more other parties to litigate a dispute. An interpleader action originates when the plaintiff holds (in our case overseas rules relating to) property on behalf of another, but does not know to whom the property should be transferred.

What this means is that Global ID is neutral in the dispute and is indicating an intention (along the rules of each legal jurisdiction to which the parties are bound) to resolve the differences between parties via the courts if those parties fail to accept the (assiduously automated) methods already built into and operative by the Global ID ecosystem. While attempting at all times to avoid the need for interpleader type friction, Global ID recognizes that existing regulations and law by respective local jurisdictions ultimately may trump any rule logic that the Global ID might set for its own stakeholder community. Hopefully Global ID rules and local laws are aligned – but if there is ever a doubt as to the ultimate authority, Global ID always defers to the law and attempts to adapt its rule set to reduce forward

ambiguity that would result in repeat occurrences of non-automated decisioning around authorized access credentials associated with Global IDs.

GID GOVERNANCE

A key component of Global ID is its governance structure, a framework governed by all its stakeholders under a federated structure, rather than controlled by any single corporate or government authority.

In order to maintain neutrality, **the GID will operate as a stakeholder driven organization.** Unlike traditional corporate or venture backed entities, GID operates independently of the control of any investor or group of investors. **The GID deliberately segregates voting and economic rights to eliminate passive equity holders' having input into GID's operating rules.** The reason for segregation is that moneyed GID equity holders could be inclined to leverage their influence to favor certain technologies, entities, or countries at the expense of others – undermining the neutral pledge of the group.

Stakeholders are not able to increase the proportion of their "say" in terms of voting rights by investing in GID as this might compromise the neutrality of the organization. Instead, GID will issue membership shares to GID stakeholders and users with voting rights. Only usage on behalf of stakeholders and users, can determine pro rata voting power – albeit with unrestricted ability to proxy one's own voting rights into a larger voting block on any key issue.

Out of scope for this paper is a description of the actual GID operating company, which runs GID on a day-to-day basis.

SUMMARY

It is the positioning of the GID Framework as a public good that is the key differentiating feature from other, prior, and centralized efforts, to create an identity solution for the world. An identity solution that happens to be portable and controlled by end users themselves while still not only meeting the needs of FIs, regulators, consumer advocates, and other stakeholders, but also including them as part of the Federated Advisory structure and Board.

TEAM

Greg Kidd, Co-Founder, Chief Executive Officer: Ripple advisor. Initial investor/advisor for Twitter/Square. Fintech investor in the valley and internationally. Formerly Promontory Financial Group, Board of Governors of the Federal Reserve in payments, Dispatch Management Services Corp chairman, Booz Allen, and the National Outdoor Leadership School. Harvard, Yale, Brown.

Alka Gupta, Co-Founder, President: eBay/PayPal, Inc., Retrevo (acquired by Nook Media,) Lycos (acquired by Telefonica), AT&T Solutions. Commerce and payments start-up advisor. Menlo Park-Atherton Education Foundation President. Wharton, Case Western.

Mitja Simcic, Co-Founder, Chief Technology Officer: Veteran in industry with experience driving cross company engineering initiatives. ROIDNA, Qloud.io, Kupi. Finds and implements the right solutions to solve business problems that are sustainable, scalable, and cost effective. Computer Science and M.B.A.

SPECIAL ADVISORS

Michael Barr: Dean of Public Policy, Professor of Law at the University of Michigan. Senior fellow at the Center for American Progress and, previously, at the Brookings Institution. He served from 2009-2010 as the U.S. Department of the Treasury's Assistant Secretary for Financial Institutions and key architect of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. Yale. Oxford University, as a Rhodes Scholar.

Tom Brown: Partner, Global Banking and Payment Systems at Paul Hastings. Advisor to payment systems and financial services on regulatory issues. VP, Senior Counsel at Visa U.S.A. Inc. Deeply involved in the company's transformation from a co-op to a shareholder owned company. University of Chicago. Columbia University.

Norman Reed: General Counsel of Carta. Former General Counsel of Ripple. General Counsel of Omgeo LLC, Managing Director The Depository Trust & Clearing Corporation. Special Counsel, Securities and Exchange Commission. Federal Reserve Bank of New York. Columbia. Ohio State University. 1st Battalion, 504th Parachute Infantry Regiment of the 82nd Airborne.

Karen Gifford: Special Advisor for Global Regulatory Affairs at Ripple Labs, Promontory Financial Group, Federal Reserve Bank of New Year. Yale, Vassar College.

Jean-Louis Schiltz: Luxembourgian based lawyer. Minister for Defense. Guest Professor at Luxembourg University. His portfolios included media, telecommunications, technology, international development and defense. University of Paris (Sorbonne.)

Arjan Schutte: Founder and Managing Partner Core Innovation Capital. Senior Advisor to Center Financial Services Innovation. Passionate industry expert. Has invested in some of the most innovative companies serving the underbanked. Entrepreneur with several venture backed companies. Lewis & Clark College. MIT.

Chris Larsen: Former CEO, co-founder, Ripple. CEO, co-founder Prosper and E-LOAN. Chris serves at the Board and Advisory levels at numerous companies and organizations including: Betable, CreditKarma, and Electronic Privacy Information Center (EPIC.) Stanford.