Centre for Finance, Innovation and Technology (CFIT)

Digital Company ID & Fighting Economic Crime: Trust & Governance Framework Working Group

Meeting Minutes

Sprint Session 13

07th November 2025 | Microsoft Teams meeting

Attendees:

Name	Company
Nikki Johnstone (Chair)	A&O Shearman
Ghela Boskovich	Smart Data and Technology Alliance
Nick Mothershaw	Select ID
James McGreevy	CFIT
Luca Britos	A&O Shearman
Emily Hyett	Yoti
Adrian Field	OneID
Lewis Utley	DNB
Katarina Pranjic	Lexis Nexis Risk Solutions
David Rennie	OIdentity
John Harrison	UCDx
Xiaodi Wang	GLEIF
Florian Chevoppe-Verdier	DSIT
Gaurav Sarin	Leading Point
Sally Henstock	TransUnion

Stuart Young	Etive Technologies
Rafael Pontes	EY
Cindy van Niekerk	Umazi
Daniel Jonas	Pay.UK
Mark Terry	Lloyds
Chor Teh	Moody’s
Gilbert Hill	N/A
Calum Roberts (Secretariat)	Fuse, A&O Shearman
Katherine Pittalis (Secretariat)	Fuse, A&O Shearman

Agenda:

(1) Welcome

(2) Risks and Regulatory Considerations for Relying Parties

(3) Open Discussion

(4) Use Case Considerations

(5) Open Discussion – How Can We Address These Risks?

(6) Next Steps

(7) Appendix

1. Welcome

Speaker: James McGreevy (JM)

1.1 JM welcomed all participants to the 13th meeting of the Trust & Governance Framework Working Group.

1.2 JM reminded all working group members of the importance of adhering to the guiding principles on competition (as set out in the slides) and encouraged participants to engage and collaborate with the working group in an open and respectful manner.

1.3 The primary objective of this meeting was outlined:

(a) Identifying risks and regulatory considerations for relying parties through the lens of the four priority use cases: (1) bank onboarding, (2) government servicing, (3) SME-supplier verification and (4) SME digital platform access.

(b) Addressing key questions on assurance levels; attribute freshness and warranties; liability for mis-issuance / mis-verification; error handling and redress; evidential standards and audit trails; independent assurance; right-to-audit and forensics; termination and continuity.

2. RISKS AND REGULATORY CONSIDERATION FOR RELYING PARTIES

Speakers: Nikki Johnston (NJ)

2.1 NJ set the scene for a practical discussion on key legal and regulatory themes encountered by relying parties adopting Digital Company IDs. She noted the focus would be on levels of assurance appropriate to incentivise adoption, rather than exhaustive risk catalogues.

2.2 NJ highlighted the potential risks for relying parties adopting new technology:

(a) **Regulatory compliance risk.** regulated relying parties will expect demonstrable compliance with legal and supervisory requirements, including FCA expectations on financial crime/KYC, GDPR, and outsourcing controls governing third-party reliance for core activities.

(b) **Data quality, provenance and keeping sources updated.** relying parties will require confidence in both the quality of data being received and the sources that are being relied upon by a Digital ID provider, and therefore that checks are up to date and reliable.

(c) **Fraud and impersonation risk.** increasing sophistication of fraud, including AI deepfakes is a growing concern. It was stated as being important to have robust binding between a company and the natural-person officer or authorised signatory purporting to act on the company's behalf.

(d) **Operational resilience and service continuity.** Heightened regulatory focus on resilience as a matter of national security. The concern that third parties, that a firm might engage of rely on to validate the identity of customers or counterparties, do not cause or extend cyber or other information security incidents, and that their services are reliable and not, themselves, likely to experience significant downtime.

(e) **Information security and cyber risk.** The risk of hacking and that customers who link a Digital ID to a bank or other firm may become targets or victims of cyber incidents compromising the data held or collected by certain DBS providers. There may also be technical risks depending on the models used to train or process data.

(f) **Change management and lifecycle controls.** Non-fraud corporate lifecycle changes, such as director appointments/resignations, name changes, addresses, and authorised signatory updates, may present a risk if administrative updates are not made in a timely manner and recurring errors if not promptly reflected.

(g) **Legal enforceability and liability allocation**. Concerns about liability for errors in data which may have been caused by faults with the data source or errors in the data source or emissions in the data source.

(h) **Consumer and complaints exposure**. Concerns that where there's an expectation Digital ID is being used to process the correct data that complaints may arise for not providing an escalation path or an opportunity to correct incorrect data.

(i) **Model and algorithmic risk.** Technical models and tools used to process, match, and score data create additional risk, including performance drift, bias, and explainability gaps.

3. OPEN DISCUSSION

Speakers: John Harrison (JH), Nikki Johnstone (NJ), Mark Terry (MT), Adrian Field (AF), Nick Mothershaw (NM) and Cindy van Niekerk (CvN)

NJ emphasised the goal of identifying "big picture" issues and aligning them with a proportionate, risk-based approach to assurance that can practically support adoption. NJ invited reflections on the most sensitive risks being observed in the market.

3.1 Competition and Market Consideration.

JH raised the need to consider competition issues as collaboration among wallet providers grows, noting early-stage market share is small but ubiquity could later trigger CMA concerns. NJ responded that competition topics would be address with A&O Shearman's competition partners in a round-up session.

3.2 Distinguishing Existing VS New Risks.

(a) MT observed that many risks cited (such as sanctions screening and impersonation) already exist in current bank onboarding and KYC processes and therefore distinction should be made between 'existing risks' and 'new risks' introduced by Digital Company ID. Digital ID primarily changes the data ingress and may relocate certain controls from bank to provider rather than creating fundamentally new risks. For example, if identification and verification move to a certified ID provider, the control for impersonation/fraud likewise shifts.

(b) AF reinforced that banks already use certified remote onboarding, and value derives from certification to open, battle-tested rules and security standards (e.g. DIATF, DBS). AF advised pulling authoritative data directly (e.g., Companies House) rather than copying to wallets, to maintain freshness.

(c) NJ stated that existing laws, including the Data Act and DITF environment, broadly facilitate Digital Company ID solutions. NJ confirmed that where risks remain unchanged or reduce (by Digital Company ID), this would be recorded in the report.

3.3 Fraud Signal Sharing: Legal Gateways.

AF described DIATF-envisaged fraud signal sharing (Synetics, Cifas, National Hunter) increasing richness of sector intelligence and closing gaps exploited by fraudsters. NJ queried data sharing mechanism for banks and noted the need to examine legal models, ICO compliance and reciprocity across sectors. NJ agreed to explore and note in the report potential legal gateways and models for fraud data and intelligence sharing that include ID providers, in compliance with data protection law.

(a) **Timeliness and data freshness.** DJ asked how "timeliness" of authentication tokens and updates should be treated and whether an ALARP-style approach is used. NJ noted variance by relying party and use case, but recognised that for some events (e.g., authority-to-act at point of transaction), reliance must be very current.

(b) MT confirmed that, from a banking perspective, information must be accurate at the time of collection, with explicit document validity windows and revalidation requirements. Sanctions risk tolerance is effectively zero, whereas fraud and impersonation controls are applied on a risk-based basis. NJ highlighted the ongoing challenge: relying parties will wish to rely on prior-verified data across a journey and over time while maintaining confidence that attributes remain current at points of access.

3.4 Commercial Models, Incentives and Data Ownership.

(a) LU cautioned that providers' fraud-detection innovations are commercially sensitive, and investment depends on maintaining a competitive business case; any mandated centralisation of proprietary signals needs to address incentives. He added that fraud can be reduced but not eliminated.

(b) JH raised the distinction between "type 1" company-owned or public/semi-public data (e.g., Companies House, identity proofs) and "type 2" provider-owned or IP-protected data (e.g., CRA/fraud analytics feeds). He noted the need to consider how the different IP and commercial regimes can coexist within a Company ID bundle without disadvantaging data owners or overbundling data that should remain separately governed.

(c) MT explained that while regulated "reliance" between banks is legally possible, in practice it is cumbersome because the receiving bank remains liable and must QA the other's process. The Chair confirmed that, for the report, this nuance should be captured as context on why banks typically do not adopt inter-bank reliance at scale.

(d) AF suggested that reliance is best framed here in terms of "levels of assurance" within DIATF and OpenID Connect metadata rather than AML "reliance" under the Money Laundering Regulations (MLRs). NM reinforced that the framework speaks to assurance levels and relying parties' risk-based judgments. NJ explained that most banks eschew MLR reliance because they remain fully accountable;

however, they may accept DIATF-aligned assurance from certified providers. JH noted the lag between MLR constructs and new identity-market realities. NJ agreed to reflect the terminology distinction in the report.

3.5 Ongoing Authentication Models

(a) JH advocated for a wallet-led, ongoing authentication model where the digital wallet acts as the user's trusted agent for accessing bank services, and streams attribute updates to relying parties in near-real-time. MT agreed that such a model would be close to "utopia" for banks, provided governance and contractual frameworks enable banks to receive and rely on updates on an ongoing basis (today addressed via periodic review or perpetual KYC listening services).

3.6 Corporate Lifecycle Changes

(a) NJ questioned whether it was realistic to place an expectation on customers to keep their data up-to-date and how corrections should flow to relying parties when source data could be wrong or compromised.

(b) CvN referred to research that indicated that one of the biggest challenges for SMEs was the need to go through a verification process time and time again. She said that SMEs would pay for a single service to update and distribute the data across providers, reducing repetitive due diligence.

(c) JH pointed to Companies House's annual confirmation statement as a statutory model and suggested that pressing a single "update" should notify all relying parties. He endorsed wallet-centric, many-to-many propagation.

(d) LU cautioned that companies update when it is in their interest; mechanisms should reduce friction and create clear benefits.

(e) AF stressed making updates "in-the-moment" by easing admin via a corporate wallet integrated to Companies House (two-way flows), which should drive more frequent updates.

(f) NJ posed escalation scenarios for erroneous source entries (e.g., fraudulent director appointments). Adrian suggested providers can flag discrepancies across sources back to directors, but determining which source is "correct" may require process design. NJ reiterated the need for practical dispute and remediation paths.

(g) MT noted a mandatory requirement for banks to report discrepancies to Companies House discovered during onboarding; NJ confirmed the same applies to law firms and that this should be noted.

4. USE CASE CONSIDERATIONS

NJ briefly presented the legal overlays across four use cases set out in the slides, with a focus on:

1. **Bank Onboarding**: requires high to very high assurance, real time accuracy at collection and strong wallet protections.

2. **Government Servicing**: SME-Supplier Verification and SME Digital Platform Access – may accept lower assurance for specific attributes (e.g. age verification), but bank's higher standards should anchor design.

5. OPEN DISCUSSION – HOW CAN WE ADDRESS THESES RISKS?

Speakers: John Harrison (JH), Nikki Johnstone (NJ), Daniel Jonas (DJ), Adrian Field (AF) and Chor Teh (CT)

NJ opened this section by noting practical sensitivities and keeping KYC data current and the reputational difficulty of challenging clients on accuracy at onboarding.

5.1 Assurance Levels

(a) NJ asked whether relying parties beyond banks would expect the same level of assurance as financial institutions, and how far ID providers can reasonably go across different use cases.

(b) JH responded that progress depends on making solutions satisfactory and attractive to banks, whose requirements are more stringent. Once banks are comfortable, other companies' expectations would be satisfied.

(c) DJ observed that outside specific legislative mandates, assurance calibration would be dynamic and risk-based, driven by agents that operate in near real-time and at granular levels, and cautioned against 'hard-coding' parameters that would stifle dynamic calibration.

(d) AF explained that all GPG 45 assurance levels are possible in practice (medium, high, very high) with limited demand for low. Higher assurance requires more triangulation points, increasing costs and user friction. He emphasised balancing the friction built into the customer journey against assurance outcomes.

(e) CT described vendors' internal governance for assurance, including validating client-submitted data (with documents) against audited financials, curating data, and layering freshness and screening to ensure point-to-point linkage. He stressed assurance as a fundamental vendor mandate and the importance of documented internal data governance confirming accuracy and update frequency.

(f) AF further recommended that, in addition to identity assurance, the wallet itself must meet quality of authentication and protection standards. He proposed that corporate ID wallets should have strong customer authentication, equivalent to bank apps, otherwise there would be a higher account takeover risk.

5.2 Liability for Mis-Issuance/Mis-Verification

MT noted how if verification and identification checks are digital then this is an important component as it would mean that fraud and impersonation control would move.

5.3 Independent Assurance

Based on the open discussion, NJ noted that to increase enthusiasm from banks and others in the market to adopt Digital Company IDs is for providers to provide assurance that the data collected from all the trusted sources is accurate and can be relied upon on an ongoing basis.

5.4 Termination and Continuity

(a) NJ raised the risk of termination of use of a particular ID provider or the insolvency of a company being communicated to a bank or some other relying party. This is relevant if companies intend to port to another provider or put a hold on any action being taken by the relying party.

(b) MT proposed establishing a validity window to allow switching (e.g. a three-month grace period) and a signal model: "green tick" (verified), "amber tick" (pending and use data at risk) and "red tick" (do not rely). He emphasised that the approach would depend on the relationship was transactional or ongoing.

(c) DJ referenced analogies to porting Digital ID to current account switching, cautioning that portability typically requires some orchestration and common processes to avoid fragmentation.

(d) AF suggested designing for new wallet setup using authoritative sources, pulling data straight from Companies House, rather than a complex porting approach.

6. Next Steps

6.1 The 14th sprint will be held in-person on 20th November 2025 at A&O Shearman. This sprint will focus on Monitoring & Maintenance Cross-Sector & Policy Alignment.

7. APPENDIX

Acronyms

ALARP – As Low as Reasonably Practicable

AML – Anti-Money Laundering

CIDASP – Company Identity Digital Attribute Service Provider

CMA – Competition and Markets Authority

CRA – Credit Reference Agency

DBA – Disclosure and Barring Service

DIATF – Digital Identity and Trust Framework

DSIT – Department for Science, Innovation and Technology

FCA – Financial Conducts Authority

GPG – Good Practice Guide

KYC – Know Your Customer

MLRs - Money Laundering Regulations