

# Minutes of meeting

## Discovery Session 2

Date: 07.08.2024 | Virtual meeting

### Agenda

1. **Introductions**
2. **Recap of Discovery Session 1**
  - Key updates
3. **Deep Dive on Corporate ID**
4. **Open Discussion**
5. **Next Steps/ AOB**
  - a. Recap of key actions to take.
  - b. AOB

Minutes	
<b>Item 1 – Introductions &amp; guiding principles on competition</b>	
<b>Purpose:</b> For information	
Speaker: HS	<ul style="list-style-type: none"><li>• <b>Leon Ifayemi (LI)</b> Reminder of the anti-competition principles all CFIT Coalition meetings are governed by.</li><li>• Welcomed everyone, thanked everyone for the support offered so far.</li><li>• <b>LI</b> confirmed the agenda</li></ul>
Comments:	None
Decision:	N/A – for information only

Actions:	None
<b>Item 2: Discovery Session 1 Recap</b> <b>Purpose:</b> For information	
Speaker: TL	<p><b>Teresa Lam (TL)</b> ran through the key takeaways from the first discovery session:</p> <ul style="list-style-type: none"><li>• In the recent sprint discussion, participants explored the concept of a Corporate ID, which is envisioned as a secure, reusable digital profile for businesses. This ID would consolidate essential entity details from reliable data sources and be adaptable based on different use cases. The goal is to improve user experience, reduce manual processes, and enhance trust and transparency in the ecosystem by preventing bad actors from entering the system.</li><li>• The focus was on how Corporate ID could specifically aid in fraud prevention and economic growth, with an emphasis on addressing types of fraud such as identity fraud, fraudulent account openings, and APP scams. While other use cases are possible, starting with a targeted approach to these issues is seen as the most practical way forward.</li></ul> <p><b><u>2 scenarios:</u></b></p> <p><b>1. KYB</b></p> <ul style="list-style-type: none"><li>• The use of Corporate ID in onboarding simplifies and enhances the customer journey. When a business approaches a bank for a new account, the bank can use the baseline information from the Corporate ID to conduct initial screenings. This approach can determine if additional information or enhanced due diligence is required, saving time and costs, enabling automation, and ensuring more accurate risk assessments.</li></ul>

## 2. Payment Verification

- The second scenario involves using Corporate ID to validate the identity of payees, helping prevent fraud in transactions, such as when a business pays a new supplier or changes account details. Key considerations, including data sharing, consent, and data protection, still need to be addressed. Feedback is requested on the two scenarios and the potential inclusion of a third scenario for periodic review and KYB re-verification using Corporate ID.

TL ran through the theory of Using Corp ID to facilitate KYB/risk decisioning:

- Level 1: Does this entity exist? Who has control over this entity?
- Level 2: Who are the parties connected to this entity?
- Level 3: What is the risk associated with this entity?

### Brief Discussion

#### Questions presented:

1. What are your views on the above scenarios?
  2. Should there be a third scenario with the use of Corporate ID for periodic reviews and KYB re-verification?
- **Louise Beaumont (LB)** Asked for the slides to be circulated before the call.
  - **Mark Devil (MD)** Raised an important question about the responsibility for maintaining and updating Corporate ID records. Specifically, if a client presents a Corporate ID during a new application, who ensures that the ID remains current for ongoing KYC processes? Is it the responsibility of the institution receiving the ID, or the entity maintaining the record? The idea is that if the record is

consistently updated, the need for scenario three may diminish over time.

- **TL (in response to MD)** highlighted the need to consider how to keep Corporate ID records consistently up to date. She mentioned two possible approaches: pulling data directly from the source when needed, without storing it in the Corporate ID, or implementing ongoing maintenance of the data. These options will be explored further in a future proof of concept.
- **Anthony (Tunic Pay)** raised a question about scenario two, asking if the process involves providing the Corporate ID to the financial institution or payment service provider at the time of payment. The idea is that the provider would then conduct the necessary checks in the background. The inquiry seeks to clarify if this is the intended business flow.
- **TL (in response)** mentioned that they are exploring the best data-sharing methods in the UK, considering existing infrastructures like open banking. The focus is on avoiding unnecessary reinvention and ensuring proper data flow, consent, and control. The optimal approach is still being discussed by the coalition.
- **Nick Mothershaw (NM):** Reverification is essential and required by regulations, posing a growing challenge for financial services to keep records updated. The difficulty lies in determining how often information needs refreshing, as some details that seem static may change, like a company's trading status. Each piece of evidence used in maintaining a Corporate ID must have clear rules for when and how it should be refreshed to ensure the information remains current and accurate.

Comments	<ul style="list-style-type: none"> <li>• <b>Nina Kerkez (NK)</b> this payment flow (scenario 2) is well managed today already, and I am unsure what we would be adding here with corporate ID at this stage. If the corporate ID is managed somewhere centrally which would be regulated, then it might make it easier in the payment processes, but today we don't have such system or regulation.</li> <li>• <b>Rob Haslingden (RH)</b> Responding to <b>NK</b> Having a central repository of IDs is risky...and is a potential 'honeypot' for hackers' so I would steer away from this.</li> </ul>
Decision:	<ul style="list-style-type: none"> <li>• N/A</li> </ul>
Actions:	<ul style="list-style-type: none"> <li>• none</li> </ul>

### Item 3: Deep Dive on Corporate ID

**Purpose:** For discussion

Speaker: LI	<p>LI introduced a Corporate ID stack,  This slide presents initial ideas and a visual representation of a Corporate ID concept, developed from recent feedback and discussions. The Corporate ID structure includes:</p> <ul style="list-style-type: none"> <li>• <b>Level 1 datasets:</b> Confirm business existence and essential details, including key individuals with significant control.</li> <li>• <b>Level 2 datasets:</b> Provide deeper insights into business behaviour, associations, and risks, such as links to multiple companies or frequent use of fraudulent addresses.</li> </ul> <p>The concept will be refined with further input, aiming to create a practical Corporate ID definition for the UK. Thanks to the banks volunteering for the</p>
-------------	--

proof-of-concept phase; their participation will be crucial for testing and validating this approach. More details will be shared soon.

**LI** Ran through level 1a and 1b datasets:

- 1a: Unique identifiers, legal business identifiers, who we have a few companies in this are on the call today.
- 1b: Business attributes, including but not limited to registered business name, incorporation, income, tax, etc. Emphasis on a mixture of public and private information.
- 1c: Focuses on individuals with significant influence over the business, such as those authorized to instruct financial service providers. Key stakeholders include:

1. Shareholders owning 25% or more of shares or voting rights

2. Company directors or partners

3. Secretaries and account operators who are authorized signatories

- Two approaches for integrating individual data into Corporate ID are:
- Partnering with established individual ID providers like YOTI and ONE ID, which could streamline the process and enhance user experience.
- Directly accessing primary data sources for corporate ID requirements.

In the future, individual ID providers may expand to include corporate IDs and vice versa.

**LI** introduced Level 2 – Multi-sourced Data Corroboration (network effects)

- This will help provide further context on the risk profile of the business.
- Combining these tools to support specific use cases is necessary.
- Valuable data sets for risk ratings include:

	<ul style="list-style-type: none"> <li>○ Registers for licensed activities and industry certifications</li> <li>○ Open Finance data for a holistic business picture</li> <li>○ E-commerce and social media data for online presence and trading history</li> <li>○ Industry benchmarks to identify abnormal financial patterns</li> <li>• This list is not exhaustive. A survey will be sent for additional input on data sets and sources, which everyone will have the chance to add to the list. The goal is to create a comprehensive data repository for improved fraud prevention.</li> <li>• LI Ran through an illustrative slide of level 2 and a potential flow of how the corporate ID stack and multi-sourced data corroboration could be used in an onboarding process.</li> </ul>
Comments:	<ul style="list-style-type: none"> <li>• <b>Ross Aubrey (RA)</b> Asked how the Corporate ID differs from a Duns ID for example?</li> <li>• <b>Sandra Peaston (SP)</b> <a href="https://www.ico.org.uk/home-office-uk-finance-financial-institutions-regulatory-sandbox-final-report-v1-0.pdf">home-office-uk-finance-financial-institutions-regulatory-sandbox-final-report-v1-0.pdf (ico.org.uk)</a></li> </ul>
Decision:	<ul style="list-style-type: none"> <li>• N/A</li> </ul>
Actions:	<ul style="list-style-type: none"> <li>• None</li> </ul>
<p><b>Item 4: Open Discussion</b></p> <p><b>Purpose:</b> For discussion</p>	
Speaker:	<ul style="list-style-type: none"> <li>• <b>Houssein El Sayed (HS)</b> Chaired the open discussion.</li> </ul> <p><b>Discussion 1: What are your views on our presented model?</b></p>

- **Tina Blocksbridge (TB):** Looking at reliance of previous banking solution: How do you mitigate the movement of bad actors, perhaps a network analysis
- **Darren Morford (DM):** A corporate ID is only as good as the data you've got, data needs to be checked in real time, not 2 days later, there needs to be a validation in real time. On the POC: it's crucial to decide whether there's consent involved or not. **DM** believes it's not a consented environment.
- **Glen Keller (GK):** Concerned risks with Identity, blurry line with credit scoring, risk and decisioning, need to be careful where we draw our boundaries.
- **Mark Devlin (MD):** emphasised positive remarks regarding the layout of the corporate ID, achieving level 1 would be a step forward and a POC on its own.
- **Emily Hyett (EH):** how do we identify individuals, linking a name from the source. How do we make sure the ID is accurate?
- **Nick Pyrke (NP):** Excellent points! Level 2 clear distinction between publicly available info and private info. Need to strike a balance between privacy, consumer data and usage of data. Social media content- cautious on this to influence business decisions.
- **Sara De La Torro (ST):** Emphasised the importance of understanding the broader purpose and value of a digital verification ID in the UK, especially for small and medium-sized enterprises (SMEs) and sole traders. They highlight the need for proactive and ongoing creation of corporate IDs to protect these entities from fraud and support their growth. The speaker also stresses that while established corporations may already benefit from such systems, it's crucial to include less established organizations in this protection and to offer them the choice to opt-in. They recommend that this process be consent-



based and inclusive, ensuring the entire market, not just a subset, is effectively covered.

- **Clare Roughley (CR):** Outlined three key principles that they believe will shape the future of Know Your Customer (KYC) processes:
  1. KYC will be decentralized.
  2. It will require permission from the entity undergoing KYC.
  3. It will rely on digital credentials issued by third parties.
- **CR** suggested that when considering different technological stacks for KYC, it's important to differentiate between types of information that can be accessed via credentials with the entity's permission and information that requires data aggregation, such as detecting anomalies across transactions or verifying corporate structures through audits.

## **Discussion 2: Which other datasets would be useful within a Corporate ID?**

- **LB:** Is there anybody from Companies House or HMRC on this coalition?
- **LI:** Companies House are in conversation- chief data officer looking to attend a future sprint. HMRC will be engaged.
- **Robyn Easton (REF):** Going back to the money laundering regulations and using them as a baseline and then mapping the data points to those requirements, whether it's identification or identification and verification of certain data points and you've got quite a lot of these here.
- **NM:** highlighted two types of identity in the context of companies:

1. **Responsible Individuals:** These are directors or partners whose identities can be verified separately from the company and are a matter of public record. Verification involves confirming who they are and understanding their other interests.
  2. **Account Operators:** These are individuals authorized to act on behalf of the company, such as signatories, but their identities are not public records. Their roles are based on company trust and policy, not public documentation.
- **NM** mentioned an upcoming project by the Open Identity Exchange to explore the distinction between core individual identities and those with delegated authority within organizations, emphasizing its importance.
  - **Michelle Bradford (MB):** as a bank, there was an onus on them to report any discrepancy reporting that we identify through you know the information that customers give us a corporate customers give us and then obviously what we see against Companies House and HMRC. Would this mean bank's obligations have been met? Who is the onus on to report discrepancies that are found?
  - **LI:** addressed two key issues regarding data verification for SME customers:
    1. **Operational Efficiency:** It would be inefficient to duplicate verification efforts if data provided by SME customers is already sourced with their consent. If the data comes directly from a reliable source, re-verifying it against another dataset would be unnecessary.
    2. **Liability:** The responsibility for ensuring the accuracy of sourced data depends on the method of acquisition. If data is obtained

through an aggregator, the aggregator might bear the liability. However, if a bank or financial service provider sources data directly from entities like Companies House, the data's gatekeeper may hold the responsibility.

- **LI** noted that while liability is a crucial issue, it won't be fully addressed in the current coalition's timeframe. Instead, it will likely be the focus of a follow-up project after initial technical work is completed.
  
- **Mark Devlin (MD)** suggested two key points:
  1. **Data Verification:** There's an opportunity to create a reliable "golden source" of data by verifying it against another trusted source, enhancing its reliability.
  2. **Identifying Hidden Bad Actors:** Many bad actors hide behind legitimate businesses, often operating as account operators in the background. Since banks have databases of all users associated with accounts, a standardized way to share this information—while respecting consent—could help identify who controls the funds in these accounts, even if these individuals don't appear in public registries. This idea is worth exploring further.
  
- **HS** (in response) acknowledged a recurring theme of data sharing and the need to consider non-public data in verification processes. They outline three key questions for discussion:
  - **Leveraging Existing Digital ID Solutions:** How can current digital ID solutions be used to validate individuals behind a business or entity?
  - **Integration with Corporate ID:** How should individual ID verification be linked to corporate ID definitions? Should it be a simple checklist or involve a more complex integration?

- **Documenting Authority:** How can we ensure that the authority of individuals within a corporate ID is accurately documented and kept up to date?
- **HS** invited feedback and comments on these points, starting with how existing digital ID solutions can be utilized.

### **Discussion 3: Verification of individuals in a Corporate ID**

- **Glen Keller (GK):** Relevance of recent Companies House reforms aimed at improving identity checks for directors. They suggest that if a director's identity has already been verified during the company's registration process and is trusted, it might be unnecessary to repeat the verification process later. While this doesn't address verifying the authority of individuals within the company, the speaker raises the point that redundant identity checks should be avoided if the initial verification is reliable.
- **LI** Thanked **GK** for his comment, and mentioned that Companies House will hopefully attend some of the future sprints.
- **Paul Baker (PB):** First step in identity verification is proving one's identity and sharing key data. They reference ongoing UK initiatives under the Digital Identity and Attributes Trust Framework that can confirm basic details like name, date of birth, and nationality, though not necessarily a person's role within a company.
- **NM:** The challenge of using digital identities for corporate representation, as digital identities are individual. They suggest the coalition should explore how to manage consent from directors to include their information in a corporate identity package. This could involve long-term consent similar to open banking, allowing a company to present its directors' identities without repeatedly

	<p>seeking approval. Alternatively, each director might need to reconfirm their identity separately when the business presents its identity. The coalition should consider various options for integrating digital identities into the corporate system.</p> <ul style="list-style-type: none"><li>• <b>CR:</b> While digital certificates, such as legal representative certificates, are not widely used due to reliance on centralized authorities, there is potential in exploring organizational wallets. These could support decentralized identities and offer a forward-looking solution for managing credentials within companies.</li></ul>
Comments (on chat):	<ul style="list-style-type: none"><li>• <b>RH</b> Other issue association with ongoing checks and maintenance is 'who carries the liability on the veracity of the Corporate ID?'</li><li>• <b>Maggie Chen (MC)</b> Do we have something that look into the historical fraudulent cases and understand how the corp ID was used or misused. Was there any commonality?</li><li>• <b>Sara de la Torro (ST)</b> How do we proactively (with consent) create and apply IDs for the smaller SMEs/ sole traders who do not necessarily have a corporate IDs and who need to be equally protected and supported accordingly?</li><li>• <b>Adrian Field (AF)</b> Have we defined the problem(s) &amp; outcomes this coalition is looking to address? We seem to be in solutioning mode.</li><li>• <b>Matthew Carter (MC)</b> Live/real time data is very important, and 'consented' data is also a very strong signal, but this will need to be integrated and/or sit alongside the more traditional database/stored data. No silver bullet exists so we need to be able to pool as much as we can so users of the data can work out what sits within their risk appetite and what doesn't - this would cover everything from SME's and sole traders to multinationals.</li></ul>

	<ul style="list-style-type: none"><li>• <b>Ethan Salathiel (ES)</b> In terms of gaps here in the level 1 ownership &amp; control part, is when you've got companies which are in part of wholly owned or controlled by overseas entities (very common). When I was a commercial RM, time and time again suspicious activity detected in the UK was linked to activity in higher risk jurisdictions and tax havens where information is very challenging to obtain to validate corporate ID. We need to think how we tackle the opaque nature of this.</li><li>• <b>Robyn Easton-Fei (REF)</b> In some ways the metadata around any Corp ID data is the most important - e.g. timestamps/sources/permissions/audit trails, to demonstrate data control</li><li>• <b>Darran Morford (DM)</b> Defining your response rules and outcomes will help you define what you need to collect. Response being not too complicated and easy to understand and actions based on the responses. Seems there is a lot being talked about but what would be the response for example is user case 1 and 2 earlier.</li><li>• <b>CR</b> Nick raises a good point. official organisational roles which are recognised by jurisdictional law can be validated by third party sources whereas delegated authorities are internal company record. Both can be discovered via the vLEI.</li><li>• <b>RH</b> Have we clarified if this is going to be a 'Consented Data' journey or not?</li><li>• <b>EH</b> I think the GDS OneLogin programme - reusable ID- is currently only being rolled out with Gov Departments rather than with commercial third parties.</li></ul>
Decision:	<ul style="list-style-type: none"><li>• <b>N/A</b></li></ul>

Actions	<ul style="list-style-type: none"> <li>N/A</li> </ul>
<b>Item 4: Closing Remarks</b>	
Speaker: LI	<ul style="list-style-type: none"> <li>Later this week, you will receive a survey related to our recent discussion. Please complete and submit it by <b>August 23<sup>rd</sup></b>.</li> <li>The survey consists of four sections: Background, Use Cases and Enablers, Data Set Prioritization, and Other Supporting Points. It will be distributed to all partners and supporters. Your input is crucial for developing a consensus on the scientific definition of digital verification in the UK.</li> <li>LI thanked those partners who have returned their signed TORs and everyone for attending the meeting. Reminded partners that the next discovery session is the following Friday (<b>16<sup>th</sup> August</b>).</li> </ul>
Comments (on chat)	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Decisions	<ul style="list-style-type: none"> <li>N/A</li> </ul>
Actions	<ul style="list-style-type: none"> <li>Survey Distribution to partners this Friday.</li> </ul>

## Attendees:

**Chair/s:** Leon Ifayemi (LI), Houssein El Sayed (HS)

Organisation
CFIT

<b>City of London Corporation</b>
<b>Yoti</b>
<b>OneID</b>
<b>FDATA</b>
<b>UK Finance</b>
<b>Lloyds Banking Group</b>
<b>CIFAS</b>
<b>KPMG</b>
<b>Cardiff University</b>
<b>Tisa</b>
<b>City of London Police</b>
<b>OBconnect</b>
<b>KPMG</b>
<b>GLEIF</b>
<b>Paragon Bank</b>
<b>Lexis Nexis Risk Solutions</b>
<b>Experian</b>
<b>EY</b>
<b>Natwest</b>



<b>OBconnect</b>
<b>CRIF</b>
<b>Nationwide</b>
<b>Experian</b>
<b>Lloyds Banking Group</b>
<b>Mastercard</b>
<b>Tunic Pay</b>
<b>City of London Police</b>
<b>Dun &amp; Bradstreet</b>
<b>Technoxander</b>
<b>Smarter Contracts</b>
<b>EY</b>
<b>Cardiff University</b>
<b>Experian</b>
<b>CTRL SHFT</b>
<b>Visa</b>
<b>OIX</b>
<b>Quantexa</b>

