OIX Guide to Support Services, Complaints and Liability

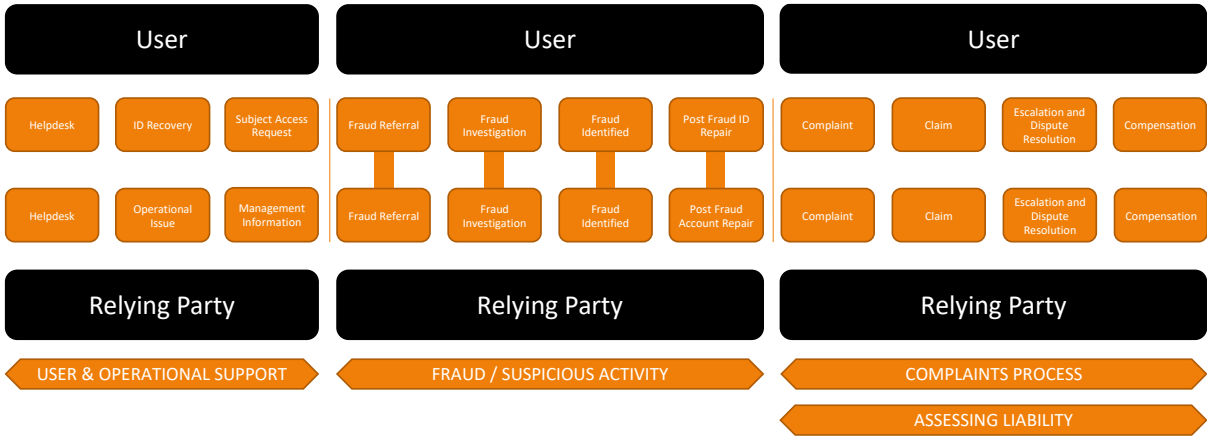
An OIX Guide | October 2022 | Version 1.0

Produced By: Nick Mothershaw, Open Identity Exchange
based on the contributions of the OIX User and Relying Party Services Working Group

Table of Contents

1. Overview

This OIX guide covers the areas of the trust framework that address operational services within the ID Ecosystem. Both user and relying parties are subject to, or trigger, these operational services, or events. From Helpdesk to Compensation. The party that needs to offer the operational services is generally the Identity Provider (IdP). Some services may also be provided by orchestrators.



The guide is organised into four Sections:

- **User and Operational Support**: User Helpdesk, ID Recovery, Subject Access Requests, Relying Party Helpdesk, Operational Issue, Management Information
- **Fraud / Suspicious Activity**: Fraud Referral, Fraud Investigation, Fraud Identified, Post Fraud ID Repair, Post Fraud Account Repair.
- **Complaint Process**: Complaints, Claims, Escalation and Arbitration, Compensation
- **Assessing Liability**

This guide does not define a detailed process for operational management. OIX recommends trust frameworks and schemes require their participants to implement an industry standard operational services management process, such as ITIL.

ITIL describes processes, procedures, tasks, and checklists which are neither organization-specific nor technology-specific, but can be applied by an organization toward strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement. ITIL has is owned by AXELOS, a joint venture between Capita and the UK Cabinet Office. AXELOS licenses organizations to use the ITIL intellectual property, accredits licensed examination institutes, and manages updates to

the framework. Organizations that wish to implement ITIL internally do not require this license.[1]

The full ITIL guide can be found at: https://e-book.business/books/ITIL-Foundation-4%20-edition.pdf

This OIX guide therefore focusses on Digital ID specific considerations within the operational management process.

Users in the context of this guide are human beings, not things.

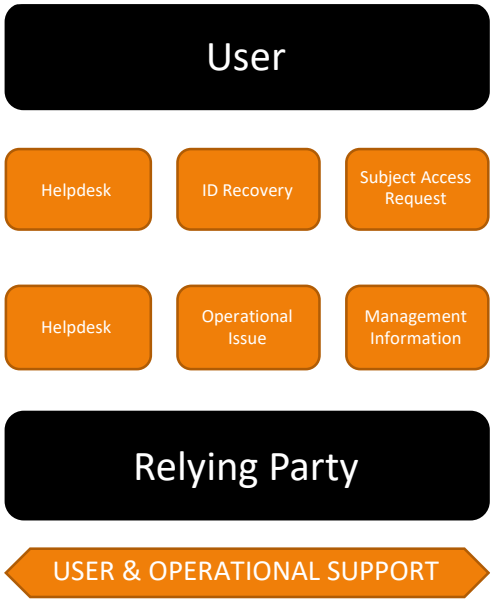
The Intended Audience for this Guide is:

- **Trust Framework and Trust Scheme operators** when designing their own trust framework / scheme. Trust Scheme operators my find this guide of particular use where the trust framework within which they operate does not address the area of operational processes in detail.
- **Accepters of Digital IDs or Relying Parties -** as it enables them be clear about what they may need to consider and do and what they might expect others to do. It will help them configure their participation and make clear to other participants in the scheme what is expected of them
- **Reusable Identity Providers** – who will have a direct relationship with the end user and therefore will need to implement and be held accountable to these operational procedures by relying parties, trust frameworks, trust schemes and the end user themselves.
- **Issuers of credentials** - who may be part of a Digital ID process and may be involved in things like identity recovery and fraud management.
- **Orchestration Providers** – who may need to understand the process flows and events based on the specific scheme operators' rules of the road

Whilst this guide is not aimed at the **end user**, they are the beneficiary of the good process and practice this guide defines.

[1] Extract From Wikpedia entry on ITIL

2. User and Operational Support



2.1. User Helpdesk

A requirement for an industry standard user helpdesk service should be established by the trust framework or scheme. The requirements might the following:

- Which roles in the ID Ecosystem must provide a helpdesk
- Agreed Hours of service
- Response and Resolution times
- Channels for engagement: Phone, Chats, Chat bots, e-mail, online self-reporting etc.
- Languages to be supported
- Accessibility support
- Monitoring and Management Information
- Any regulatory reporting
- Publishing statistics
- Agent vetting and training
- Documented processes and scenarios

Many identity providers will use help desks that provide multiservice support that may cover a wider range of support beyond identity. This should be taken into account when planning for the Digital ID elements of the help service.

From a Digital ID specific point of view, the general problem will be that a user cannot access a service they want to access. The user will probably not know why this is – simply that their ID is not working.

Following user help desk scenarios should be planned for:

User Scenario	Considerations

User unable to achieve a required ID assurance level	ID assurance levels are usually not transparent to users and are often difficult to explain. Users may split into the following types: • New • Existing – requiring re-verification • Step up Agents will need to explain the ID proofing process, the ID proofing options available to the user and why, if they are fundamentally stuck, they cannot use their ID for the use case they are trying to access.
Downgrade in assurance level resulting in an inability to access a service.	Due to expired credentials, fraud risk or simply passage of time since the user was ID proofed, the user's ID assurance may no longer be valid. Agents will need to explain to users what their options are to re-achieve their assurance level.
Expired Credentials resulting in an inability to access a service.	Some credentials, such as passports or driving licences have clear user presented expiry dates. Other credentials might be short lived, such as a Covid Test is often only regarded as valid for 72 hours. The user will need to get a new version of their credential from the credential issuer.
User cannot access RP service (and it's the IdPs fault).	This may be multiple RP Services. It may be time critical. The agent will need to explain why the service has been unavailable and when it will be restored.
Lost / Invalid Authenticator	The user will need help to recover their ID and replace their authenticators.
Updating Credentials	User wants to understand how to update their credentials.
Complexity of replacing authenticators when they are bound to an LoA.	Levels of assurance typically require authenticators of a specific type and quality to be used. When these need to be replaced, perhaps because the user has lost one, the user may need to be partially ID proofed to do so. The agent will need to explain this requirement to the user and direct them to the ID Repair process.
Unsupported ID documents.	The user is trying to use documents that are not acceptable. The agent will need to explain why and explain what alternative ID Documents are acceptable.
Unsupported devices.	The user is trying to use a device that is not acceptable. The agent will need to explain why and explain what alternative devices are acceptable.
Lost recovery codes	The user may have been issued with recovery codes for their account which they have lost, or not received. The agent will need to help the user get new codes or manually recover the users account.
Suspected Fraud	The user thinks their ID has been used by an ID Fraudster. A referral should be raised by the helpdesk to the fraud team.

2.2. ID Recovery

If the user cannot use their ID because their authenticators have expired or have been lost, they should go through an ID Recovery process.

There are two ways ID recovery is achieved:

- Self-serve – where the user is taken through an ID Recovery user journey.
- Assisted – where a help desk agent helps the user through the process, possibly resetting elements of the account for the user.

The first consideration when trying to recover an ID is – is the user the legitimate user, or is this an ID fraudster trying to take over the account.

If there is any reason to suspect the user is a fraudster a fraud referral should be raised and passed to the fraud management team to investigate.

To ensure that this is the genuine user some, or all, of the ID proofing process is usually run.

Once it has been established that the genuine user is trying to recover their account, new authenticators can be set up. The choice of authenticators might be driven by the requirements of levels of assurance the user has obtained. Higher levels of assurance demand stronger authenticators.

It could be that an ID is too damaged to recover at all as it can no longer be trusted, for example if it has been taken over by the fraudster. In the event of an account takeover items such as email account or the ability to clone a phone may still be in the domain of the fraudster. In that case, it may be necessary to close users existing account and create a new one using new parameters, such as a new contact email. However, if an ID is linked to relying party as an access method, consideration need to be given as to how that link should be re-established.

2.3. Subject Access Requests

Transparency is a key principle of Digital ID ecosystem. Users should be able to get a copy of all data held about them on request.

Parties in the ID Ecosystem who are data controllers are likely to have a statutory obligation under local data protect law to provide the user with a copy of data held about them through a Subject Access Request.

Parties who are Data Processors will need to refer users to the Data Controllers they are the processor for in the event of receiving a subject access request.

Most of the data held in a Digital ID will be already transparent to the user: the credentials, digitized and derived. The Digital ID will also include records of who the user has shared their data with – their consent history.

There may be other data collected for the purposes of fraud detection that may not be transparent to the user. Depending on the legal approach used to collect this data, for example 'legitimate interest', it may not be a requirement to provide the user with this data as part of a subject access request.

Prior to providing the user with their data because of a subject access request, the identity of the user needs to be verified. With a Digital ID, this should – of course- be able to be done digitally. So Subject Access Requests should be a self-serve option as part of a Digital IDs' account management features.

The user will be able to see from the data provided who their data has been shared with, with their consent. The Digital ID provider should enable the user to generate a Subject Access Request pro-forma so that the user can ask each relying party they have shared with data with what data that relying party holds about them.

It is important not to confuse as subject access request with a request by the user to move their data to another Digital ID provider – data portability. Data Portability is a key feature of Digital ID ecosystems and will be dealt with by a separate OIX Guide.

If the Digital ID provider is a public body, they may be subject to "freedom of information" – FOI – requests. This is where public release of information that is in the public interest is requested. Again, this is NOT a subject access request. No personal data should be released as part of a FOI request.

2.4. IdP Helpdesk for RPs

A requirement for an industry standard B2B helpdesk service should be established by the trust framework or scheme. The requirements might include values for the following:

- Agreed Hours of service
- Response and Resolution times
- Channels for engagement: Phone, Chats, Chat bots
- Languages to be supported

From a Digital ID specific point of view, the relying party operational scenarios in the following section will need to initially supported by the help desk, with rapid escalation processes to issue diagnosis teams for serious incidents.

A problem may end up being outside of the IdPs control – in an orchestrator for example – so the Help Desk may need to inform the relying party of the situation and hand off the problem to the other party.

Many identity providers will use help desks that provide multiservice support that may cover a wider range of support beyond identity. This should be taken into account when planning for the Digital ID elements of the help service.

2.5. RP Operational Issue

The relying party may experience operational issues that are affecting the normal expected operation of the service. These will be reported to the IdP RP Helpdesk.

Trust Frameworks / Schemes may require IdPs to be independently certified under ISO27001 / ISO9000 or other standards and that the recommendations and approach in this section is compatible with such certifications.

A typical support service will be multi-tiered:

Support Tier	Function
Helpdesk	First point of contact. Information gathering. Allocation and management of the problem.
First Line	Immediate issue resolution. Critical System down / inaccessible issues.
Second Line	Less critical issues. Issues that can be dealt with through configuration or data fixes.
Product	Fixes that require changes to the software itself.

From a Digital ID specific point of view, the following relying party operational issues should be planned for:

Operational Issue	Considerations
Issues with the rate of success. Rapid changes from the normal rates for ID creation and assertion.	What has caused the drop off in success rates? Is there a fault in a component of the proofing / authentication process? Are some users unable to access the service? Is It a user channel (desktop / mobile / specific device) issue? This could quickly become a critical issue.
Suspected Fraud	The RP thinks one or more IDs have been used by an ID Fraudster. A referral should be raised by the helpdesk to the fraud team.
Queries about data provided about a user: data errors, inaccuracies, evidence queries. Unable to match users.	Data may be causing RP system to fail. Or to be unable to match a user's record. Has the data changed at the IdP end since last provided to the RP? Are the any data format issues causing the problem?

Queries about credentials becoming invalid.	Users may be providing credentials to the RP that have now become invalid. This could be because a digitized credential, such as a passport, as expired. Or because a derived credential, such as “Covid Safe” or a Level of Assurance is no longer valid, or able to be refreshed.
Unknown / broken access keys when using IdP for account access.	The user is using the Digital ID to logon to an RP account. The RP cannot match the access key provided by the IdP to one it issue / agreed to accept.
Quality of service – SLA issues.	Service not available during agreed hours. Service response too slow.
Cyber-attack from IdP: man in the middle / replay.	RP is receiving requests from a rogue actor. Could be a Denial of Service attack on the RP, or a fraudulent attempt to access accounts.
IdP down / connections lost. Orchestrator down	Not service from one or more IdPs. Not service from any IdPs. Cannot connect to the orchestrator. Note: This may be an orchestrator problem. The Orchestrator may have its own help desk the RP can contact in this event.
Platform / tech problem in the RP domain.	A change has occurred at the RP that means its configuration is no longer meeting requirements to call out for or receive a Digital ID. Equally a required change to continue to be compliant has not been applied by the RP, resulting in errors or a failure.

2.6. Management Information for RPs

The following management information requirements should be considered to allow relying parties to monitor the health and success of the service. This information will often be fed into a **Relying Party Digital ID Key Performance Indicator dashboard**, where the relying party monitors the overall service received from the Digital ID service alongside internal KPIs such as onboarding success rates, ID proofing costs, fraud rates, compliance incidents.

Operational:

- UX Service Levels: planned and unplanned downtime.
- API Service Levels: planned and unplanned downtime.

Helpdesk:

- Calls by time-period
- Pick up times
- Resolution times

- Open Calls
- No resulting in complaints
- Open complaints

ID Assertions:

- Success Rates
    - New Users
    - Existing Users
    - User requiring step up
- Users requiring re ID Proofing due to expired credentials / time outs.

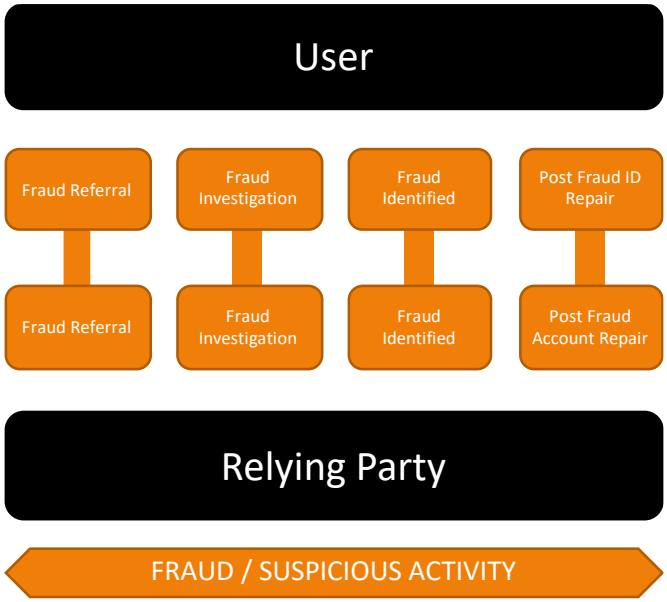
Fraud Detection:

- Number of Frauds Detected
- Fraud False positive rates

The Trust Framework could require that IdPs share fraud statistics with the framework for analysis. It could also require them to be published anomalously to allow benchmarking of IdPs.

Management information should have agreed measurement periods (e.g. daily, monthly) and agreed times for provision (e.g. daily 1 day in arrears, 5 days after month end). Essentially an SLA on the Management Information.

3. Fraud / Suspicious Activity



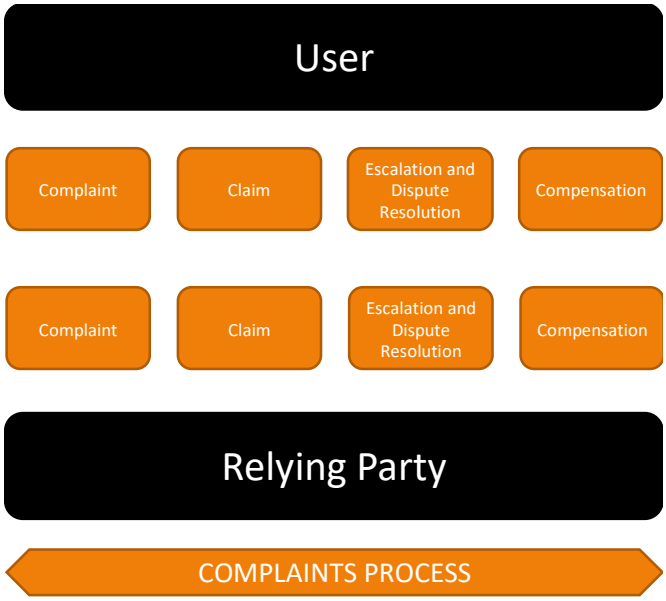
The Fraud Management process covers the following steps:

- **Fraud Referral –** a suspicion that ID fraud is occurring on a user's account. The referral could from a user, IdP help desk agent or relying party.
- **Fraud Investigation –** the process of assessing whether ID is in fact occurring.
- **Fraud Identified** – What happens when an investigation determines ID fraud has occurred.
- **Post Fraud ID / Account repair** – How is the damage the fraudster has done unravelled and the users ID re-protected.

Fraud Management is covered under section 7 of the OIX Fraud Controls Guide.

In the event of fraud occurring, some party may be held liable for losses incurred. The 5. Assessing Liability section in this document covers this scenario.

4. Complaints and Disputes



The Complaints process should support the following lifecycle for both Users and Relying Parties:

- **Complaints** – raising, management and resolution of a complaint, hopefully to a mutually agreed position.
- **Claims** – the raising of a claim for loss associated with a complaint.
- **Escalation and Arbitration** – where a complaint cannot be resolved between the complaint raiser and the party against whom the complaint was raised, third party arbitration might be required.
- **Compensation** – Payment of any agreed claim to the injured parties.

It's important to note that complaints could come simultaneously from Users and Replying Parties about the same issue, for example when an ID cannot be used or it has been stolen by a fraudster.

4.1. Complaints

Users and Relying Parties must be able to raise a formal complaint against any party in the Trust Scheme / Framework. The most likely party complaints will be raised against is an Identity Provider.

Complaints must be dealt with in a timely manner. The Trust framework / scheme should set complaint response and resection timeline obligations on parties.

4.1.1. User Complaints

The following types of user complaint should be anticipated:

User Complaint Type	Considerations
My Digital ID did not work when I needed it to	The user may not have been able to logon or access services to do a failure of their Digital ID. For example, the user was refused boarding on a plane because their COVID Safe status in their Digital ID would not show. Was this a failure on the part of the ID provider, a credential provider or was the user at fault (e.g failed to connect a test to the Digital ID).
Can't achieve a LoA / couldn't access a service they wanted to.	Users may not have sufficient ID documents / data to achieve the proofing rules required for LoA. Could Assisted Digital help? Could someone Vouch for the user? Does the user need to be passed to an IdP who specialises in the users demographic / circumstances (e.g. vouching). Is this a matter for the Trust Scheme / Framework to address as the IdP is working optimally within the rules?
Can't step up LoA.	Same as above.
Your failure meant I could not access an RP I have accessed before. (	This is often reverification problems, or lost / forgotten authenticators. Has this now been rectified? What level of inconvenience did the user experience? Did they suffer any loss as a result?
My data is wrong.	Usually goes back to the credential source, not the IdP. Can this be corrected? I Is the data is part of a Digitized Credential - where is the data coming from? How can the user correct it?
I've moved and I cannot update my address	This is often a transient problem until the users ID documents / data used for credentials catches up with the house move. How can the user help themselves through this process? What credentials do they need to update and with whom? How long will the data then take to catch up?
Suffered fraud.	Who was at fault? See Liability Consideration section of this document.
Excluded.	Lack of ID documents or data to meet IdP offered proofing techniques. Could Assisted Digital help? Could someone Vouch for the user? Does the user need to be passed to an IdP who specialises in the users demographic / circumstances (e.g. vouching). Is this a matter for the Trust Scheme / Framework to address as the IdP is working optimally within the rules?
My IdP is not on an RPs acceptable list of IdPs.	Explain the commercial situation that leads to this situation. The user will need to choose and ID provider the RP accepts.

Unable to move my ID from you to another IdP.	Investigate why? Are credentials transferable? Does the new IdP accept the same credentials?

4.1.1. Relying Party Complaints

The following types of relying party complaint should be anticipated:

RP Complaint Type	Considerations
Any user driven complaint	The RP may report many of the same complaints as users when an incident has occurred that regard a specific user, per the list in the section above.
Multiple Fraudulent IDs	The RP may detect that many IDs have been used to access their services fraudulently. Who was at fault? See Liability Consideration section of this document.
IdP not available / unplanned downtime.	An IdP, or IdPs were not available causing users to be unable to access the RP for a specific amount of time.
IdP API errors	An RP received API errors which meant some users were unable to access the RP for a specific amount of time.

4.2. Claims

A claim is where a user on a relying party is attributing a loss and / or compensatory value to an issue.

The first thing to establish is whether any party is at fault. Several different parties need to be considered. Whilst the ID Provider is the party that often sits at the centre of the relationship between the relying party and the user, other parties such as orchestration providers or credential issuers might be the party at fault.

The second thing to establish is whether the claim is tangible and measurable. Has the user or relying party suffered direct or indirect financial loss? Have they spent considerable time dealing with the matter? Have they suffered any distress as a result?

The type of loss will vary depending on the scheme, for example:

- I could not buy an age-related product
- I could not get a mortgage

In these examples, the user will not have suffered any direct financial loss, but may have been unable to enjoy access to services due to a failure on the part of the digital ID provider.

However, the relying party will have lost potential revenue, and so may have a claim for financial loss.

For other examples, the user may suffer more direct financial loss.

- I could not show my COVID Safe status and was refused entry to a venue, or could not travel. I missed my gig, or for travel, I had to wait and buy another ticket.
- My ID was taken over by a fraudster who opened a credit card in my name and ran up a £3,000 debt.

In the case of fraud, it needs to be determined who, if anyone, is at fault. This is covered in the section on Liability Assessment.

4.3. Escalation and Dispute Resolution

Complaints should ideally be dealt with by the parties directly involved, typically the user or relying party and the ID provider.

If this is not possible and a mutually agreed resolution is not achieved, there must be an escalation route.

OIX has liaised with https://www.ombudsman-services.org/ to explore escalation approaches.

Ombudsman Services recommends a "confidence approach" that gives systemic support to users and ensures that each escalation is a learning experience for the trust framework / scheme. OIX concurs with this confidence approach.

The next consideration highlighted by ombudsman-services is the type(s) of dispute resolution to be offered:

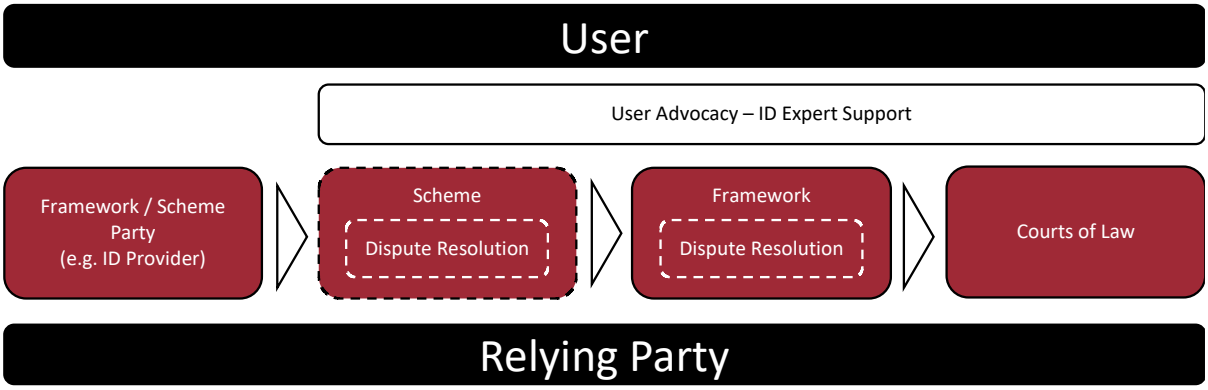
Type of Dispute Resolution	Description	Key points
Arbitration	Private Court	Formal and legalistic Final decision Both parties pay
Mediation	Facilitated Resolution	Strong on relationships Relies on good faith Doesn't always lead to resolution Process is confidential
Adjudication	Assess strength of different cases	Different shades Compliance with law and codes Often adversarial process
Ombudsman	Usually form of adjudication but may mix with elements of mediation.	Access and informality Inquisitorial Fair and reasonable test Remedy not compensation

Having an independent representative who understands Digital ID from all perspectives: users, RPs, IdPs in order to properly understand viewpoints, capabilities and constraints is vital. In this respect, the Trust Framework / Scheme is well placed to help with escalated matters. OIX encourages Trust Framework / Schemes to do this.

It is also however important that there is a route to independent representatives. A balanced approach offered by an ombudsman should be considered.

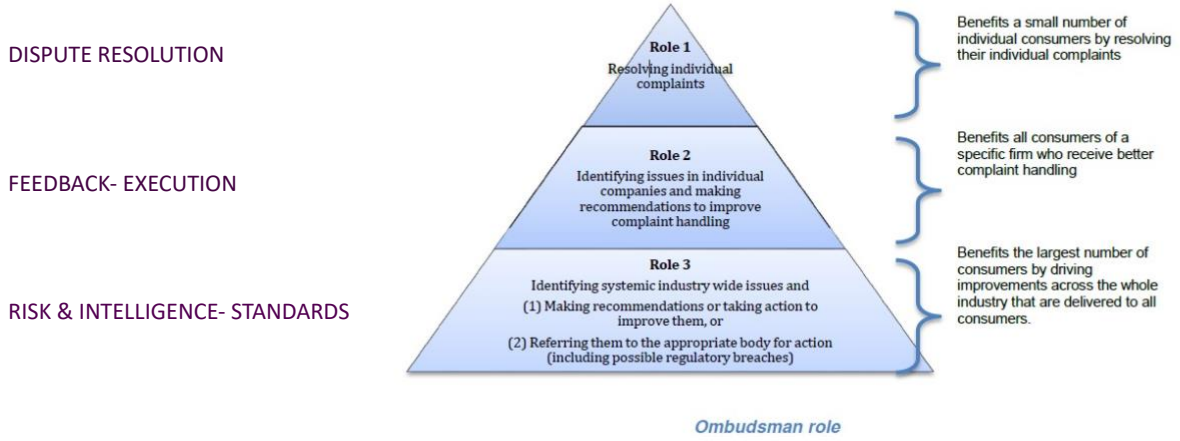
Ultimately a trust framework is a legal construct. Referral to a court of law is the final step if agreement cannot be reached. However, the way an ombudsman scheme usually works is that the provider / supplier agrees via a deed poll that the decision the ombudsman reaches will be legally binding on them. The ombudsman decision can be rejected by the end user/ consumer who can still go to a court in theory. In practice what happens in ombudsman schemes is you almost never see it reaching a court because the ombudsman decision has given an end user (and potentially a court which did get involved) a very strong signal about whether their case has merit or not. That's one of the key benefits of an ombudsman approach versus the courts - it's quicker, cheaper and doesn't need legal expertise to raise or to contest a complaint.

The following diagram shows how escalations might work:



To support users, expert advocacy may be necessary. Users will be trying to uphold a complaint against expert ID services providers and so cannot be expected to do this without the correct support.

It is vital that feedback is captured as part of the dispute resolution process and that it is used to improve the framework or scheme going forward. The following diagram from ombudsman-services shows how this process should result in updates to the rules and standards in the framework, or indeed in legislation, to improve matters for users and relying parties.



4.4. Compensation

If a claim is upheld, compensation needs to be agreed. Compensation for users and relying parties could take the following forms:

- Compensation for Provable Financial loss

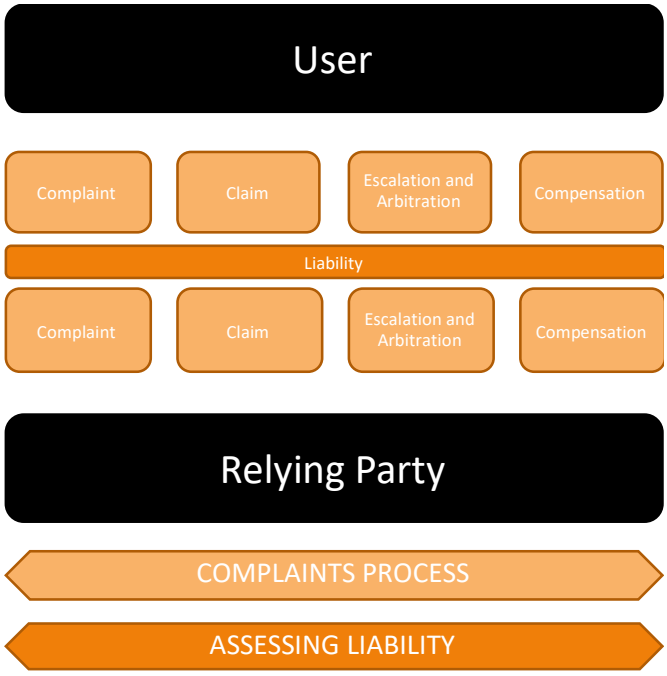
- Compensation for time spent because of the issue
- Compensation for distress (most likely an end user compensation feature).
- Compensation for costs

Trust Frameworks / Schemes should consider whether Insurance / Compensation Mechanisms are required to ensure compensation can be claimed.

These mechanisms may be a Scheme, or event Identity Provider, commercial feature. For example an IdP may make part of its service a guaranteed payment in the event of an upheld claim. A Scheme could make this a feature of being part of the Scheme, analogous to the ATOL scheme used in the travel industry.

Such compensation mechanism might even include compensation to relying parties, or even the user, in the event of fraud losses. (Although in the Assessing Liability section below we suggest a particular treatment for fraud losses).

5. Assessing Liability



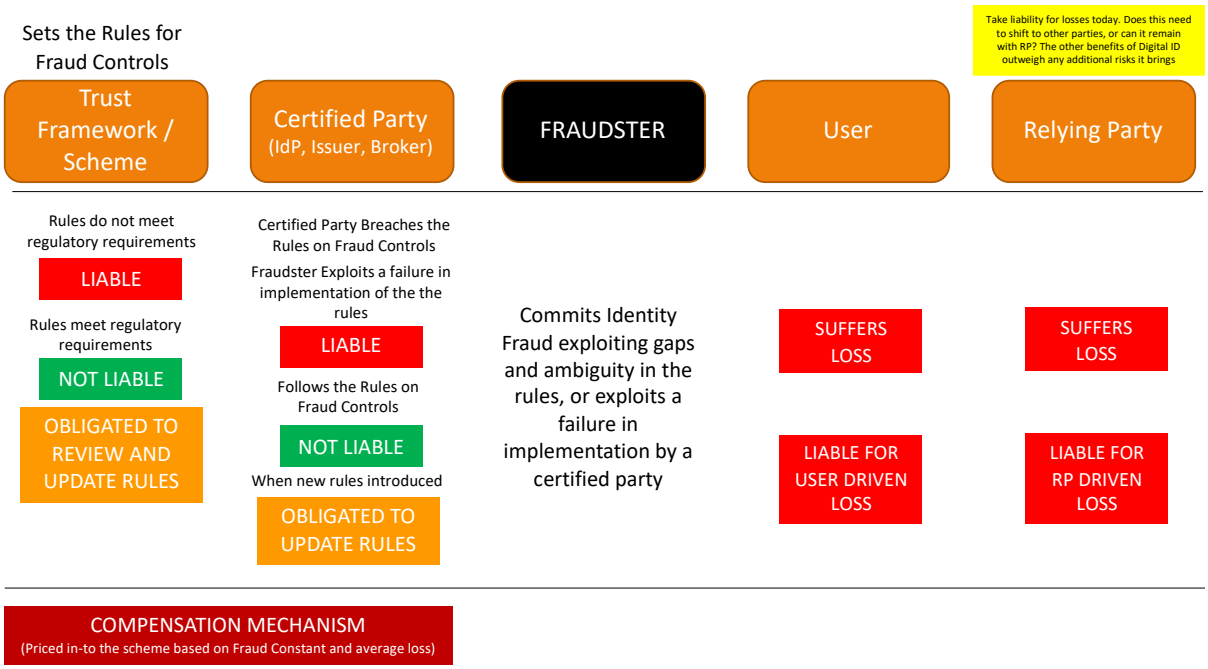
Assessing liability is a parallel process to the complaints process. At each stage there will be an exploration of which parties may be at fault.

Most Trust Frameworks will operate fault-based liability approaches. Only when a party has been proven to be at fault can they be held liable. As a trust framework is a set of rules, if the party has followed the rules, they are unlikely to be judged to be at fault. It is then a valid question to ask – are the rules correct? There may be obligations on the framework to update rules that are proven to be incorrect, but can the framework itself be held liable for ill-conceived rules?

When a party is proven to have breached the rules, then they are likely to be held and fault and may then be held liable for any loss incurred by other parties in the framework as a result. The amount and nature of the compensation will be use case and scheme specific and is often a commercial feature of Digital ID service.

It may be agreed that fault, and thus liability, across more than one party in the ecosystem, in which case several parties might share costs.

Identity Fraud is a specific topic where liability assessment needs careful consideration. When identity fraud occurs who, if anyone, is at fault? If the framework has defined the best rules possible to mitigate against fraud, and the fraudster innovatively beats these rules, can anyone be held at fault? The diagram below considers who might be held liable in the event of identity fraud occurring:



The Trust framework / scheme would set rules for fraud contols and manangement that certified parties (IdPs, Issuers, Brokers) need to follow. The trust framrwork / scheme should be setting rules that meet – as far as is possible – any regualtory requirements for fruad management for the use cases involved. If the trust framework / scheme fails to do this properly, they could be held liaible for any fraud loss incurred by users or relying parties.

However, assuming the rules set meet the regulatory requirement, the trust framework / scheme would not be held liaible for frauds that manage to circumvent the rules set. It would be ttypical for there the be an obligation on the operator of the framework / scheme to review the rules if frausters are getting through, and update the rules – if possible - to prevent new fraud techniques as they emerge.

Cetified parties must follow the fraud controls and managememt rules set by the framework / scheme. If they do so they would not be held liaible for frauds that manage to circumvent the rules. Thre must be an obligation on the to update control to reflect new rules as they are implemented by the framework /scheme to prevent new fraud techniques as they emerge. Typically a tight deadline for cimplinace with new rules is implemented so they holes in the system that are found byt a fraudster are plugged as rapidly as possible.

If a user suffers loss and they are a fault, for example they have given away their password, they they would be liaible for that loss. If the user is not at fault, and no certified party or the framework / scheme is at fault, no party is liaible for the users loss. However in practise the scheme might cover this through compensatorty mechanisms or by demanding certified parties carry certain insurances.

If the relying party suffers loss and they are at fault, for example they had a data breach or staff compromise, they would be liable for that loss and any loss incurred by users as a result. If the relying party is not at fault, and no certified party or the framework / scheme is at fault, no party is liaible for the repying parties loss. However in practise the scheme

might cover this through compensatorty mechanisms or by demanding certified parties carry certain insurances.

Insurances

- Assuming a no-fault position on Identity Fraud an assessment would need to be made on whether Professional Indemnity, Cyber Risk and other standard insurances are sufficient

A more detailed exploration of liability issues can be found the OIX paper: How to Approach Liability