Minutes of meeting

Sprint 5

Date: 18.09.24 | Virtual meeting

Agenda

1. **Introductions**
2. **The 'What'**
    - Updated Corporate ID Stack with Datasets
3. **POC Questionnaire**
    - Key Results
    - Impact Measures
4. **Open Discussions**
    - Additional Impact Measures
    - For a Corporate ID, how should consent be managed?
    - Who should obtain the consent?
    - Should there be perpetual consent for the agreed purpose?
5. **Next Steps**
    - AOB

Minutes	
Item 1 – Introductions & guiding principles on competition **Purpose:** For information	
Speaker: LI	• **Leon Ifayemi (LI)** Welcomed all partner attending the meeting. **Discovery Phase – Playback of Key Themes and Activities**

	• **LI** Ran through the previous 4 sprint outcomes: The coalition has assessed the wider landscape, prioritised datasets in the corporate ID definition via our survey and refined the scope of our proof of concepts. • Reminder of the anti-competition principles all CFIT Coalition meetings are governed by. • **LI** confirmed the agenda.
Comments:	None
Decision:	N/A – for information only
Actions:	None

Item 2: Updated Corporate ID Stack

Purpose: For discussion/information

Speaker: LI	**Corporate ID Stack Overview:** • **LI** Ran through the updated corporate ID stack that now incorporates ranked datasets from the Discovery Phase survey. • Special acknowledgment to Charlie Boundy (Companies House) for valuable input on bucket structure. **Key Elements of the Corporate ID Stack:** i. **Global Business Identity Credential:** A unique global identifier for businesses, e.g., DUN's number or LEI, explored through multiple data sources. ii. **Local Registration:** Information from Companies House, including company directors, SIC codes, and other key details. iii. **Licensing:** Relevant for companies in regulated industries, leveraging appropriate regulators (e.g., FCA for financial services).

	iv. **Operational and Trading Status:** Data from HMRC, credit agencies, and open banking for evaluating revenue and transaction behaviour. v. **Personal ID and Verification (ID&V):** Focus on individual influencers and their authority, supported by various ID providers. vi. **Risk Parameters:** Common risk parameters for banks, with room for customisation based on individual risk appetites. • This iteration reflects contributions from various partners during the last Sprint, aiming to standardise the corporate ID framework. • Appreciation extended to all partners for their collaborative efforts in refining the corporate ID stack.
Comments	• none
Decision:	• N/A
Actions:	• none

Item 3: POC Questionnaire

Purpose: For discussion

Speaker: LI, AF,	• **LI** extended appreciation extended to POC partners (NatWest, Lloyds, Monzo) for completing the questionnaire, providing insights into current operations and future KYB and onboarding benchmarks. **<u>Key Results</u>** • **Uniform Data Requirements**: Banks surveyed shared similar data needs, suggesting a corporate ID could function across multiple departments under one policy.

	• **Aggregator vs. Wallet Preference**: General preference for using data aggregators or wallets, though a hybrid model combining both is also considered. • **Data Sharing & Consent:** Consensus on embedding long-term data-sharing guidelines within T&Cs, but consent limited to onboarding and fraud risk assessments. Separate consents needed for other services like loans. • **Corporate ID Limitations**: Corporate ID won't address all data challenges; qualitative information must still be manually updated. • **Automation Potential:** Up to 90% of the data collection process could be automated, reducing manual input and certified document requirements. • Prototype UX flows and designs based on feedback will be shared in upcoming sprints. • Further discussions on aggregator vs. wallet models to take place in future sprints. • **LI** Opened the floor for discussion. • **Adrian field (AF)** emphasised that while corporate ID handles company data, it's ultimately a human (e.g., a director) who applies for a loan or bank account. He proposed incorporating role-based IDs where, for example, a director's ID token can prove their authority, rather than relying solely on corporate ID. • **AF** suggested that individuals could present corporate data via a wallet app, reflecting that it's the person, not the company, engaging with financial institutions. • **LI** acknowledged the alignment in their thinking, noting that wallets can grant signatory rights at the point of onboarding or execution.

	• **LI** stressed the importance of consistency across wallet and aggregator providers, pointing to a need for standardisation in the hybrid model. He invited **AF** to preliminary workshops to capture his thoughts ahead of the wider group discussions. • **Adam Prince (AP)** Highlighted the ongoing issue of keeping business data (e.g., SIC codes) updated, particularly for small businesses. Stale data often requires reverification or validation, no clear solution was proposed. This issue was particularly tied to Companies House data. • **LI** suggested a potential solution where underlying data sources revalidate the data periodically, either annually or biennially. This idea will be further discussed and shared with partners. • **LI** acknowledged the specific issue with Companies House data, confirming it's a critical area to address in future discussions. • **Jon Roughley (JR)** inquired if similar research had been conducted from the business perspective, especially regarding data acceptability and what drives adoption. • **LI** confirmed such research has been done and mentioned that impact numbers would be shared later in the session, with data gathered from a panel via the Federation of Small Businesses and Sage. • **Lewis Utley (LU)** agreed with Adam's concerns, stressing that annual updates are insufficient. Data needs to be much more current, especially when companies are facing issues, to ensure accurate and timely verification.

	POC Persona • **LI** Focus on Small Businesses: The POC will focus on smaller limited businesses in business banking, specifically micro-businesses (5-10 staff, turnover < £2M) and small businesses (fewer than 50 staff, turnover < £10M). Sole traders and large corporates are currently out of scope, as agreed by POC partners. • The findings align with the results of the Discovery Survey, available in the annex of the presentation. **SME User Feedback** • **LI** working with the Federation of Small Businesses (FSB) and Sage, the POC will gather feedback from about 50 small and micro businesses through an onboarding flow demo, presentations, and focus group questionnaires. This ensures the work reflects real business needs, not assumptions. Results will be shared by late October or early November. **Suggested Impact Measures** • **For Financial Service Providers**: Metrics include reductions in onboarding bad actors, improved detection rates, time and cost savings in verification, and reduced drop-off rates during onboarding. • **For Businesses**: Key metrics focus on improving KYC user journeys, operational efficiency, fraud reduction, and lower administrative burdens, while assessing readiness and willingness to adopt and pay for corporate ID solutions. • **JR** inquired if the POC partners believed the solution would improve access to business finance for firms using it, and whether this could be a compelling factor for SMEs to adopt the solution.

	• **LI** confirmed that 100% of feedback suggested the corporate ID could be valuable beyond just onboarding and KYB (Know Your Business) processes. It could be extended to lending and other financial products, but this would require different terms and consents. • The current POC is focused only on onboarding and KYB, but there was an acknowledgment of its potential for broader use cases in the future. • **JR** commented that it seemed the corporate ID's value proposition currently benefits lenders more than SMEs. • **LI** explained that this observation remains to be validated through ongoing research, including surveys and focus groups. Ethical considerations regarding SME data collection will also be addressed in future sprints. • **Mark Devlin (MD)** suggested that one of the potential benefits for SMEs could be the ability to move seamlessly between financial institutions without having to prove their identity repeatedly. He felt this should be clearer in the seven listed points. • **LI** agreed with **MD** and stated that this would be added to the list of metrics to track. They will also develop questions to measure this aspect. • **Clare Roughley (CR)** Proposed asking SMEs to provide their requirements for a corporate ID solution, particularly in terms of interoperability and flexibility. For example, SMEs might want the ability to issue credentials within their organisation to employees or business partners. Examples of such requirements include

	interoperability, especially with payment contexts, and the control features offered by a corporate ID. **CR** emphasised that SMEs might want capabilities to issue credentials that demonstrate employee relationships in a digital context. • **LI** Thanked **CR** and brought up the question of whether there were additional impact measures that the partners think should be tracked **<u>Open Discussion: Any Additional Impact Measures?</u>** • **AF** highlighted the broader benefit of enabling SMEs to streamline their due diligence processes when starting up. Currently, SMEs go through multiple steps—registering with Companies House, getting a bank account, obtaining licenses—which are all separate due diligence processes. The benefit of the proposed solution would be allowing SMEs to spend less time on administrative tasks and more on growing their businesses. • **Paddy O'Keefe (POK)** raised the idea of whether the use of corporate ID could help SMEs build a credit history. He also pointed out that, depending on a company's behaviour (e.g., being debanked), the system could work in reverse, potentially flagging adverse behaviour. • **LI** acknowledged **Paddy's** point and mentioned that while the focus is not on credit and lending use cases, it might be helpful to ask participants which other use cases, beyond onboarding, they would want to repurpose the corporate ID for. This would provide a ranked list of desired use cases. • **Stefano Buscain (SB)** raised a simple but important point, cautioning that the system should avoid circular logic. For example, if a digital

	corporate ID is required to obtain licenses, but those licenses are also used to obtain the corporate ID, the process could become circular. Managing this risk would be crucial. • **MD** Focused on the need for the corporate ID to remain evergreen (continuously updated). He explained that SMEs would not want to continually provide new information to lenders due to changes in their records. He questioned whether the service would be maintained by SMEs or if the financial industry would bear the costs, as it benefits from the efficiencies. • **LI** agreed with Mark and mentioned that as part of the proof of concept (POC), they would need to determine how the information would be updated and how to present the entire user journey. This would lead to evaluating whether SMEs are willing to pay for the service and how much, based on ease of use and the frequency of updates. • **AF** responded to Mark's earlier question about data responsibility. He explained the "bring your own wallet" approach, where SMEs would have control over their own data. They could update it (e.g., a company name or address change) and broadcast the change securely to relevant parties, bringing SMEs closer to their own data management. • **LU** added a cautionary note, explaining that while SMEs could update their own data, there must be a verification process. He pointed out that businesses sometimes provide incorrect or inflated data (e.g., employee counts), which would undermine trust in the system if not addressed.

	• **AF** suggested that self-asserted data from SMEs could be verified and then used to issue trusted, verifiable credentials. For example, an SME's employee count could be verified and then issued as a trusted credential by a third party.
Comments:	• **AF** CH data (like any user-contributed data with free-form entry fields) has other data quality issues, e.g. county spellings in addresses, this could cause entity matching gaps • **Yaro Zozulya (YZ)** If Corporate ID will be consent based paid for service, does it assume that it will be one of the ways to get onboarded and fraudsters are more likely to use a traditional less secure method which will undermine the key objective of Corporate ID?
Decision:	• N/A
Actions:	• **LI** to invite **AF** to future workshops on model discussions.

Item 4: Open discussion: Consent and Permissions

Purpose: For discussion

Speaker:	• **LI** opened the discussion by emphasising the importance of consent management for corporate ID, considering the regulatory and policy landscape. He invited input on key questions, such as who should obtain consent, whether consent should be perpetual, and how the POC partners had suggested perpetual consent as a potential solution. • **AF** raised the question of how consent applies to a legal entity. Under GDPR, consent pertains to individuals, but how does this work when applied to a company? His query focused on whether consent, typically relevant for individuals, can extend to legal entities.

	• **Nikki Johnstone (NJ)** explained that in typical scenarios like bank accounts, directors are authorised to act on behalf of a company and provide both company and personal data. Consent collection often works through contractual arrangements, with companies representing that they have the necessary consents. She pointed out a key challenge: collecting and maintaining up-to-date information on shareholders for KYC purposes. Even with regulatory requirements, obtaining perpetual updates from shareholders can be difficult. • **LI** followed up by asking whether consent is only required from those with authority to act on behalf of a company, like authorised signatories, and whether shareholder data would also need to be continually updated. • **NJ** for KYC purposes, banks still require shareholder information, even if shareholders aren't directly involved in actions like opening a bank account. This would mean that shareholder data needs to be verified and kept up to date, either by the company or through shareholder participation in an aggregator service. Banks would expect their clients to ensure that shareholder data is current. • **LI** asked if any representatives from banks could provide insights into how they manage periodic reviews of shareholder data and other granular information. He highlighted the importance of understanding how frequently data is refreshed and how banks ensure accuracy. • **MD** emphasised the importance of systems that monitor shareholder data and cross-reference it with other industry data sources. When discrepancies are identified, the customer is contacted for verification. This model helps banks maintain data integrity, with reviews every five years unless triggers arise indicating data issues.

	• **LI** mentioned that obligations might vary depending on stakeholder authority. Shareholders might experience auto-refreshes for data sources, while directors might need to update data manually on a periodic basis. It underscores the need for flexibility in managing data obligations based on stakeholder roles. • **Glen Keller (GK)** raised concerns about addressing fraud and understanding Ultimate Beneficial Owners (UBOs). Fraud prevention requires scrutiny at various levels, especially since small companies with offshore owners or complex parent structures may bypass oversight. Stressed the need to close these loopholes to prevent fraud effectively. Proposed a model where consent for data use is dynamic and trackable, allowing for easy monitoring and revocation of consent for specific use cases. This approach would enhance user control and transparency, ensuring that businesses aren't overburdened by constant onboarding requirements. • **Tony Curzon price (TCP)** introduced a broader perspective, noting the need to measure the macroeconomic benefits of fraud prevention. He links the initiative to improving the UK's global competitiveness as a professional services provider, hinting at how a robust fraud prevention system could attract foreign businesses and drive economic growth. He draws analogies to industries where digitisation led to global standards and success. **Who should obtain consent?** • **CR** highlighted that while legal persons are not subject to GDPR, employees' actions might invoke it. For small businesses, where the

	line between personal and corporate identity can blur, education is needed on the proper use of corporate identity credentials versus personal credentials. • **JR** suggested involving SMEs in focus groups to better understand their willingness to provide perpetual consent, considering their concerns about data sharing. It's vital that the solution aligns with the comfort levels of the SMEs, who are the end users • **MD** mentioned one significant challenge in managing perpetual consent within businesses, specifically when key individuals, such as those initially providing consent, leave the organisation. He points out that many organisations fail to update their banks about such changes, which leads to outdated records of consent and raises questions about the validity and maintenance of this consent. • Emphasised that the critical question is, who ensures that the consent remains active and valid in these scenarios. He suggests that it may be necessary for SMEs to have an obligation to inform banks when key personnel change to ensure that consent remains accurate and relevant. • **Christopher Laws (CL)** echoed concerns about consent, pointing out that it's a complex issue with legal ramifications that need to be carefully addressed. The team needs to explore the legal frameworks surrounding ongoing consent and who within the organisation holds the authority to grant and maintain it. • **POK** added that businesses must be able to revoke access to corporate data for employees who are leaving or being removed. This

	is critical for ensuring that only authorised individuals have access to sensitive corporate information, especially in a dynamic business environment. • **LI** raised the question about how frequently stakeholders change and how banks currently maintain updated records of consent from SME customers. He suggests leveraging existing processes and improving them to handle consent updates more efficiently. • **POK** expressed concern about the potential risks of insider threats when organisations fail to update consent. He emphasises the need for processes that allow the quick revocation of access if there are concerns about certain employees, noting that failure to do so could lead to financial losses for the SME.LI • **LI** agreed, pointing out that the current process, where authorised signatories can simply notify the bank and update records, may need enhancement. He raises a further question about the extent to which corporate ID could be used not only for onboarding but also for facilitating instructions, such as removing or adding authorised signatories. • **Rob Haslingden (RH)** interdependencies between validating directors' identities, maintaining updated data for the corporate ID, and the need for frequent updates, possibly more than once a year. He notes that this may vary depending on the sensitivity of the data and the nature of consents, which could require different levels of permission.

	• **AF** idea of "role-based IDs" where consent for corporate data can be transferred as roles change within a company. He points out that while this system might solve some problems, it would still require manual actions to confirm and update the roles. • **LI** there has to be a mechanism for updating this, manual entry by the incumbent. • **GK** suggested linking the system to Companies House, which could trigger automatic updates when changes in directorship occur. He stresses the importance of not overcomplicating the consent process, recommending a use-case-driven approach where consent is perpetual when necessary but reviewed periodically, similar to how companies handle ICO registrations. • **NJ** raised two key points regarding perpetual consents and data quality in relation to banks and other intermediaries. When discussing who needs to collect consent and what type is required, it depends on the data controller requesting it. Banks may not need explicit customer consent due to their ability to rely on legal bases for data processing, but intermediaries like aggregators would require specific consents. • **NJ** highlighted issues around data quality, noting that poor data upkeep could lead to low user confidence. A potential remedy could involve sharing information about bad actors, such as fraudsters who alter company details to mask identities. A recent law change allows banks to share information on bad actors with other institutions, which could help improve data accuracy and encourage more participation.

	• **LI** echoed **NJ's** points, particularly regarding fraud databases like CIFAS and the Fraud Action Database. He acknowledged the lack of standardised data sharing mechanisms between banks for flagged accounts and emphasised the need for technical improvements. • Asked whether data consent requirements apply equally to banks and aggregators • **NJ** clarified that banks could rely on legal processing grounds for data they collect, but intermediaries like aggregators would typically need independent consent from customers. • **POK** suggested an ID stack system, where individuals' corporate identities could be transferable between companies. This could empower employees who move between organisations, enabling them to retain personal attributes linked to their professional profiles. • **LI** Mentioned that Level 5 of the corporate ID stack is focused on individual data.
Comments (on chat):	• **RH** When looking at the issue of Consent, can we consider this in the context of what the key data components are that we're suggesting should be included in Corporate ID. Some are easier to process under different processing terms to consent i.e Legitimate Interest, and others are more complex such as Open Banking that requires overt consumer Consent for a limited time. • **CR** https://search.gleif.org/#/record/724500ORDYU6423N3851 • **CL** I was going to raise the same topic which Glen & Clare. Consent probably needs to be varied by use case (KYC v Fraud for example), do we have expertise in the coalition to advise us on what is legally required?

	• **AF** OB uses consent, e.g. for sharing transaction data via AISP - if sharing from a business bank account, is the transaction data classed as personal data in GDPR? • **RH** Good point. OB data is shared under PSR/PSD2 rules and not GDPR...so different governance process. • **NJ** We (A&O Shearman) can happily support on that. Happy to do a separate session but will otherwise send feedback / thoughts via email to Leon. • **AF** a director resigning at CH could trigger a credential revocation process, or appointment an issuance process • **AF** Synectics is another fraud data source (One Login uses this, as do we) • **AF** people don't consent to CRAs holding data - they have separate legal bases. Is 'consent' the right word to use relating to corporate data? gets confusing with 'consent as GDPR basis'
Decision:	• **N/A**
Actions	• None
Item 4: Closing Remarks	
Speaker: LI	• **LI** An interim paper is set for publication in November, with feedback and approval from partners before dissemination. Input will also be sought from POC partners. • Upcoming sprints will cover corporate ID verification, data components, customer flows, and possible models (aggregator, wallet, or hybrid).

	• Partners were thanked for their contributions. The next sprint will be on October 4th, ongoing feedback was encouraged to shape the final blueprint.
	• N/A
Decisions	• N/A
Actions	• None

Attendees:

Chair/s: Leon Ifayemi (LI)

Total attendance: 49

Organisation
CFIT
CoLC/CFIT
Lexis Nexis Risk Solutions
Esynergy
OneID
Virgin Money
Experian

EY
A & O Shearman
Sage
Visa
Dun & Bradstreet
Nationwide
Companies House
Fintech West
TransUnion
Mastercard
Innovate UK
FDATA
Yoti
TechnoXander
University West of England
DnB
CTRL- SHFT
HSBC
CRIF

Lloyds Banking Group
OIX
GLEIF
Alloy
Open Data Consultancy