Minutes of meeting

Sprint 6

Date: 04.10.24 | Virtual meeting

Agenda

1. **Introductions**
2. **Cifas Presentation**
    a. Presentation by Sandra Peaston, Director of Research and Development at Cifas
    b. Open Discussion
3. **Company ID Model**
    a. Company ID: Data Model and New Roles
    b. Open Discussions
4. **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. • Reminder of the anti-competition principles all CFIT Coalition meetings are governed by. • **LI** confirmed the agenda and introduced Cifas.
Comments:	None
Decision:	N/A – for information only

Actions:	None

Item 2: Cifas Presentation

Purpose: For discussion/information

Speaker: SP	• **Sandra Peaston (SP)** Introduced Cifas and outlined the objective to provide a 10-minute overview of the organisation's data sharing capabilities and the National Fraud Database (NFD). • The focus was to familiarise participants with the use of data for fraud risk assessments, particularly for those less familiar with the organisation's offerings. • Cifas has been sharing fraud-related data for 35 years, connecting over 750 organisations. • Members report fraud cases to the NFD, which other participants can access to assess risk. The system is designed to be reciprocal: members must contribute data to benefit from it. • Emphasis on community collaboration in fraud prevention. **National Fraud Database (NFD)** • Core database, running for 35 years, consisting of 2 million recorded fraud cases. • Primarily includes identity fraud (1.3 million cases), misuse of facilities (~400,000 cases), facility takeovers, and false applications. • Open to public and private data sharing as per the Serious Crime Act 2007. **Other Databases and Tools:** • Insider Threat Database: For employment risk assessment. • Vision: Ongoing customer monitoring solution.

	• Identity Check: Digital identity verification under Home Office framework.
	
	Data and Fraud Types:
	• Major types of fraud recorded:
	  ○ **Identity fraud**: Constitutes the largest proportion (1.3 million cases), often involving the misuse of consumer or company details.
	  ○ **Misuse of facility**: Fraudulent use of bank accounts (~400,000 cases).
	  ○ **Facility takeover and false applications**: Significant types affecting both consumers and companies.
	• Organisations can match fraud cases using various identifiers, such as personal information, document numbers, and even facial recognition.
	• Address matching is used but refined to reduce false positives by focusing on high-risk addresses.
	
	Additional Services:
	• **Facial Matching & CaseLink:** Links fraud cases across the database, identifying networks of fraud using face recognition and other attributes.
	• **Proactive Alerts:** Alerts for members about potential risks, including insider fraud and identity fraud associated with particular addresses or domain names.
	• **Intelligence Services:**
	  ○ Provides risk alerts and reports based on emerging fraud trends.

	○ The new **Entity-Based Intelligence Reporting Service** will offer actionable intelligence to subscribing members based on leads developed by the organisation's team. **<u>Open Discussion</u>** • **LI** Thanked Sandra for her presentation, highlighting the future vision and the importance of reciprocal data sharing. • Introduced the Q&A session and posed a question to the group: • **How would organisations ideally absorb fraud data—directly into systems and processes or via third parties? If through third parties, how would this data be utilised within their services?** • **SP** Clarified the question by discussing how many organisations currently access fraud data via credit reference agencies for years. • Stated that while credit reference agencies are integrated into application systems, there's potential for broader use of the data. • Encouraged organisations to consider how the data fits into their operational "stacks" and how they would prefer to ingest it. • **Adrian Field (AF)** Mentioned that many certified ID providers, including his, already consume fraud data as part of identity verification (ID&V) checks under the GPG 45 profiles. • Noted that fraud data sourced from the National Fraud Database or similar providers is fed into corporate ID verification processes, highlighting an existing integration route. • **SP** Acknowledged Adrian's comments and explained that there are two parts to the process: • **Identity Verification (ID&V):** This part of the service focuses on verifying whether the person or organisation is who they claim to be.

	• **Fraud Risk Assessment:** The second element assesses whether the person or organisation has a history of fraud, e.g., involvement in money laundering or other fraudulent activities. • Stressed the importance of filtering data to focus on relevant fraud risk information, especially when the identity verification process has already been completed. • **Rob Haslingden (RH)** Raised a detailed question regarding the verifiability of fraud scores in the ID&V process. • Asked Sandra and Adrian to expand on the role of fraud scores and their authenticity in the context of corporate ID verification. • **SP** Clarified that Cifas does not provide a specific fraud score but supplies data on fraud cases, such as identity abuse or fraudulent applications. • Explained that the provided data is integrated by third-party organisations into their own risk assessments, in line with a handbook that governs how the data should be used (e.g., not automatically declining impersonation victims). • Highlighted that the decision-making process rests with these third parties based on the data they receive. • **AF** Agreed with Sandra's points and added that some fraud scoring mechanisms are defined by frameworks such as the Digital and Technology Future (DATF) framework and GPG 45 standards. • Mentioned that his organisation uses SYNCTICS, a fraud database provider that supplies fraud scores. • Discussed that these fraud scores are now being integrated into processes like One Login, where fraud data points are fed into identity verification processes at Companies House.

	• **Nick Mothershaw (NM**) Expanded on the GPG 45 framework, noting that its scoring model categorises profiles as low, medium, or high risk based on various data points. • Explained that this scoring includes factors like fraud and mortality hits, which contribute to the overall risk score. • Emphasised the need for traceability in fraud scoring—organisations not only want a score but also the evidence behind it to ensure transparency. • **RH** Appreciated the insights and stressed the importance of confidence in the fraud score, especially in corporate ID verification processes. • **Teresa Lam (TL)** Introduced a question from **Penny Dunbabin's** comment regarding the significance of company impersonation compared to individual impersonation in fraud cases. • **SP** Responded that the majority of cases in the National Fraud Database relate to individuals, but company impersonation is also prevalent. Highlighted that out of the 36,000 company cases recorded in the database, a significant number involve company impersonation. • Identified **three common fraud types**: 1. Impersonation of companies. 2. Misuse of company accounts for illicit funds. 3. Fraudulent applications using company identities. • Stated that corporate identity fraud is likely the largest proportion of these cases, though she would need to verify this with more precise statistics.

	• **LI** Thanked Sandra for her contributions and moved the meeting forward to the next agenda item. • Introduced Rob Haslingden to present on the group's proof of concept model, which would be followed by a 35-minute discussion.
Comments	• **Penny Dunbabin (PD)** How significant is impersonation of companies (as opposed to impersonation of individuals)?
Decision:	• N/A
Actions:	• none

Item 3: Company ID Model

Purpose: For discussion

Speaker: RH	**<u>Introduction to the Model</u>** • **RH** thanked the participants and acknowledging the feedback received on the first draft of the proposed model. The model's purpose is to improve the way data is shared with financial services providers to mitigate fraud risks during the SME onboarding process. **<u>Primary Objective</u>** • The fundamental goal is to enhance how data is shared during onboarding, particularly for new limited companies, to reduce the risk of fraudulent activities entering the financial ecosystem. Along with reducing fraud, additional goals include facilitating ease of onboarding, cost savings for banks and SMEs, and faster access to financial services for SMEs. **<u>Process Flow</u>**

	• The onboarding journey begins at Companies House, where companies register. Company directors and Persons with Significant Control (PSCs) go through an identity verification process using Gov UK's one login system. • After registering at Companies House, directors and PSCs will need to verify their identities again as part of the company ID process, which creates a challenge, as identity data from Companies House isn't portable. **<u>The Company ID Pack</u>** • A company ID provider would create a Company ID Pack, which contains **two key components**: 1. Information on who is authorised to sign for the company (directors, PSCs, authorised signatories). 2. Details of the company's business function (trading address, financial performance). • The pack will be created with certified providers and must contain authenticated and verified data. Providers may specialise in either verifying individual identities or compiling business information. **<u>SME Interaction</u>** • Once the data is collected, the SME can review but not directly amend the Company ID Pack to ensure it remains tamper-proof. They can challenge data through the company ID provider, which must verify any changes. **<u>Onboarding with Banks</u>**

	• When an SME applies for a bank account, the bank prompts the SME to share its Company ID Pack. The SME selects their company ID provider, and the bank ingests the pack into its decisioning system to assess risk. • Banks can collect additional data beyond the Company ID Pack, including business information from external sources like Dun & Bradstreet or social media. **<u>Company ID Intermediary</u>** • Introduced the concept of a Company ID Intermediary, which would act as an orchestration layer between banks and multiple company ID providers, helping to streamline the data access process. This role is similar to Account Information Service Providers in open banking.
Comments:	• **AF** DSIT are launching a new trust registry of certified providers - the 'Digital Verification Services' (DVS) register - this should be the marketplace for corporate ID providers, with a new use case of corporate ID for IDPs to certify for (as it is quite different to individual ID&V)
Decision:	• N/A
Actions:	• N/A
Item 4: Open discussion: **Purpose:** For discussion	
Speaker:	• **LI** opened the discussion. Questions included: **1. What specific company director and PSC ID and V data would financial institutions require for SME onboarding compliance,**

	and what are the document requirements for non-director stakeholders? • **Mark Devlin (MD)** Highlighted that banks generally seek a standard set of data for directors, but verification challenges arise, especially with partial data (e.g., month and year of birth, instead of the full date). • Stressed the importance of aligning data sets across institutions. • For non-directors, banks apply similar ID verification standards as for directors. • Suggested that a bad actor can be anywhere in the organisation, so a uniform standard across all stakeholders is ideal. • **LI** Asked for further input on whether varying levels of ID verification (IDV) are necessary for different stakeholders like directors, shareholders, and authorised signatories. • **MD** Reiterated that all individuals, regardless of their role, should undergo the same verification standards to mitigate fraud risks. Differentiating standards could create vulnerabilities. • **Paddy O'Keefe (POK)** Echoed Mark's points, stating that simplifying compliance by maintaining uniform standards across all roles would reduce risks. • **RH** Raised a counterpoint on whether certain stakeholders, such as bookkeepers or accountants, could be authorised by directors without full IDV checks. Acknowledged the complexity this could introduce but stressed it might streamline onboarding in some cases.

	• **Nick Mothershaw (NM)** Pointed out that Companies House ensures directors are verified for their purposes but does not guarantee identity beyond that. • Banks and FIs would still need to conduct separate identity checks to verify that the individual representing the company is genuine. • **RH** Agreed, noting that while it adds friction, the dual verification process offers a higher level of assurance. • **Charlie Boundy (CB)** Supported Nick's explanation, adding that Companies House registers directors but does not validate who acts on behalf of the company downstream. • Emphasised the need for company ID providers to verify authorisation downstream effectively. • **MD Principle Objective:** Focus on making it difficult for bad actors to enter the process. Strong identity verification should not be reduced. • Gathering more information at the initial stage allows for better cross-checking with other data sources like DMV. Matching directors across different entities strengthens verification. • Once a thorough check is done for a client, they should not need to repeat it when dealing with other providers, reducing friction in accessing financial products. • There should be a distinction between onboarding processes for SMEs and larger corporates. Smaller firms may require more stringent checks, whereas large multinationals may not need the same level of scrutiny.

	Question 2 Discussion: RH Raised the question of whether ID documents should include biometric confirmation or digital certification as part of onboarding. • **RH** Feedback from consultations emphasised the need for explainability in whatever methodology is used to authenticate identities. This is critical as different providers use varied methods. • The group was asked to consider if there is a preferred approach to identity verification that should be adopted. • **AF** Highlighted the importance of allowing both electronic and paper-based sources of evidence, as supported by the government's DITF framework. • With the rise of generative AI and deep fakes, digital evidence offers additional security measures. There is a need to move away from relying solely on paper-based evidence. • **RH** Emphasised the need for a set of standards that provides banks with confidence in the methodologies being used, mentioning the potential for regulatory approval. • **Af** added that the UK's Digital Identity Trust Framework (DITF) could give the necessary legislative backing to these standards. • **Geraint Rogers (GR)** raised concerns about verifying the identity of individuals presenting company IDs, specifically around biometric authentication and authorisation checks. • **AF** responded by explaining how various checks, including liveness and impersonation checks, can be used to verify identities alongside document scanning for additional security layers.

	• **RH** summarised the key takeaway that more detailed articulation is needed on data points and tools for validating IDs. The goal is to create a consensus among banks on these standards. • A collaboration between Adrian and Rob was agreed upon to develop these points further, and feedback from banking coalition partners would be sought. • **GR** noted the need to address the relationship between data and its owner, emphasising this as a key principle of the DITF framework. • **Em Hyett (EH)** highlighted the importance of leveraging the UK's existing trust frameworks, like GPG 45, to establish well-understood levels of assurance, particularly in the context of reusable digital identities for SMEs. • **POK** discussed the need for access to ID documents beyond the onboarding process, including during internal investigations or legal orders. • There was a consensus on the importance of reciprocal data sharing, potentially using datasets like those from the City of London Police. • **Julie Dawson** (**JD**) highlighted the risks associated with lost and stolen documents, stressing the need for advanced face matching, document authenticity, and liveness checks. She mentioned the potential for using E-signatures and cryptographic sealing to enhance security. **Question 3: Role of Corporate ID Intermediaries**

	• **LI** Introduced a discussion on whether corporate ID intermediaries and aggregators would help streamline connectivity between company ID providers and banks. • **CR** Asked for clarification on the role of these providers—whether they would help SMEs manage their identities or act as aggregators. • **RH** Clarified that company ID providers would hold verified information in partnership with SMEs, with the potential future addition of wallet functionality. • **AF** Expressed skepticism about adding an additional layer of aggregation, noting that many corporate ID and individual ID providers already adhere to global open standards, allowing easy integration with KYB (Know Your Business) platforms. • Expressed skepticism about the need for an additional intermediary role. Believes the market is already well-served. Sees no clear value added by this additional role. • **SP** Shared a similar view, questioning the necessity of an additional intermediary, particularly if organisations already use external KYB (Know Your Business) providers. • Acknowledged the potential benefit of intermediaries for organisations that handle processes internally. • Highlighted the risk of limiting competition if new providers can't integrate quickly. • Mentioned that intermediaries could help with faster integration for slow-moving organisations and potentially aggregate other external data sources for risk assessment. • Suggested that intermediaries might be redundant if KYB providers already offer these services.

	• **Jay Patel (JP)** Suggested that intermediaries might play a role, particularly in verifying information from corporate ID providers. • Gave a brief overview of Encompass Corp ID's platform, which secures and stores corporate data and documents, allowing banks to request this information securely. • Emphasised the opportunities for multiple firms in this space. • **NM** Agreed with earlier points, particularly around the need for an aggregator if there are multiple corporate ID providers. • Pointed out that without an aggregator, companies would need to repeatedly deal with different providers, creating friction and inefficiency. • Highlighted the importance of reusability for corporate IDs. • **LI** Confirmed that reusability was a key requirement from coalition partners during the discovery survey. • Stressed that the solution needs to accommodate both scenarios: one with multiple ID providers offering complete choice and one with limited choice. • Added that aggregators might be necessary to facilitate choice for SMEs, especially when connecting to multiple providers. • **Louise Beaumont (LB)** Argued that as the market grows in complexity, aggregation will naturally occur to reduce the "neural load" of managing multiple providers. • Believes that aggregation is probable given the value it would generate.

Comments (on chat):	• **AF** For the corporate ID aggregator role - there are already KYB platform vendors that enable FS buyers to plug in different ID&V sources/methods, sometimes as 'no code' flows to suit their process/risk. I'm not sure what a new role would add that we don't already have. KYB platforms compete for FS clients. • **PD** Are you in touch with National Business Crime Solutions? Quite a number of retailers use them for reporting retail fraud, so an individual who has committed fraud may be on their database. • **Charlie Boundy (CB)** To be clear on the Companies House steps, I've fed back to Leon that this looks feasible in principle but needs wider review within CH and DBT… the tricky bit is the handover to an ID Provider • **Matthew Carter (MC)** If fraud can come from anywhere in the organisation, does this mean the value of the 'UBO' data is diminishing? • **To Google Calendar <calendar-notification@google.com>ny Curzon Price (TCP)** Is a DSIT registry the *actual* marketplace, or does it provide the input data for a marketplace? (The OBIE registry is not itself the marketplace for OB apps.) Public bodies often find it hard to do what marketplaces need to do - eg base listing order on market feedback. (Remember all the testing outfits called aaaardvark for Covid travel documents because of alphabetical listing rule) • **Lorraine Salmond (LS) (replying to TCP)** Yes it's a registry rather than a marketplace. • **AF** DSIT have invested quite a bit of money it - we need to see what is delivered. My concern is creating 2 marketplaces, potential data gaps etc… (Replying to **TCP**) OBIE does have a 'regulated providers' list https://www.openbanking.org.uk/regulated-providers/

	• **TCP** yes, but who uses that as the starting place where they choose a provider? • **AF** it depends on how service availability is communicated, where customers are told to look - if there are multiple places and the actual registry is separate, there are gaps for fraudsters to exploit • **TCP** perhaps what this means is that marketplaces need *some* regulation - e.g. on listing requirements - but not the same as registries. Or, if there is a single marketplace, then it should not be run by DSIT which will find it very hard not to get embroiled in JRs on editorial & listing policies • **Dan Standish (DS)** Most banks have in place digital identity document validation services, inclusive of an anti-impersonation check to match the individual to the document. This is the baseline position we need to take, and serves as a huge deterrent. The tricky element for those providers though, is not all solutions are equal. Some solutions will have been deemed not fit for purpose by some firms, therefore relying upon a vendor you know not to be strong poses challenges. • **AF** exactly **Dan –** we layer additional checks on top of this and bank SCA, the bank does the initial ID&V creates multiple layers of security • **DS** Indeed - but if bank B is then to leverage what bank A has completed, and Bank A's ID&V solution is not one that Bank B would have used - should and would Bank B rely upon it and take on that client? • **Renuka** I would mirror what **Paddy** just said - even for ongoing fraud monitoring or where accounts get taken over for example. Doing regular checks to ensure the ID still matches and is right is something we would want to keep on top of.

	• **DS** Last two pennies worth - we should prepare as an industry for 'APP' type scenarios where clients are tricked and coerced into completing ID checks on behalf of criminals • **AF** US & EU are moving to a digital/data first ID model, from wallets with data trails/certifiable sources. UK needs to keep up! • **MD** We educate our customers not to clink on links that take them to external sites, as part of this work we need to ensure that there is a secure and trusted way in. • **David Mcfarlane** If SMEs are paying for the service to create their digital ID pack, which banks then use as a core ID&V component at onboarding.. What happens further down the line if the SME stops paying for the service. Does that instantly render their Digital ID as 'dead' and trigger a process where the bank would have to independently cover all the data previously validated by the ID, so essentially re-onboard the SME? Basically, what happens if the SME stops paying an ID provider? • **TCP** what about aggregators on the SME side of this market? • **MD** I don't see an intermediary being any different to the aggregation approach that in in place today. Adding additional actors may add additional friction in the system. • **Robyn Easton-Fei** Additionally, would need to agree what metadata around the Company ID is shared with the bank by the Provider - e.g. Company ID history including creation, updates, previous uses - to help share a richer view • **TCP** do you need an aggregator market if the standards for CompID are mandated?
Decision:	• **N/A**

Actions	• **Rob Haslingden & Adrian Field** to collaborate on a detailed proposal for ID validation processes and standards. • Feedback from banking coalition partners to be gathered on proposed standards. • Follow-up discussions with Geraint Rogers and others on authorisation and identity ownership concerns.
Item 4: Closing Remarks	
Speaker: LI	• **LI** Summarised the discussion and updates on the coalition's progress. • Highlighted upcoming events, including the next Sprint on October 16th, the delivery phase of the project, and the interim white paper to be published in November. • Mentioned the potential for future guest speakers and the **opportunity for a Coalition Partner to host our Showcase event.** • Asked for organisations interested and that have the requirements to reach out to us.
	• N/A
Decisions	• N/A
Actions	• None

Attendees:

Chair/s: Leon Ifayemi (LI)

Total attendance: 56

Organisation
CFIT
Open Data Consultancy
Bank of England
Cardiff University
Cifas
CoLC/CFIT
Companies House
CTRL- SHFT
Daon
DnB
Dun & Bradstreet
Encompass
Experian
EY
FDATA
GLEIF
HSBC
Innovate UK

Lexis Nexis Risk Solutions
Lloyds Banking Group
Mastercard
Monzo
Nationwide
NatWest
OIX
OneID
Revolut
Sage
Santander
Starling Bank
TechnoXander
The Home Office
Tisa
Tunic Pay
UK Finance
Virgin Money
Visa

Yoti