**Centre for Finance, Innovation and Technology (CFIT)**

**Digital Company ID & Fighting Economic Crime: Market Opportunity Working Group**

**Meeting Minutes**

Sprint Session 11

8 October 2025 at 11:00 am | Microsoft Teams

**Attendees:**

| Name | Organisation |
|---|---|
| Rob Haslingden (Chair) | CFIT |
| Sajni Shah | CFIT |
| Adrian Field | OneID |
| Chor Teh | Moody's |
| Cormac Mealey | EY |
| David Rennie | Orchestrating Identity |
| Emily Hyett | Yoti |
| Florian Chevoppe-Verdier | DSIT |
| Francis O'Neill | Lloyds Bank |
| Gaurav Sarin | Leading Point |
| Ghela Boskovich | FDATA |
| Henry Balani | Encompass Corporation |
| Howard Wimpory | Encompass Corporation |
| Jake Bowen-Bate | Amiqus |
| John Harrison | UCDx |
| Leighton Hughes | City of London Corporation |
| Lewis Utley | Dun & Bradstreet |
| Louise Beaumont | Mastercard |
| Nicky Hickman | Digital Egret |
| Nikki Johnstone | A&O Shearman |
| Richard Seaman | Dun & Bradstreet |
| Stuart Young | MyIdentity |
| Joseph Kamyar (Secretariat) | Skadden, Arps, Slate, Meagher & Flom |
| Martin Katunar (Secretariat) | Skadden, Arps, Slate, Meagher & Flom |

**Agenda:**

1. Welcome
2. Legal and Regulatory Considerations, MVP Review
3. Open Discussion:
    a. Legal risk assessment
    b. Understanding where liability is concentrated

4. Next Steps

## 1. Welcome

*Speakers: Rob Haslingden (RH)*

1.1. RH opened the meeting, welcomed attendees, and outlined the agenda. The eleventh sprint will focus on legal and regulatory considerations; the working group will review the digital company ID data flow, examine compliance requirements, and discuss where liability is concentrated.

1.2. Attendees were reminded of the competition law guidelines and the importance of complying with them.

## 2. Legal and Regulatory Considerations: Introduction

*Speakers: Nikki Johnstone (NJ) and Rob Haslingden (RH)*

2.1. NJ highlighted that the session's main purpose was to explore the key legal and regulatory risks, whether there are any gaps in legislation and regulation, and how such gaps could be resolved. NJ noted that commercial models and contractual arrangements will primarily determine liability allocation. The session will consider whether the most pressing legal and regulatory considerations rest in regulation, guidance or otherwise. NJ encouraged attendees to share feedback and consider these issues with their own legal teams to help identify and address risks.

2.2. RH referred to the slides presented at the meeting, outlining the key actors involved in the digital company ID data exchange process, including authoritative data providers, holder service providers, aggregation players, and relying parties. He emphasised the need for ongoing access to data sources to maintain an accurate digital identity and highlighted how this framework brings into focus important issues around consent and liability as data moves through the digital company ID ecosystem.

2.3. RH further described the company ID MVP data flow and partner responsibilities, where an SME consents to share personal and business data via a web hosting partner into a digital wallet, with an orchestration provider integrating the data and securely sharing the data with relying parties. RH noted that the CFIT team is already considering how liabilities and responsibilities will be allocated among the parties. RH added that the meeting slides represent an initial attempt to outline the roles and responsibilities of participants in the digital company ID data ecosystem, including whether such participants act as data controllers or processors. RH invited attendees to provide feedback to help further clarify and refine these roles.

2.4. RH highlighted the need to triangulate personal and company ID information to ensure the accuracy and validity, referencing the sources such as Companies House, HMRC, and credit reference agencies. He emphasised this process would enhance trust and provide assurance about the accuracy of the company ID information.

2.5. NJ discussed several key areas of law relevant to digital company ID, including the Data (Use and Access) Bill, the complex interplay with the GDPR requirements, and financial crime legislation, including anti-money laundering and sanctions regulations. NJ further highlighted the impact of forthcoming guidance from the Joint Money Laundering Steering Group, and the challenges of cross-border data sharing and interoperability under frameworks like the EU's eIDAS regulation. NJ emphasized that organisations in the digital company ID space will need to work closely with legal advisors to navigate these overlapping regulatory obligations, and highlighted the importance of understanding the specific obligations of each party in the data flow.

2.6. NJ noted that while there are government-issued codes specifying suitable digital ID attributes for right to work and right to rent checks, there is currently no equivalent code for KYC or KYB processes involving corporate entities. NJ queried whether establishing a code with minimum standards for corporate identity verification could be a helpful starting point.

## 3. Open Discussion

*Participants: Adrian Field (AF), Chor Teh (CH), David Rennie (DR), Francis O'Neill (FO), John Harrison (JH), Nikki Johnstone (NJ), and Rob Haslingden (RH)*

3.1. Accreditation providers:

3.1.1. RH asked whether, as with personal identity providers, the government should be responsible for accrediting digital company ID providers based on the proposed trust and governance framework, and whether this approach would underpin the sourcing and attestation of data in the company ID process.

3.1.2. AF confirmed that this is broadly how accreditation works today for personal ID providers: UKAS (the United Kingdom Accreditation Service) oversees national accreditation schemes, appointing auditors such as Kantara and BSI to certify digital verification service providers. He explained that certification is conducted by independent auditors within the UKAS framework, not directly by the government. AF and RH agreed that the working group should recommend that a similar approach is replicated for digital company ID accreditation.

3.2. Mandatory versus voluntary accreditation:

3.2.1. NJ raised the question of whether certification for digital company ID providers should be mandatory, noting that the current DTIF framework is voluntary and self-certification is not required. AF confirmed that participation in the framework is optional, except for certain use cases like digital criminal records checks, which are mandated. He suggested that, at least initially, certification should remain optional, with the possibility of making it mandatory in the future if the voluntary approach proves insufficient. NJ observed that maintaining an optional certification regime could differentiate the UK from the EU, where mandatory certification is required, and may offer competitive advantages for international providers.

3.2.2. DR highlighted the increasing complexity of regulations and the significant compliance burden on both regulators and organisations, with some estimates suggesting 10–12% of GDP is spent on regulatory compliance. He questioned the effectiveness of some of the regulatory requirements, noting, as an example, that there is little evidence that increased compliance requirements are reducing money laundering or fraud. DR suggested that, given these challenges, the voluntary accreditation model described by AF may be the practical way forward, and argued that the practicality of the voluntary model should be demonstrated to the government.

3.3. Code of practice:

3.3.1. NJ raised the question of whether additional assurances – such as new codes of practice or mandating certification for digital company ID providers in certain use cases – should be introduced. She referenced open banking, where licensing and compliance requirements were imposed to address specific risks, and suggested that a similar approach could help manage risk for relying parties in the digital company ID context and ensure a viable framework for digital company ID.

3.3.2. DR recommended an incremental and voluntary approach to developing standards for digital company ID, suggesting codes of practice should be built gradually. He emphasised that attempting to address all aspects of digital company ID at once would not be feasible.

3.3.3. NJ suggested that, rather than mandating certification for digital company ID providers, it may be beneficial for government bodies such as the Department for Science, Innovation and Technology (DESIT) or the Office for Digital Identities and Attributes (OFDIA) to develop additional codes of practice or technical standards for specific use cases. She proposed that introducing credential standards or codes of practice on verification assurance – similar to those already established for personal ID – could help provide greater comfort and confidence to counterparties engaging with company digital ID services.

3.3.4. AF agreed that a clear set of rules defining what constitutes a company ID and the associated roles and responsibilities should be established. He noted that whether these rules are included in the main DIATF or in a supplementary code is less important, as long as the foundational standards are clearly set.

3.4. Competition law considerations:

3.4.1. NJ raised competition law considerations associated with the involvement of international companies and big tech in the UK digital ID market. NJ noted the risks of market lock-in, which may lead regulators such as the CMA and FCA to focus on this area. NJ queried whether the working group's report should consider recommending minimum standards for availability and restrictions on bundling digital ID with other services.

3.4.2. DR noted that the digital ID market is complex and benefits from having both large and niche players who can address specific market needs and provide specialist solutions. He cautioned against limiting market diversity, emphasising that big tech can play a valuable role alongside smaller providers, and that in some cases, their scale may be advantageous, while in others, niche providers may be better suited to deliver services to certain components of the ecosystem.

3.4.3. JH suggested that the goal should be to create digital public infrastructure, similar to payment systems, rather than fostering competition between individual digital ID providers, which would fundamentally change the nature of the competition question.

3.5. Open banking comparison: NJ provided a brief overview of the open banking legal framework, explaining that it was initially mandated by the CMA following a competition law review, which required nominated banks to develop APIs for third-party access to account information and payments. This led to the creation of the Open Banking implementation entity to set minimum technical standards. The contractual arrangements between banks and third parties are not mandated, but are not prohibited either, allowing parties to go beyond the minimum expectations. The subsequent PSD2 regulation formalised a liability framework, ensuring that banks are responsible for refunds and compensation in cases of unauthorised or defective payments. This ensures clarity for customers regarding where to seek redress and delineates liability between banks and open banking providers.

3.6. Data sources and managing data transfers:

3.6.1. JH highlighted the complexity of company ID, noting that there are at least two types of entities involved – the company itself, which controls and releases its own "visible" data, and banks and other relying parties, which access both "visible" and "invisible" data (such as sanctions, PEPs, fraud and credit reference checks). He questioned how switching between

corporate wallet providers would be managed given that part of the data is not controlled by companies.

3.6.2. RH suggested that the core data attributes forming the digital company ID are sourced from authoritative providers, while additional risk-related data such as sanctions, PEPs, and risk scores remain separate and are applied by banks according to their own risk appetite and use cases. He explained that switching company ID providers would be a matter for the customer to communicate with their bank, which would then decide whether to accept the credentials of the new provider based on the provider's accreditation and the bank's own risk assessment, making it a relationship management issue between the bank and the customer.

3.6.3. JH pointed out that while the components of a company ID – comprising both "visible" (controlled by the SME) and "invisible" (typically accessed directly by banks) data – have been defined, there is not yet agreement on whether these should be delivered under a single commercial contract or two separate ones. He suggested that, due to the differing nature and control of these data types, company ID may ultimately require two contracts for these two data sources.

3.6.4. RH argued that back-office data like sanctions and PEPs are not part of the company ID dataset and are handled separately by banks, while the company ID is based on "visible" data shared by the SME.

3.6.5. CT agreed with RH, stating that there should be no conflict regarding PEPs and sanctions data, as these screenings are required regardless of the digital ID provider and are handled separately from the company ID. He emphasised that company ID should be designed for interoperability, allowing users to switch providers.

3.6.6. AF agreed that integrating multiple data sources for banks is a matter of commercial and contractual choice, unrelated to the core company ID project. He explained that relying parties can easily connect to different vendors via APIs, allowing banks and other relying parties to select their preferred data sources. AF also clarified that the aim of this working group is not to build a centralised platform; instead, the digital company ID should serve as a data feed into existing AML and onboarding platforms, with banks and other relying parties retaining the freedom to choose among various competitive solutions in the open market.

3.6.7. JH clarified that he is not advocating for a centralised platform, but is interested in the future evolution of company and personal digital IDs, particularly whether they might eventually support advanced applications such as payments and communications. He noted that such developments may fall outside the core business interests of current providers, and

emphasised the importance of considering long-term possibilities and broader use cases, rather than focusing solely on immediate challenges.

3.6.8. AF clarified that the current scope of the working group does not extend to payments. JH acknowledged this but questioned whether such a narrow focus is appropriate, suggesting that it may be short-sighted.

3.7. Liability:

3.7.1. AF explained that, digital identity providers, as data brokers, presently guarantee the accurate transfer of data from the original source to the relying parties (such as banks or telecommunication companies) without alteration, but identity providers do not assume liability for errors at the source or for downstream GDPR risks. He emphasised that any transfer of liability should be addressed through commercial agreements, either bilaterally or via broader multilateral schemes, and advised starting from the current position of no liability.

3.7.2. RH argued that current liability and compliance models need to evolve, particularly to address banks' desire to reduce their responsibility for rechecking data. He emphasised that, for trust and assurance in digital company ID and other smart data schemes, each party contributing data to the ecosystem should stand by its accuracy. RH also highlighted the importance of maintaining persistent links between company ID providers, relying parties, and authoritative data sources to track and confirm changes in digital company ID data over time. This persistent, dynamic approach is distinct from existing personal ID models and is essential for maintaining accurate company profiles and detecting potential fraud or suspicious activity.

3.7.3. AF emphasised that, beyond ensuring data accuracy, it is important to verify that the person presenting the data is its legitimate owner, to prevent impostors from misusing correct information. RH agreed, reiterating his point about the need for digital company ID providers to assume greater liability. AF responded that before any such shift in liability is considered, there must be a clear understanding of the specific risks involved, as it is not possible to accept liability without first defining and assessing those risks.

3.7.4. DR highlighted the importance of having a consistent liability model for government involvement in digital ID schemes. He noted that while government has traditionally acted as a data source, if it also serves as an identity service provider, it should be subject to the same liability standards as any other market participant.

3.7.5. NJ noted that the implementation of digital ID will likely require multiple contractual relationships to meet the specific needs of relying parties. NJ questioned whether the default expectation is for an ID provider to contract

directly with both the SME and the relying party, or if this relationship would typically be managed by an orchestration provider. AF responded that either model is acceptable, and it should be left to each bank to decide with whom they wish to contract.

3.7.6. NJ summarised the differing perspectives on liability for digital ID providers, and opened the discussion to the group, asking whether there is consensus that digital ID providers should assume minimal liability for data deficiencies, given that banks conduct their own checks with various providers.

3.7.7. AF explained that the level of liability a digital ID provider should assume depends on their role in the data flow. For example, if the provider is simply passing data through APIs from a credit agency to a bank without modification, their liability should be minimal, mainly limited to aggregation which is done for contractual simplification. However, if the provider is storing data, protecting it, or performing data triangulation and aggregation to create new credentials, they add more value and, consequently, may assume greater liability and assurance obligations. The key distinction is whether the provider is merely transmitting data or actively processing and generating new data elements.

3.7.8. NJ noted that banks might be concerned about whether the individual submitting company details for a digital ID has the proper authority to do so. She questioned whether relying parties would expect digital ID providers to guarantee that the company has granted appropriate authority for the deployment of its digital ID for specific services.

3.7.9. JH highlighted that company ID could serve as an externalised authorisation framework, allowing companies to visibly assign specific permissions to individuals. This external visibility of authorisations, which is currently lacking, would be highly valuable.

3.7.10. RH emphasised that banks and other relying parties want to avoid rechecking information already supplied in the company ID, preferring to rely on its accuracy for automated verification. This expectation shifts liability away from the bank and onto the company ID service provider, who is then responsible for ensuring the accuracy of the data and for being notified of any changes by the SME. RH noted that accredited company ID providers should be expected to stand behind the accuracy of their information, and highlighted the need to clarify how liability is distributed among all parties involved, including the SMEs, the ID providers, and the relying parties.

3.7.11. FO agreed with RH, emphasising that as data moves through the digital ID ecosystem, each service provider is responsible for the accuracy of their output, so that by the time the data reaches the bank or another relying party,

it can be relied upon as verified and factual. He noted that while banks may apply their own risk assessments and use additional data sources, they should be able to trust the integrity of the data received through digital company ID. FO also stressed the importance of banks providing feedback if they identify discrepancies – such as through sanctions or PEP screening – to prevent incorrect or fraudulent information from being used elsewhere, suggesting that a feedback mechanism should be built into the system.

3.7.12. DR reiterated the importance of ensuring that banks do not have to duplicate checks already performed in the digital ID process, as this would be inefficient. He emphasised that banks should be able to rely on data provided through the company ID, with the assurance that appropriate checks have been conducted according to established codes of practice or standards. This approach would allow liability for data accuracy to shift away from the bank to the original data source and the individual supplying the information, thereby achieving the key benefit of reducing the bank's liability and streamlining the verification process.

3.7.13. JH agreed with FO that banks need to trust data received from company ID. However, he clarified that banks should only provide feedback on data for which they themselves are the authoritative source – such as a company's credit line – rather than on data supplied by others. This allows banks to contribute verified attributes to the company ID, which can then be aggregated and shared as needed.

3.7.14. AF agreed on the importance of a two-way data flow between the company ID wallet and the bank and other relying parties, noting that some data should be visible to the data subject, while other information – like fraud signals – should remain hidden to avoid alerting potential fraudsters.

## 4. Next steps

*Speakers: Rob Haslingden (RH)*

4.1. RH concluded the meeting by thanking participants for their contributions and stating that the key discussion points will be documented and used as the basis for the next meeting, where the group will further discuss liability and contractual considerations.