Pinsent Masons

OPEN IDENTITY EXCHANGE White Paper

DIGITAL IDENTITY: HOW TO APPROACH LIABILITY

May 2020

Angus McFadyen
Pinsent Masons LLP

OPEN IDENTITY EXCHANGE

The Open Identity Exchange (OIX) is a technology agnostic, non-profit trade organisation of leaders from competing business sectors focused on building the volume and velocity of trusted transactions online. OIX enables members to expand existing identity services and serve adjacent markets. Members advance their market position through joint research and engaging in pilot projects to test real world use cases. The results of these efforts are published via OIX white papers and shared publicly via OIX workshops. OIX members work together to jointly fund and participate in pilot projects (sometimes referred to as alpha projects). These pilots test business, legal, and/or technical concepts or theory and their interoperability in real world use cases. OIX operates the OIXnet trust registry, a global, authoritative registry of business, legal and technical requirements needed to ensure market adoption and global interoperability.

Contact:

Nick Mothershaw, Chair & Chief Executive

nick.mothershaw@openidentityexchange.org

PINSENT MASONS LLP

Pinsent Masons is a full-service international law firm. We respond to the pressures and opportunities facing businesses globally with legal excellence and innovation.

With office locations on four continents, wherever your commercial interests take you, we have the footprint and expertise to provide support. We recognise that giving a first class service goes beyond just legal excellence. A deep understanding of local cultural and commercial issues, and an innovative approach, underpins all of our advice. We understand the key political, economic, commercial and regulatory issues, helping to minimise risk and maximise opportunities.

We provide a strong local presence with an excellent understanding of the local market, backed up by our innovative technologies and global resources.

Contact:

Angus McFadyen, Partner

angus.mcfadyen@pinsentmasons.com

CONTENTS

1 INTRODUCTION

Growing the digital economy relies on digital identity. We must therefore eliminate the barriers that exist.

Two significant barriers to greater adoption of digital identity are whether:

- it fits within the regulatory regime applicable to the relevant use case, and
- the volumes of digital identity that any individual Scheme or IDP can bring will make adoption sufficiently compelling.

If those can be overcome then the debate quickly turns to risk of using digital identity and the level of trust in digital identity. Liability can be a key part of this and we seek to tackle it through this paper, developing a positive debate on it alongside wider aspects of reliability.

The lead author of this paper is Angus McFadyen, Partner and technology lawyer at Pinsent Masons LLP. This paper is based upon the output of a working group of 26 participants representing a range of roles in the digital identity ecosystem. This working group was formed as part of the Open Identity Exchange (OIX) and TechUK joint programme of work – the Economics of Identity. Organisations represented on the working group included the following, in addition to a number that preferred to contribute on a "no names" basis:

IdenTrust	Cabinet Office
Mvine	ID Crowd
Barclays	Locke Lord LLP
Post Office	Idemia
Experian	Condatis
tScheme	Consult Hyperion

This paper is also informed by an open survey extended to a wider group of interested persons, including the members of OIX and TechUK.

Our survey: 77% survey respondents involved in either providing or adopting digital identity have experienced liability as a significant issue.

Throughout this paper we use the terms set out in the glossary at Appendix A.

OIX and Pinsent Masons would like to thank the working group participants, and all others, that have contributed to this paper.

2 HYPOTHESIS

Expectations regarding liability by those in the digital identity ecosystem can often be mismatched, creating a gap, with imposing liability sometimes seen as the solution to risk (acting as an insurance or guarantee). This paper seeks to close this gap by examining:

- who is active in the digital identity ecosystem, their key liability concerns, and the two main categories of liability;
- to what extent can an identity be trusted when it is presented (often referred to as "asserted") and sought to be trusted and relied upon by another to make a decision or form a relationship, how does this differ by use case, and what are the liability consequences of trusting a fraudulent or incorrect identity;
- what liability should underlie the trust placed in those who deliver digital identity services, and what other key factors should form the basis of trust; and
- overall, building on the above, whether there is a lens that can enable more positive liability debates and move a large part of that debate to the topic of reliability.

If such a lens can be found then this would be considered a big win by many in the digital identity ecosystem – lowering the barriers to adoption of digital identity. A summary of our recommended actions to achieving this is below:

SUMMARY OF RECOMMENDED ACTIONS

Action 1. All must openly debate Scheme suitability. This must be supported by greater transparency and consistent terminology across Schemes to avoid the default position of relying upon liability to solve a mismatch.

Action 2. Legislators, regulators, and industry bodies, must: increase explicit recognition of digital identity solutions as an acceptable approach to identification and verification; and, change laws, regulations and guidance that inhibit the use of digital identity by making them technology agnostic in line with recent legislative trends.

Action 3. Schemes need to examine the suitability of their audit trails, testing these against scenarios to ensure that there is a reasonable balance between the ability to identify error (and, where relevant, fault) and the need to protect privacy and ensure data minimisation.

Action 4. Build transparency into Schemes, finding consistent means of constructing Trust Frameworks, and using Trust Marks.

Action 5. Schemes need to clearly define a value and liability proposition that is simple, transparent, and fits the use cases that it is suited to. This may include zero or fixed liability models where appropriate.

Action 6. All must engage in liability debates through a lens that brings in the full context, avoiding approaches that can place risk that can be addressed through practical measures above the potential benefits.

This paper is not limited to the UK's digital identity ecosystem, however, certain aspects of it are based upon the current legal position in the United Kingdom.

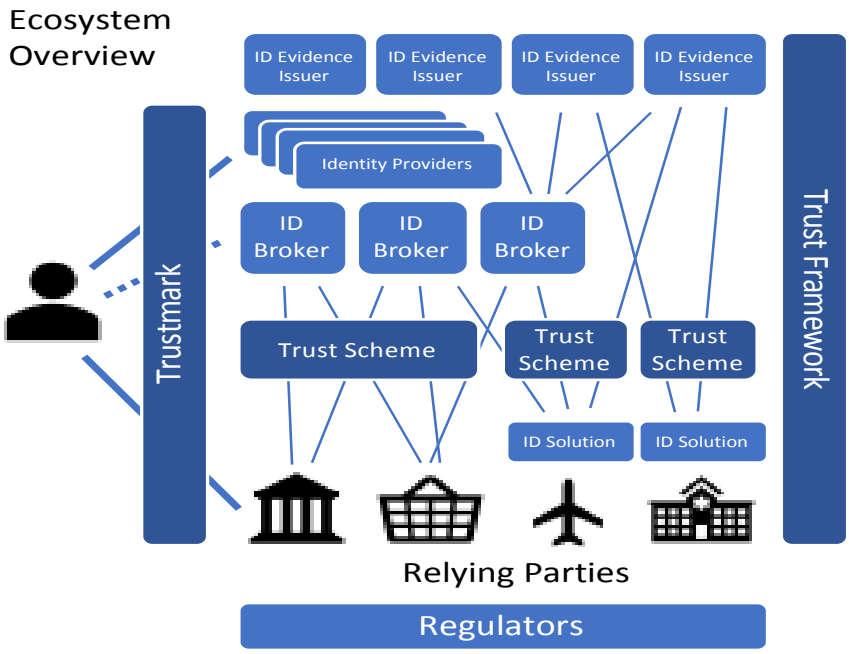
3 THE ECOSYSTEM & KEY CATEGORIES OF LIABILITY

Summary: Those that perform different roles in the digital identity ecosystem all want a successful ecosystem but will have different concerns around loss and liability. This will drive different liability approaches. With those approaches, one of the key distinctions is liability based around an incorrect identity, and liability from other operational matters.

3.1 Roles in the digital identity ecosystem

The digital identity ecosystem involves many different roles. The roles differ between each implementation – for example, centralised and federated models will differ, as will self-certified / self-sovereign models, and one person may perform more than one role.

An overview of the roles that are typically involved is shown below. This focuses on a single Trust Framework and Trust Mark, with several ID Brokers, Schemes and Regulators in the ecosystem. It also includes a specific role for ID Evidence Issuers, who provide evidence and verification services around an individuals ID. In this model Relying Parties might construct their own ID Solutions to meet the requirements of a Trust Framework and Scheme, or might rely on an ID Provider(s) to do this for them. Each of the roles is described in more detail in Appendix 1. Not all Schemes will have all of these roles.



In addition to what is shown above there would also be a number of ID Technical Service Providers (IdTec) supporting those in the ecosystem – IdTec Providers are rarely part of the wider Trust Framework as they would normally only be contracted to the RP / Scheme Operator / IDP / IdEI that appoints them. Rules around the suitability and requirements for IdTec Providers may however form part of the Trust Framework to support overall levels of trust in a Scheme.

3.2 Contrast with offline (i.e. manual, paper, eyeball) identity checks

The roles shown above are, in many cases, applicable to the offline identity checks that have been operating for many years. However, those offline processes do not require such a well defined

ecosystem and largely rely upon implicit trust. There is either little or no liability, or Trust Framework, supporting offline processes.

For example, offline, HM Passport Office (in the role of ID Evidence Issuer) will never know when a paper passport is presented to assert the identity of a User when starting a new job with its employer (a Relying Party) in the offline processes - equally, there is no explicit acceptance of liability by HM Passport Office or detailed disclosure of processes that have been followed. Trust is implicit, relying upon the quality of the processes that the general public and businesses believe are applied, and the fact that passports have generally been accepted for many years as a means of identification and verification.

Objectively, can this implicit trust be said to be better than trust built through adherence to (including certification or confirmation against) a defined regime? There is recognition, including through organisations like the Financial Action Task Force / FATF, that the transparency and assurance achieved through such a defined regime can give a better outcome.

3.3 Typical liability related concerns

What we observe with the increasing adoption of technology services in general, and the same is true with digital identity, is that many concerns are the same for offline and online / digital identity – certainly for Users and Relying Parties. It is with the move to digital identity that these concerns, and the distinctions between the roles in the ecosystem, come into sharp focus.

We also see concerns around complexity, openness / transparency, automation, and reliability being raised by all around online ecosystems. Liability is a component part of all of this, supporting the overall trust that all those involved in online ecosystems like digital identity need to see evidenced.

Reflecting upon this and from the perspective of each role engaged within a Scheme, we have identified some of the key liability related concerns below – it is these concerns that often underlie liability (and, by extension, trust) debates around digital identity.

	Liability related concerns
Users	Concerned about identity fraud – someone assuming or misusing their digital identity or Attributes – and other misuse of their data. (When we refer to Users, we are generally referring to humans or corporates – a User could also be a device with a distinct identity.)
Relying Parties (RPs)	Concerned that reliance on incorrect or fraudulent identity might result in significant losses due to fraud, and/or render them liable to individuals whose identity may have been stolen. Concerned that regulatory obligations may not be complied with by the use of digital (rather than more traditional) processes. Concerned with non-availability of an IDP (e.g. through security compromise) meaning that Users cannot access their accounts.
Identity Providers (IDPs)	Concerned that some Digital Identities or Attributes that they support may be incorrect or fraudulent, and that reliance on them may result in loss being suffered by Users or an RP for which they are held liable. Concerned about the service and related data being misused.

Identity Evidence Issuer (IdEI)	Public and private sector bodies (e.g. HM Passport Office, DVLA, credit reference bureau) who are concerned that release or use of the information that they provide might be used in unexpected ways, violate laws applicable to them (e.g. GDPR[1]), or otherwise expose them to risk of fines and penalties. Also having similar concerns to the IDP regarding incorrect or fraudulent Attributes, although Attributes are often provided with limited or no claims of accuracy.
Scheme Operator	Concerned about having a commercially sustainable Scheme that is safe, secure and trusted.

Beyond financial loss, all ecosystem participants are concerned about reputational damage that can be suffered – imposing liability could offer some compensation but will never solve that concern as it is unlikely to restore (or, better, prevent) the damage. Wider issues around trust that go towards reducing reliance on liability, and that are touched on later in this paper, are key to consider.

3.4 Key categories of liability

To frame the liability analysis through this paper we need to get into what we mean by liability. Liability is a term that is too often used to talk about any risk. Here, we look at it in two overarching categories:

	Description	Examples
Transactional Liability (aka processing or incorrect identity liability)	Liability that may arise in the context of identification or verification process.	Liability resulting from incorrect information / Attributes, defective processes / procedures related to the assessment of Attributes, or an invalid or fraudulent digital identity.
General Liability	Liability related to wider (non-Transactional) operations.	Liability resulting from a breach of security around one digital identity, or a database of multiple Digital Identities.

Further categorisation is required beyond this but breaking the issue in two enables a better debate.

Given the focus of the concerns around digital identity (as outlined above), we see that the key to unlocking the liability debate is addressing Transactional Liability, and doing so in a manner suitable to each Scheme having regard to the interests of all participants, and the use cases it supports.

It is our view that being able to pass through Transactional Liability between Scheme participants is not essential to establishing trust in a Scheme; it is specific to each Scheme.

General Liability on the other hand is typically a category that is easier to resolve given the parallels that many of the associated risks have in other technology based services.

[1] Regulation (EU) 2016/679

4 TO WHAT EXTENT CAN AN ASSERTED IDENTITY BE TRUSTED?

Summary: Not all Schemes and digital identities suit all use cases or risk appetites. It is important to understand and communicate these differences to enable IdPs and RPs to work together, and for digital identity to not be misconstrued as an "insurance" or infallible solution. If this is done then a better debate around liability – based around the proper delivery of service – can be had.

4.1 Not all Schemes or Digital Identities are the same

The nature of identification and verification will vary by Scheme and use case – some use cases will (due to regulation or the consequence of identity fraud) be subject to stronger levels of verification to achieve the required level of trust and regulatory compliance.

Different Schemes are calibrated in this respect (and Digital Identities within individual Schemes may also be so calibrated), meaning that they will be more suitable to some use cases than others – features such as the range and source of Attributes, how Attributes are evidenced, and how regularly they are checked / refreshed are all examples of how Schemes are differentiated. Examples that illustrate this include:

- Gov.UK Verify, originally designed for UK public sector use and recognised under eIDAS;
- Bank ID, originally designed for Norwegian bank use (e.g. account opening); and
- the needs of organisations such as the UK National Health Service, which would both include identification and confirmation of a wide range of broader Attributes (e.g. qualifications, experience, professional development).

4.2 Factors contributing to a trusted identification and verification process

Ultimately, the identification and verification process must satisfy the needs of the RP. Accordingly, for each of its use cases (which, for a retailer, may vary from an age check for alcohol sales to suitability checks for a credit relationship, or KYC checks for financial institutions), the RP must establish reasonable confidence about the identity of the User with whom it wishes to establish or continue a relationship. The RP can use offline checks, digital identity, or a combination of the two, to achieve this. The RP is sometimes in a unique position of continued engagement with the User – some IDPs will only have a one-time or occasional interaction with the User, whereas an RP could have a greater exposure, and so greater data available to it that might indicate User related risk.

With both offline and digital identity processes, in addition to identity abuse such as money muling, there are two principle types of identity fraud that may arise:

- 'theft' where a User impersonates another person; and
- fabrication where a User establishes a new or amended set of identity details that is not true.

There are then also incorrectly issued or relied upon identities that are free of fraud but which carry some of the same risks.

To understand the mitigations against the risks of fraudulent or incorrect identities, thereby supporting trust, the following areas need to be established:

- that Attributes provided by the User come from appropriate sources and describe a 'real' person – i.e. it is strong enough;
- that Attributes don't relate to a compromised identity or appear to have been fabricated – i.e. it is valid and current;
- that the User can demonstrate its connection to those Attributes; and
- that all of the above is done in a tested, reliable, way that satisfies laws, regulations, and standards (including internal standards) applicable to the use cases.

Outside of digital identity, these checks revolve around reviewing paper documents (passports, driving licences and utility bills) and with additional electronic verification available through credit reference bureaus or proof of funds checks.

4.3 Standards for establishing trust

A significant number of organisations currently see digital identity verification as more risky than offline processing. This is despite the known challenges in training staff effectively and the variability of accuracy and consistency offline.

Our survey: 25% take this view and 64% see it as more risky than other IT services.

It is true that aspects of digital identity, particularly when you consider scaling, present different risks – these are considered further in section 6.

Currently there are no generally accepted (cross-industry) standards defining the exact process for performing or scoring 'satisfactory' checks or being able to trust a verification process. There are isolated examples of sector or use case specific guidelines but these are rarely comprehensive or limiting. Instead, such as for RPs governed by current European money laundering legislation (which includes the financial sector, legal sector and others like estate agents):

- a risk-based approach is often applied and this allows proportionality to guide but also leaves uncertainty;
- in the UK we have the benefit of detailed guidance from the industry wide Joint Money Laundering Steering Group (JMLSG), which is approved by HM Treasury – as such, adhering to it is seen as the main approach to follow.

That said, even with JMLSG, digital identity solutions have only been recognised in updates proposed in early 2020[2] and these updates provide little guidance on selection of appropriate solutions. Whilst the recognition is positive, the choice of solution is seen as potentially exposing any RP that adopts them to regulatory enforcement action for relying upon unsuitable processes – this slows the market, but should change given recent developments in those laws.

Whilst considering use cases under European money laundering legislation, it should be recognised that the legislation allows for "reliance" – this is where one RP is able to rely upon a confirmation of the User's identity from another similarly regulated person (here, the IDP). "Reliance" from this perspective can lead to confusion given that the word is used across the industry. This is important to recognise as "reliance" under European money laundering legislation:

[2] As at May 2020, the JMLSG is consulting on these updates. It is expected to confirm the updates later in 2020. Feedback has been provided to the JMLSG that Scheme suitability and reliability are key factors, with eIDAS or other recognition being one of a number of means of demonstrating this.

- comes with potentially boundless liability for that IDP. This means that it is not viable in a commercial context (it is typically only used intra-group where liability risk is contained by the close relationship of those in the RP and IDP roles);
- must be seen as distinct from almost all digital identity solutions, even where a regulated person is acting as an IDP, as it is a different form of regulatory solution; and
- even where it is relevant, does not remove the need for suitability and reliability assessments by the RP.

Other examples of relevant standards include: eIDAS based assurance levels (low / substantial / high); PAS499; PAS1296; BBFC guidelines; DBS; and, UK Government's Good Practice Guide 45.

4.4 Developing improved standards recognition for trust

If the verification capability (including error rates) available through digital identity are examined and compared to offline processes, the technology is demonstrably there to enable more efficient and effective risk based identification and verification decisions. Simple demonstrations of this focus on consistency and throughput capability.

Positive steps have been taken to recognise this by legislators and regulators, but only in limited ways – for example, the latest European money laundering legislation MLD5[3] allows customer identification and verification through "*reliable and independent source,* including*, where available, electronic identification means, relevant trust services [under eIDAS]…or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities*".

However, many legislative and regulatory barriers remain and this can lead to inertia in the market – for example, the Home Office's guidance[4] on age verification for the sale of alcohol requires identity evidence to feature a "*holographic mark or ultraviolet features*", which is not possible for a digital identity product.

4.5 Not meeting the appropriate standard for trust

If a Scheme or digital identity is applied to the wrong use case, or a fraudulent or incorrect digital identity is used, then the impact of that is linked to the use case involved. In some use cases, and circumstances, the impact will be trivial – in others it can be contained by other protective measures or analysis – in the worst case it can lead to material ongoing loss for Users and RPs.

That risk of material loss exists today and is not unique to digital identity.

Taking one of the more highly regulated use cases, the example given below illustrates the risks and losses that may be suffered by a bank (as an RP) accepting a User who has a fraudulent identity:

	Example – identity fraud in Bank customer on boarding
Law that binds the RP	• EU Money Laundering Directive (**MLD5**) • UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 • UK JMLSG Guidance

[3] Directive (EU) 2018/843 – MLD5 – see Article 1(8)
[4] Home Office: Revised Guidance issued under section 182 of the Licensing Act 2003, April 2018

	Example – identity fraud in Bank customer on boarding
Risks faced by the RP	• Credit risk (non-payment) • Fraud risk (money laundering, loss of funds, used to support further identity checks leading to fraud on others) • Regulatory risk (penalties, damages or fines from the failure to meet legal obligations) • Damaged reputation (reduced business or loss of customers) • Criminal offences
Financial loss that the RP could suffer	Greatest likelihood at the top: • Loss of capital / funds (for example, where a credit card is issued) • Paying damages to impacted persons • Regulatory investigations, fines, and undertakings • Loss of profit linked to reduced business

Taking a less highly regulated use case, the example given below illustrates the risks and losses that may be suffered by an online retailer (as an RP) accepting a User who has a fraudulent identity:

	Example – identity fraud in online age restricted sales
Law that binds the RP	These will vary depending upon the product type, with examples including: • Alcohol: The Licensing Act 2003 • Cigarettes: Children and Young Persons (Sale of Tobacco etc) Order 2007 • Movies / content: Video Recordings Act 1984
Risks faced by the RP	These risks are typically restricted to cases of persistent failure, lack of reasonable due diligence / measures, and where action has not been taken in response to regulatory support or warnings: • Criminal offences • Suspension or loss of licence to trade • Damaged reputation
Financial loss that the RP could suffer	Greatest likelihood at the top: • Fixed penalties and fines • Loss of profit linked to reduced business • Potential civil law suit

Given all these risks and potential losses, we must start to examine where responsibility should fall. As a generalisation, this can be seen as follows:

	Responsibility	Who shoulders this
Type 1	Selecting an appropriate Scheme and type of digital identity for the use case, and ensuring that it continues to be appropriate.	RP, with the support of Regulators.
Type 2	Complying with the requirements related to the Scheme (including General Law, Specific Law and Contract).	Each ecosystem participant (RP / IDP / IdEI / Scheme Operator) within its sphere of control.
Type 3	Other events / uncontrollable external events.	Each in respect of its own business.

This generalisation reflects the typical position applied to technology services worldwide.

4.6 Digital identity as business insurance

There must be no expectation that any Scheme is able to say that all Digital Identities managed or issued by it are valid, with no potential for error or fraud. Digital identity cannot remove this risk. Attributes such as government issued passports or IDs that support digital identity are themselves subject to error and fraud, and layering technology on top will not remove (although can improve) this.

That said:

- if suitable controls are in place to manage technology and scale related risks as a whole, digital identity is capable of being more efficient and effective in detecting error and fraud than offline equivalents when used at scale; and
- digital identity may, in some cases, not provide the whole solution – for example:
    - some Users may be unable to generate a sufficiently verified digital identity;
    - if digital identity is used for new customer on-boarding, then it may not provide all of the required information (e.g. telephone numbers, tax / NI numbers) and so top-up processes will be required;
    - RPs will typically have many more points of engagement with a User than an IDP and so have the ability to apply additional controls; and
    - under many regulatory regimes RPs are unable to discharge themselves of the need to maintain oversight of services that they rely upon.

What is rarely recognised is that there is either little or no liability model, and no comprehensive Trust Framework, supporting offline identity processes. That is despite the fact that they are widely relied upon at scale. For example:

- a financial institution that conducts a face to face interview involving checking a customer's identity;
- the customer presents a UK passport as evidence and the interviewer takes a copy of the passport and visually checks the document as part of the identity check;

- the customer is subsequently accepted;
- at some point in the future it transpires that the passport is a fraudulently obtained genuine document (FOG); and
- the institution will not go back to the UK Passport Office demanding compensation for any losses that may have been incurred as it knows that it will have zero prospect of success.

Digital identity cannot be seen as a business insurance policy or a guarantee of outcomes, though it can form an important part of an improving process and controls approach if we break through the offline inertia.

4.7 Call to Action

Action 1. With the support of OIX's work based upon interoperability, we call on all those engaged in the digital identity ecosystem to openly debate the suitability of particular Schemes, and Digital Identities within each Scheme, to specific use cases. That can be delivered through transparency. Achieving transparency will involve a move towards a single more consistent terminology for describing digital identity and suitability. Through those efforts, we can increase understanding and, consequently, trust in digital identity without creating a time consuming comparison between Schemes by each potential RP.

Action 2. With the support of OIX's work on sector analysis and engagement, call on legislators, regulators, and industry bodies or groups, to:

- increase explicit recognition of digital identity solutions as an acceptable approach to identification and verification; and
- change laws, regulations and guidance that inhibit the use of digital identity by making them technology agnostic in line with recent legislative trends.

Through this we can reduce concerns around liability being incurred due to the use of unrecognised systems and processes, consequently increasing trust in digital identity.

5 WHAT LIABILITY SHOULD UNDERLIE TRUST?

Summary: The law that impacts digital identity leaves a significant gap that should be filled by a well constructed contract. Within that contract, rules around the proper operation of service and (conscious of privacy) the need to maintain logs/records will be core to an effective liability regime (potentially with a reverse burden of proof where this is not done in the agreed manner) – a regime that we would typically see being based around faults in the service (rather than one which guarantees the absence of identity fraud) and aligned to the use cases that it supports. Liability debates are, however, no substitute to understanding how a scheme operates and reduces the risk of identity fraud and other errors arising.

5.1 Sources of liability rules

The basis of liability in the context of digital identity is not consistent from country to country. There are, however, themes and concepts that can be applied to frame debates in a relatively consistent manner. That includes the Transactional Liability and General Liability categorisation outlined in 3.4. It also includes the framework referenced in previous OIX analysis for identifying the source of relevant laws - this is developed below:

	General Law	Specific Law	Contract
Source	Set by legislators, courts (in common law jurisdictions, such as the UK and Ireland), and Regulators		Set for the Scheme
Applies to	Everyone across the jurisdiction	Identified participants in the digital identity ecosystem – as defined by the law	Participants that agree to be bound by the contract
Examples live in the UK	GDPR, consumer contract law[5], criminal law (e.g. fraud)	eIDAS[6], MLD5, Licensing Act 2003	Contracts that govern each Scheme (part of the Trust Framework)

Internationally, there are very few "Specific Laws" for digital identity – as with many areas where technology is developing at pace, it can generally be observed that the laws that apply are the General Law principles that apply to many other activities. Whilst product liability laws are increasingly extending to systems that are embedded within physical / hardware products, we are not yet in a place where they extend to online services such as digital identity (the focus is on those with a higher risk such as autonomous vehicles).

With an ecosystem as complex as that for digital identity, in our view it is rarely possible or commercially desirable to rely upon the existing General Law and Specific Law to make up the Trust Framework for a Scheme – Contract is a key component to enable trust. This is likely to remain the case, even where General Law and Specific Law can provide material components of the Trust Framework, for example:

[5] Such as the Unfair Terms in Consumer Contracts Regulations 1999
[6] Regulation (EU) No 910/2014

- for solutions that use open banking systems that operate under the European payment services directive (PSD2)7 we will not have a commercial model unless this is added by Contract to the Trust Framework; and
- eIDAS provides a framework for (amongst other things):
    - digital identity interoperability in the public sector, cross-border; and
    - the provision of trust based digital services,

in each case, establishing liability principles (based around fault and the burden of proof). However, it expects Contract to guide these principles and allows liability regimes to be built through Contract.

Liability is typically based upon a duty being breached

Whilst there are liability models that establish liability regardless of fault or intention being evidenced (typically referred to as "strict liability"), these are rare in the commercial context outside of the insurance market and specific areas of harm (such as nuclear power). This is true internationally where strict liability under General Law or Specific Law is largely unknown for technology / computer systems. This is partially due to the limiting / cooling effect that blanket strict liability can have on a market – it increases the risk of relevant business and reduces the availability of insurance.

More often, liability is "fault based" – this means that it is tied to:

- a duty or contractual obligation that has been breached; and
- losses that are suffered as a result by the person to whom the duty or obligation is owed.

Within the applicable laws there are then typically rules on what losses can be recovered, and obligations on relevant persons to minimise / mitigate the losses.

Alternative models of liability, such as pooled liability (referenced later), are also possible but are largely discounted at present as a solution for many countries given the current size and maturity of the digital identity market. We see insurance as the most viable means of supporting current liability demands.

It should also be noted that the term "negligence" and associated duties operate differently between countries – generally, in this paper, we avoid use of that phrase and instead refer to breach of a duty by the person that owes that duty (or contractual obligation).

5.2 Liability constructs around identity

For those that run offline identification and verification in-house or, if outsourced, as part of wider business process outsourcings, the liability that:

- the RP is exposed to will be defined by the General Law and Specific Law that it is subject to, and any Contract with its customers; and
- the RP could pass through to another person (where there is an outsourced element), such as an IDP or IdEI, will almost certainly be based upon the principles of fault linked to duties and negotiated liability positions set in Contract.

With digital identity, the exposure and ability to pass through is largely the same. The duties that could be breached between an RP, Scheme Operator, IDP and IdEI, in relation to Transactional

[7] Directive (EU) 2015/2366

Liability are most commonly established (or, if not established, then subject to controls) in Contract through the Trust Framework for the relevant Scheme. The Contract established through the Trust Framework will also seek to guide the application of General Law and Specific Law so that commercially agreed financial limitations and exclusions are applied - although note that certain duties and liabilities under General Law or Specific Law cannot be limited.

We see a fault based liability model that distinguishes between Transactional Liability and General Liability as most appropriate – and Contract as the means of achieving this. This is primarily because:

- it supports an appropriate allocation of responsibility in line with 5.3;
- it enables proportionate risk to be assumed by each party in accordance with allocations of risk agreed in the Contract (which in some use cases, and in respect of some risks and losses, will involve exclusions and limitations, but not always); and
- the consequent proportionate risk allows businesses to be run, insurance to be purchased, and investment to be made, within the digital identity ecosystem.

We do note, however, that some countries (when compared to the likes of the UK, the United States or Canada) have a wider system of General Law that reduces the flexibility that can be available to largely control liability through Contract.

This treatment is consistent with the trust models adopted in a number of other digital identity Schemes - both in the UK and internationally. A limited number of these examples are outlined in Appendix B.

With both a strict liability and fault based regime, there are options in terms of fixing or limiting financial exposure where a relevant event arises. We explored through the working group and surveys having fixed levels of Transactional Liability - for example, a payment by an IDP of £x for each incorrectly issued digital identity or incorrect Attribute, rather than liability being linked to losses suffered. The view is that this is viable but not preferred – this, as well as pooled liability models, should be considered over time as the ecosystem develops.

Our survey: 64% favoured proportionate, loss based, liability (potentially with limits); 21% favoured fixed sum liability, irrespective of losses suffered – this has the benefit of simplicity but loses proportionality; and, 15% favoured a zero liability model, presumably to reduce costs and use case dependent.

If liability is based upon fault (whether proportionate or fixed in terms of the amount recoverable) then it is necessary to be able to prove the fault and legal responsibility for it, under the applicable General / Specific Law. Below we consider the fault principle in a General Liability scenario and then look at the concerns around evidence.

5.3 Scenario of a fault based regime in General Liability (security breach)

Security is a key concern of every role in the digital identity ecosystem. Looking at it in the context of General Liability illustrates how it and many similarly categorised risks would be treated. This scenario is an indicative illustration rather than one that seeks to identify the full range of losses or claims / cross claims that could arise in such a complex scenario.

(A) **Scenario overview**	A database containing the data for multiple Digital Identities has been compromised with access falling to a nefarious actor. (Assume for the scenario that this is a full compromise, which should not occur

	in a well secured system.)
(B) **Source of relevant duty?**	General Law: EU GDPR, which may give two categories of duty: (i) those directly imposed by GDPR, and (ii) those which GDPR mandates are included in certain Contracts. **Specific Law**: Sector and data set dependent, which may impose an obligation to notify affected individuals and regulators within set times. **Contract**: Agreed security procedures and terms supporting General / Specific Law.
(C) **Is a duty breached?**	A security breach may or may not represent a breach of a duty. A duty will rarely expect perfect outcomes - proportionality is key. In particular, GDPR doesn't, and neither would most Contracts, expect there to be no risk of this Scenario arising but they would each expect particular proportionate protective measures to have been taken by reference to the state of the art. So, we must break this scenario in two – first, where there is a breach of the duty (i.e. fault); second, where there is not a breach of a duty (but the scenario has nevertheless occurred).

(D)(i)
 	
Fault
	This could arise where a person (which we will assume is the IDP, but it could be an RP, Scheme Operator, IdEI or TSP) has not complied with its duties to implement appropriate security measures.
	
	• **User impact**:
	  ○ A new, or re-verified, digital identity may be required.
	  ○ Potential distress or financial loss stemming from the security breach, including identity fraud and reduced access to employment / services / finance (through damaged credit scores, being linked to a breached identity). This may take a long time to be resolved. Users could potentially claim from any ecosystem participant that it has a relationship with.
	• **IDP impact**:
	  ○ The IDP may be obliged to notify, compensate Users, and/or offer protective measures under GDPR, depending upon the nature of the breach / impact.
	  ○ The IDP may also be required to support the action for the Users noted above and support RP liability as noted below.
	• **RP impact**:
	  ○ Reverification of the User's new or reconfirmed digital identity with the RP may be required, depending upon the Use Case – for example, if the digital identity is used once at onboarding then this will not be relevant. (Time / cost.)
	  ○ Possible losses stemming from use of compromised Digital Identities by the RP where the compromise is not detected for a period of time.
	  ○ Compensation for loss suffered by the RP would probably be made as a claim under Contract against the IDP for breach of duty, and so

	is subject to the agreed position as well as the General Laws on what losses are recoverable and what mitigation measures expected of the RP. • **IdEI and Scheme Operator impact**: This is more limited and will be specific to the scenario. Incident response will remain an important matter for these and all others in the ecosystem (including TSPs). GDPR would offer limited recourse between participants in the ecosystem – generally such liability would rely upon Contract. The limited recourse of GDPR is focused on properly apportioning liability incurred to the affected Users where multiple parties are at fault[8]. There is also the possibility of fines being levied under General Law such as GDPR. Generally, these should be expected to be applied based upon conduct and the fault (or innocence) of each party that the relevant regulator has authority over. Principles of General Law (in the UK, under case law) can prevent claims to pass fines and other such conduct based losses imposed by law to others.
(D)(ii) **No fault**	This could arise where a person (which we will again assume is the IDP) has complied with its duties to implement appropriate security measures but the nefarious actor has used sophisticated measures to effect the compromise. User and RP impact: Same as for (D)(i) (fault), but unlikely to be entitled to compensation (this would be ex gratia / voluntary). As there is no fault, liability is unlikely to follow under most Contracts but other obligations (such as notification) will remain. This is a scenario where the impact on the RP may be significant due to the need to re-verify potentially a large number of Users at its own cost. There are mitigations to this risk: Due diligence and ongoing assurance over the security measures that are in place within any Scheme that is adopted. This can be supported by Scheme Operators (where there is one) requiring participants in their Schemes to obtain certification or to report on security testing that is periodically required. Insurance, in particular cyber risk insurance, is an increasingly relevant mitigation. Careful attention is required to the nature of the policy to ensure that it would support a cyber incident affecting a supplier, which should be the case for an effective policy. Maintaining cyber incident response procedures, and testing them periodically, to ensure that it can effectively mitigate the effect of a data compromise. Support in this respect is sometimes bundled with insurance.

[8] GDPR – see Article 82: "(1) Any person who has suffered material or non-material damage as a result of an infringement of [GDPR] shall have the right to receive compensation from the controller or processor for the damage suffered. (2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation… (3) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. (4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. (5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2. (6)…"

(E) **Timing**	Finally, there is also an important issue around the time gap between the event, it being detected, it being understood, notification and containment (which may not always run in that order). Notification is an important feature of enabling others in the ecosystem to mitigate the effects of a security breach, but there are important questions around how well understood the breach needs to be before notification, the speed of notification (noting that there are some fixed timelines in legislation) and what information is provided – if this is mismanaged then losses can continue unabated and confusion can spread.

As is noted elsewhere in this paper, this scenario illustrates an allocation of liability that is common in the technology and service industries – very little is unique to digital identity in terms of principles. What can be unique to digital identity, however, is the nature and scale of the impact on the User and (arguably less so) the RP.

We must ensure that such impact is carefully analysed in designing and operating Schemes (including against the backdrop of data minimisation, and security, principles) so that the impact of any potential security breach (regardless of fault) is limited to best protect the User – both the immediate and longer term. This extends to looking at how compromised Attributes can be identified and rectified, how shared signals / intelligence can support the prevention of identity fraud, and communicating to the Users what they can control (e.g. updating address details when moving home).

5.4 Evidencing fault and the burden of proof

Once a liability approach is settled, one of the most important areas for debate is how it could be shown that a duty has been breached. This involves looking at:

- what evidence (i.e. data) is available; and
- who that evidence is available to.

Digital technology related laws (such as the European-wide PSD2[9]) is increasingly looking to shift this burden to the person that is relying on technology to deliver a service to its customers/users – whether that's appropriate in digital identity is an open question and, in our view, such a shift should be limited to areas of real harm (such as autonomous vehicles). As such, debates in digital identity should focus on what records / data are collected, and how this is held, to support any question of liability. Only if there is a breach of the duty to maintain or provide access to such records, and other evidence is not available, should a liability shift (reverse burden of proof) be considered in our view – this is an issue that is being debated much more generally, internationally, with the rise in capability and use of robotic processing and artificial intelligence.

That debate must be conscious of the principles of data minimisation and privacy which will cut across a perfect evidence trail and may push a reliance on non-personal data (potentially metadata). The data that is held within a Scheme should not increase the potential for User harm, or a reduction in User trust.

[9] Directive (EU) 2015/2366 – see Article 72(1): "…the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge…"

5.5 The limited effectiveness of liability models

Whatever liability regime is established, it must be recognised that liability is an after the event backup protection. It is at least as important to focus on preventing liability from arising - that is a matter where interests are fully aligned across the digital identity ecosystem. Any liability debate should have this in mind.

As such, debates on liability should be held in the context of the overall trust model and questions such as those below should be considered:

- Governance: How does the Trust Framework induce the right behaviour by Scheme participants?
- Oversight: How are technical standards established in the Trust Framework monitored and enforced?
- Monitoring: Is compliance built into the systems that underlie the Scheme (e.g. can data sent in an incorrect format be identified and rejected)?
- Resilience: How is resilience built into those systems (e.g. in relation to security risk, disaster recovery, and incident management)?
- Assurance: What due diligence can be undertaken on the systems and the Scheme more broadly, and how is this supported by the Scheme Operator (e.g. by requiring independent certification, or by the Scheme conforming to a Trust Mark)?
- Disputes: How will disputes be resolved and what enforcement action could be taken (e.g. limiting, suspending, or ending, a participant's role in a Scheme where it is a multilateral arrangement)?
- User protection: How will Users be protected if their digital identity is compromised?

Answers to questions like this will enable liability based debates to be held in the context of the real risks that remain to be addressed and the likelihood of those risks arising. It will also narrow the risks where it is relevant to consider liability as part of the solution – there are many risks where practical measures are a better mitigation than the threat of financial recourse.

5.6 Call to Action

Action 3. We call on those that are responsible for Schemes to examine the suitability of their audit trails, testing these against scenarios to ensure that there is a reasonable balance between the ability to identify error and (where relevant) fault, and the need to protect privacy and ensure data minimisation. As the UK Trust Framework is looking to be developed by the UK Government, this is an area where input is required and OIX could create a model policy.

Action 4. We call on all those engaged in the digital identity ecosystem to build transparency into Schemes (again, also as an input into the UK Trust Framework looking to be developed by the UK Government), finding consistent means of constructing Trust Frameworks to ease due diligence and understanding, and consider the use of Trust Marks to assist in this transparency exercise. Through those efforts, we can enable risks, and their mitigations, to be clearly understood which will build trust for each Scheme. This can also be built into principles for Schemes being developed by OIX.

6 A LENS THAT CAN ENABLE MORE POSITIVE LIABILITY DEBATES

Summary: With an understanding of how a scheme operates and its use cases, commercially acceptable liability models can be debated and agreed. There is evidence of this, at scale, globally. Liability must not be seen as the only or primary means of achieving trust – trust is a much wider concept where the importance of liability depends upon the use case and commercial construct of each Scheme. In addition to liability resting with particular participants, we have the opportunity to explore insurance and pooled liability models / disputes schemes as market demand grows for such approaches.

6.1 Building the context

To find suitable liability positions requires a lens that takes in each of the matters discussed above. In summary, this includes recognising and accepting:

- **Categorisation**: A distinction between Transaction Liability and General Liability.
- **Suitability**: Each Scheme and digital identity will suit some use cases but not all.
- **Context**: The liability construct for each Scheme must fit the use cases that it supports, and be captured within a Trust Framework that brings together the General Law, Specific Law and Contract.
- **Roles**: An appropriate allocation of responsibilities must be set out between each role in the ecosystem.
- **Fault and evidence**: A fault based, rather than strict liability, model is generally preferable and enables a fair allocation of risk, provided that it can be supported by evidence and suitable bounds.
- **Public good**: That a vibrant digital identity ecosystem that supports our digital economy will only be blocked by liability positions that do not address the above – we must all collaborate, focusing on reliability alongside, if not over, liability.

6.2 Liability models that are live and successful

There are a number of liability models live in countries around the world. A number of those that we have examined are outlined in Appendix B.

What we observe is that:

- **Zero liability models are viable** for either low risk use cases, or where the quality of trust generated from other features (such as the ID Evidence Issuers) is such as to be able to replace liability - or certainly Transactional Liability - as a protection.

Our survey: 61% said that the liability model should calibrate to the use case and, more, 68% said that the level of assurance/confidence should be the defining factor – there is typically a correlation between use case and assurance / confidence levels. This calibration may inherently be achieved by a model that links to fees per transaction.

- **Fault based liability is typical**. Commercially appropriate and legally valid exclusions and caps on liability are in place. Only those that have a particular construct or circumstance (e.g. the procurement process behind Gov.UK Verify) have positions that would rarely be

recognised in the context of other commodity / scalable technology services (e.g. cloud services).

- If a Scheme or digital identity is **used outside of its stated purpose, the RP should take the risk** and responsibility of doing so through the liability mechanism.
- Whilst liability is a complex topic, **liability models need to remain simple and aligned to use cases**, to be transparent and effective.

We consider that there is no reason why more Schemes should not build on similar or potentially simpler models. We outline below how a number of the concerns raised earlier in this paper could be addressed through such models:

	Liability related concern	**Example approaches**
User	Identity fraud and misuse of data	A data security breach, or misuse of data, could stem from any participant. Equally, any participant with access to data could theoretically misuse that data (e.g. for unsolicited marketing). This is addressed by the way that (in the UK and EU) GDPR applies to 'controllers' and 'processors', providing for duties to be owed directly to Users – the solution for the Trust Framework is to support this (e.g. through appropriate privacy policies and security standards) but there may not need to be new User facing liability mechanisms depending upon the Scheme and the potential for harm that it presents. Some survey respondents queried whether Users actively engage in liability analysis – focusing instead on the risk of identity fraud and trust more generally (based upon adoption by others and reputation). This may change with a market growth and depends upon the countries / cultures / groups that each Scheme serves.
RP	Faults in the creation of the digital identity by IDPs (Transactional Liability) Faults in wider Scheme operation by IDP or Scheme Operator or IdEI resulting in exposure (General Liability)	Transactional Liability can only be established if there is a standard of service that links to a duty – as such, the Trust Framework must define Scheme operations and quality measures. If these are breached (potentially in a material manner or to any extent) then it is appropriate for fault based liability mechanisms within Contract based boundaries to operate. Typical examples of these boundaries are: • losses directly resulting from the breach of duty by an IDP potentially being recoverable in line with the General Law; • special losses (aka consequential / indirect loss, which does not naturally flow from the breach of duty but which only arises in special circumstances), and sometimes other specific or less tangible loss being excluded, with there also being suitable disclaimers; and • financially capped liability that is proportionate

		and sustainable with different volumes of Scheme use. Service credits / liquidated damages may also be appropriate depending upon the commercial construct. This recognises that participants usually: • want to build a charging model that links cost to the scale of use and nature of service (as such, higher charges could be expected for verification to a greater level of certainty); and • wish not to "insure" business risk by including a significant risk premium on charges.
IDP	Protection from disproportionate liability Recourse for misuse of service or related data	IDP to RP liability is addressed above. IDPs will also have an interest in: • ensuring those that they make Digital Identities available to use those Digital Identities in an appropriate manner; and • suspending / stopping digital identity provision / access to those where it identifies material issues.
IdEI	Recourse for misuse of service or related data	IdEI liability will often be tightly limited or excluded given the commercial interests of the IdEI, and the "distance" between the IdEI and the end use of the Attributes. The IdEI will wish to be able to stop Attribute provision if it identifies material issues in the use of those Attributes – likely supported by liability, although chains of use make this challenging and legislation like GDPR provides greater comfort that those down the chain will act properly.
Scheme Operator	Maintaining a commercially sustainable Scheme	Whilst being unlikely to incur significant losses as a result of issues in the Scheme, the Scheme Operator will wish to ensure that it does not (if it is a multilateral Scheme) incur liability that could result in collapse of the Scheme. The ability to do so will be impacted by the extent of the Scheme Operator's role.

6.3 Pooled compensation model

As well as point to point liability, there are models in other markets where pooled liability is adopted. There is a view that pooled liability (i.e. having a central point for recourse for those that suffer liability) can provide enhanced trust and means of recourse if a responsible party is no longer solvent or not cooperative (although the latter is also addressed through central complaints bodies). Examples of this in the UK include:

- the Dispute Resolution Scheme (DRS) that is being established by the banking trade body UK Finance, to address historic SME banking disputes on behalf of a group of banks; and
- the UK's Financial Services Compensation Scheme (FSCS) which protects against insolvent financial intuitions.

This is distinct from central dispute resolution systems which do not themselves accept liability or pay compensation.

Our survey: 40% of respondents say that a pooled liability model could be the best means of building trust and enabling recourse for Users – with 23% preferring direct IdP liability and others focusing on other aspects of building Trust (e.g. Trust Marks).

The positive nature of a pooled liability model can be described as follows:

- In a use case where a digital identity is asserted in a single domain, such as inside a corporate environment, the liability rests in a clearly defined place and is simple to manage. However, in a use case where a digital identity is asserted across multiple domains, such as multi-company environment, the liability burden is either total on one party or another, or it must be shared across all parties, with evidence of fault potentially being challenging to locate.
- Any repartition of liability must be either equal upon each party or proportionate to the level of influence the party has in the overall transaction. These are difficult to establish.
- Therefore, a pooled liability driven model, where all participants participate in a shared pool from where risk can be hedged and claims for liability can be settled is an option. Lloyd's of London insurance market provides perhaps one of the most prominent examples of such a pooled liability model in action. It is a global and well understood ecosystem. Lloyd's names ultimately underwrite the claims upon the pool in the event that a claim has to be made. In turn, Lloyd's brokers and specialist underwriters working on the floor at Lloyd's write contracts to carry liability for claims. Underwriters and cover holders work together in syndicates.
- Operationally, the smooth working of the London insurance market illustrates how a pooled liability driven model satisfies the needs of all participants in an ecosystem.

A number of participants in the working group are of the view that for as long as a pooled liability driven model for digital identity goes unexplored and unattempted then its potential to solve the liability debates will never be realised. However, it is also recognised that there's significant cost involved in such a model, and key challenges such as the following would need to be tackled:

- Assessing the quantum / value of loss and compensation due for digital identity failings – this is a much greater challenge than for other compensation schemes that can (for example) focus on capital or money that a saver has lost from a bank account.
- The market question of to what extent less robust or less prudent entities should be supported by others.
- How to identify and deal with vexatious complaints or claims in an efficient manner that avoids undue burdens on the market.

In time, the market in various countries may mature to an extent that a pooled model could be viable and provide greater trust, particularly to the User – however, generally, the current scale of, and divergence within, the markets and the cost of such a scheme seem to place it out of reach. That does not mean that the conversation should end there. There should be a continuing debate about the right time to evolve such a model – it could be developed as a full compensation scheme or it could be a backup for when Scheme participants are no longer able to sustain their own liabilities, such as with the UK's Financial Services Compensation Scheme / FSCS.

In the mean time, government backed online dispute resolution services (which operate across a wide range of industries across Europe) are available to consumers to help manage complaints where they access digital services.

6.4 Call to Action

Action 5. We call on those that are responsible for each Scheme to clearly define a value and liability proposition that is simple, transparent, and fits the use cases that it is best suited to. OIX can support this through developing best practice approaches.

Action 6. We call on those that are engaged in liability debates to do so through a lens that brings in the full context, avoiding approaches that can place risk that can be addressed through practical measures above the potential benefits. To do this:

- the overall business case for digital identity adoption (incorporating efficiency cost savings and loss reduction – where sufficiently evidenced); and
- the practical measures within the relevant Schemes,

must be factored into liability debates more than they have been in the past.

APPENDIX A GLOSSARY

These terms are to aid the reader in understanding this paper. Work is ongoing through OIX to consolidate a single set of these terms to improve communication across the industry.

Term	Meaning
Attribute	A characteristic represented by a piece of data related to the User – for example date of birth or address, or data that demonstrates / corroborates other data (e.g. proof of address).
ID Broker	A person who provides access to multiple Schemes but is not itself (in that role) a Scheme Operator, IdP, or IdEI. That person has a contractually binding agreement with at least one IdP and one RP.
ID Evidence Issuer / IdEI	A source of Attribute information, which may include the ability to confirm other Attribute information. This can be public and private sector bodies (e.g. HM Passport Office, DVLA, credit reference bureau)
Identity Provider / IdP	A person able to create, maintain, and manage digital identity information (either made up of, or derived from, Attributes) for Users.
Relying Party / RP	A person that uses an IDP to establish an individual's identity, usually in order that the individual can access a service.
Regulator	A governmental or regulatory body (such as, in the UK, the Information Commissioner's Office) whose rules or oversight a Scheme participant is subject, or a quasi-regulatory or industry or standards body whose rules and guidance Scheme participants typically adhere to.
Scheme	A contractually binding digital identity ecosystem, consisting of multiple parties, with at least one IdP and at least one ID Broker.
Scheme Operator / ID Hub	The person with responsibility for managing or operating the Scheme. For a Scheme with a single IDP this may be the IDP. For a Scheme with multiple IDPs, this will typically be an independent person.
ID Technical Service Provider (IdTec)	A person that supports the technical systems / infrastructure that is used for the Scheme but is not itself the Scheme Operator. That person may be engaged by the Scheme Operator, an IDP, an RP or an IdEI. That person will not have a legal relationship with the User as it only acts on behalf of those that would have such a relationship.
Transaction	The collection, storage, processing, communication, and/or use of information relating to digital identity by or between any of: the User; an IDP; an RP; or, a Scheme Operator.
Trust Mark	A signifier that a product, service, or company, meets an accepted standard of quality as dictated by a Regulator. This is sometimes known as a certification mark or quality mark.
Trust Framework	A set of technical, business, and legal rules, standards, processes, and requirements that govern the operation of a digital identity system and corresponding Transactions. These are Scheme specific but may reference or contain standardised material.
User	A person (which could be an individual or a corporate entity) or thing that wishes to demonstrate its identity.

APPENDIX B EXAMPLES OF LIVE LIABILITY MODELS

	Manual checks	Social media login	Gov.UK Verify	BankID	Aadhaar
Territory	Worldwide	Worldwide	UK	Norway	India
Use cases / users	All offline use	Website login	Public sector (increasingly open to private sector)	Banks	This is a national mandated scheme in which the whole population is enrolled
Structure	No formal structure – recognised by regulators but no underlying trust framework other than contextual. Societal.	Contractual	IDPs contract with a single government body – other public sector RPs sit behind this body. Private sector is subject to bilateral agreements between IDPs and RPs governed by rules of the Trust Framework.	The trust framework of the scheme establishes a direct IDP - RP connection (similar to many payment schemes in the UK).	Government provided ID that may be accessed by approved third parties
IDP - RP Liability model	No liability of document issuers (although may be for those that certify copy documents).	Zero IDP liability.	Generally fault based.	Fault (negligence) based.	Here the government acts as the IDP, although more accurately as an IdEI that others can choose to rely upon.
IDP - RP liability limits and other relevant matters	Zero IdEI / IDP liability – unless otherwise agreed bilaterally. Reliant upon document authenticity and checks run by document issuers. Largely reliant upon industry practice.	Zero IdEI / IDP liability. Limitations on use of data by RPs are set.	Uncapped liability for: fraud, wilful breach; and, breach of cyber security duties. General liability cap in each 12 months. Not liable for loss of profit (a concept not easily applied to the public sector), but liable for specified losses, including wasted expenditure and compensation to third parties. No liability for fault caused by IdEI Attributes. This liability model is a result of a public tender exercise based upon projected volumes.	Unlimited liability if wilful or grossly negligent (a concept that does not transfer easily to all countries). General fault based liability limited to NOK 100,000 per transaction (c. £9,000). If the subject (or Relying Party) fails to fulfil certain obligations they can be held liable for losses that may arise, and claims against the IDP may be reduced or fall away. Reverse burden of proof for certain matters. Exclusion from the scheme is also possible for more material and repeated breach.	Zero government liability. RPs (or connected IDPs) are liable to the government and required to comply with standards.