CFIT | Centre for Finance Innovation and Technology

Fighting Economic Crime Through Digital Verification

The Case for Adopting Digital Company ID in the UK

March 2025

Coalition Members

We would like to offer sincere thanks to our funders at HM Treasury and the City of London Corporation for their counsel and support. They and our multiple industry, academic and regulatory partners have enabled CFIT to deliver our coalitions that drive positive social and economic change across the UK economy. We are grateful to all of our supporters for their cooperation and their creative solutions to the issues that CFIT has effectively addressed. And finally, a note of thanks to the entirety of the CFIT team, for its work to date.

Financial Services

Revolut
NatWest
BARCLAYS
monzo
Santander
OakNorth
HSBC UK
VISA
nationwide
LLOYDS
MONEY
Funding Circle

Tech Companies, Fintechs & ID Providers

Thought Machine
Konfir
GLEIF Enabling global identity Protecting digital trust
PRIVTECH LIMITED
Daon
aperi data
YOTI
Google
mistho.
Datavillage
obconnect WE DELIVER OPEN BANKING
VERIFOXX
NayaOne
Sage
moneyhub
SMART DATA FOUNDRY
TRUELAYER
TECHNOXANDER
one ID
encompass the full picture, fast
LEADING POINT

Public Sector & Regulators

CITY OF LONDON
HM Treasury
PSR Payment Systems Regulator
FCA FINANCIAL CONDUCT AUTHORITY
Home Office

Trade & Membership Bodies

SUPERTECH
FinTech West
fdata europe — Financial Data and Technology Association
TISA
techUK — FOR WHAT COMES NEXT
INNOVATE|FINANCE
fsb — Federation of Small Businesses
pa — the payments association
UK Finance
FinTech Wales

Credit Rating, Reporting & Credit Reference Agencies

CRIF — Together to the next level
experian
TransUnion
EQUIFAX

Data Analytics, Risk Solutions & Fraud Databases

cifas — Fighting Economic Crime Together
ALLOY
sopra steria
tunic PAY
LexisNexis RISK SOLUTIONS
dun & bradstreet
zally
MOODY'S

Academia, Research & Advocacy

LSE
CARDIFF UNIVERSITY — PRIFYSGOL CAERDYDD
CRC Credit Research Centre
THE UNIVERSITY of EDINBURGH
TONY BLAIR INSTITUTE FOR GLOBAL CHANGE
EST 1892 LSBU
ucd — a community interest company
MANCHESTER 1824 — The University of Manchester
University of East London | Centre of FinTech

Professional Services

EY — Shape the future with confidence
OliverWyman
CtrlShift
A&O SHEARMAN

Contents

Foreword

Charlotte Crosswell OBE, Chair, CFIT

Economic crime impacts every individual and business in the UK.

The most immediate and tangible consequence is direct financial loss. Consumers are cheated out of their life savings. Businesses lose their working capital reserves that can be the difference between success and failure. Fraud is the UK's most prevalent crime, and the number of victims is increasing every year. But the financial impacts are also felt more widely. Depending on the nature of the crime, either taxpayers or financial institutions – meaning, by extension, their customers and shareholders – may share in the cost of reimbursement. The leakage of capital into the black market and away from productive, legitimate investment and consumption, affects the UK economy, to the tune of £6.8 billion a year. This undermines ongoing efforts to promote economic growth.

The consequences of economic crime extend beyond increased costs. A loss of trust in the financial ecosystem acts as a brake on growth, deterring consumers and businesses from making purchases and investments. Financial crime affects a market's competitiveness internationally and its ability to attract capital from abroad.

Onerous compliance protocols have become a necessity. For banks, this is a legal and regulatory obligation, but it layers process upon process, swells overheads and may at times contribute to a culture of risk aversion. SMEs (small and medium-sized enterprises), who account for 99% of private sector employers and 50% of the private sector workforce, face a disproportionate share of this increased administrative burden, with cumbersome 'Know Your Business (KYB)' processes driving inefficiency and compounding an already challenging operating environment.

A verified Digital Company ID, in effect a digital passport for businesses, could solve many of these problems in one fell swoop. It shuts bad actors out of the financial system, fosters trust, streamlines operations, eliminates unnecessary red tape, and enables faster financial transactions.

In other words, the prize on offer is not just the reduction in fraud and financial crime – though that alone would make this a worthwhile initiative. It will also make doing business easier, remove friction from the ecosystem and drive economic growth.

Many nations have successfully implemented Digital ID – for both individuals and corporations. Their systems simplify processes, reduce fraud and enhance economic efficiency.

The UK has historically been a leader in financial innovation. The Data (Use and Access) Bill, that is progressing through Parliament, will establish the statutory footing for personal digital verification. The Government is preparing to integrate these digital identity products into processes such as age verification, buying alcohol and property purchases.

But with other markets already leading the way, we must move fast and take the next step now. Falling behind is not an option. Bold action is needed to maintain a competitive position and protect the

UK's reputation as a safe place to do business. That means driving forward the development and adoption of both personal and Digital Company ID.

This represents another crucial stepping-stone on the UK's journey towards a fully integrated digital Smart Data economy. The recent letter from Nikhil Rathi, Chief Executive of the Financial Conduct Authority, setting out how financial regulations can be aligned with the UK's growth agenda, recognised as much – simultaneously calling for action in the field of digital verification and acknowledging the importance of Smart Data schemes.

Policymakers should seize this opportunity for financial innovation. The Government, working in collaboration with industry, regulators and academia, must consider the Blueprint's recommendations and take decisive steps now to shape the next decade.

There is an opportunity to ensure that, ten years from now, we can look back on the far-sighted decisions taken in 2025 to drive forward these new digital verification initiatives, delivering a transformational impact on UK financial policy and economic growth.

Charlotte Crosswell OBE, Chair, CFIT

> “The UK’s leading financial services sector is key to driving growth and putting money in people’s pockets through the Plan for Change. CFIT’s work in countering fraud demonstrates the UK’s position as an innovator within the global financial ecosystem. I look forward to considering the Coalition’s findings as part of our range of work to grow the sector”.

Emma Reynolds MP, Economic Secretary to the Treasury

Executive Summary

Addressing the Growing Threat of Fraud

Fraud infiltrates every corner of our economy, causing immense harm to businesses, destroying lives, and imposing financial losses on an unprecedented scale. Every part of society is a victim of fraud for various reasons including the creation of substantial red tape, driving excessive administrative tasks that hinder firms' abilities to fight fraud. This problem is further exacerbated by a lack of access to verified, authenticated and unified data, which could be resolved by the use of Digital Company ID.

Economic crime has an enormous impact on businesses and individual victims, with fraud accounting for over 40% of all crime across England and Wales[1]. In a 2023 Home Office report, the cost to the economy from fraud was estimated to have reached £6.8 billion per year[2]. UK financial services organisations are also spending £34.2 billion each year on financial crime compliance to tackle fraud related issues[3]. Beyond these numbers, financial institutions face the challenges of meeting necessary regulatory requirements and reputational damage from fraud-related attacks or shortcomings.

Fraud in the UK is growing every year. Criminals exploit gaps in data sharing between financial institutions, allowing them to commit fraud elsewhere after being discovered and offboarded by previous institutions. Whilst emerging technologies including Artificial Intelligence (AI) can help fight fraud, there is an amplified risk that AI and tools such as deepfakes, have made, and will continue to make fraud more sophisticated and scalable.

The ripple effects of fraud extend far beyond monetary loss. High levels of fraud erode social trust, disrupt market efficiency, and damage societal cohesion. SMEs, which often already operate with limited administrative resources and lower brand recognition, face a disproportionate impact from numerous compliance requirements and operational inefficiencies due to their size. Increasing administrative burdens on SMEs and the persistence of fraud slows SME growth by creating significant barriers, including opening bank accounts, accessing finance, onboarding vendors and managing supply chains. This in turn creates frictions which constrain the broader UK economy and its capacity to grow.

Ultimately fraud undermines trust, productivity, and economic resilience. Addressing this threat is critical to safeguarding the UK's financial stability, enabling economic growth, and fostering a more secure, transparent economy.

The Transformative Potential of Digital Company ID

The Centre for Finance, Innovation and Technology led a Coalition of over 70 of the most influential experts in financial crime ranging from global financial services institutions, technology innovators, Government agencies, policymakers and academics, to demonstrate that Digital Company ID, which is a unique digital representation of a business entity for the purpose of digital verification, is a scalable, transformative solution to fighting economic crime. By addressing systemic vulnerabilities, Digital Company ID paves the way for a fairer and more resilient economic system that benefits businesses, consumers, and society and helps foster economic growth.

Our key findings, which are set out below, are backed by both qualitative and quantitative analysis of the onboarding and KYB journey when an SME wishes to open a new bank account, supported by in-depth discussions and data-driven research to determine the economic benefits of Digital Company ID.

To achieve this, over a period of eight months, the Coalition:

- Conducted thirteen coalition-wide workshops, alongside specific workstream meetings, focus groups and in-depth interviews, to define the problem statement and resolve barriers.
- Defined and mapped datasets to create a framework for a reusable Digital Company ID for the bank onboarding and KYB use case, which also focused on secure data sharing between financial services firms.
- Developed a proof of concept (POC) that achieved industry consensus on Digital Company ID architecture and potential solution following registration at Companies House.
- Validated the POC with a representative sample of SMEs and financial institutions.
- Addressed emerging risks by identifying and introducing safeguards to mitigate threats of Digital Company ID misuse by bad actors.
- Created actionable recommendations for industry, Government and regulatory stakeholders.

Key Findings:

- **Fraud is Prevented Through Unified Data Sharing:** Digital Company ID enables seamless, trusted and secure data sharing across firms and sectors. By closing exploitable gaps, disrupting fraud networks, and swiftly identifying and addressing fraudulent activities, it has the potential to directly reduce fraud for both large institutions and SMEs, alongside the indirect impacts of enabling financial institutions to redeploy compliance savings into strengthening anti-fraud efforts.
- **Greater Access to Data Fosters New Products and Economic Growth:** Real time data held securely in the Digital Company ID creates trust and transparency. Further, increased verified data access leads to new products and services being offered both by and for SMEs, resulting in economic growth.
- **Reduces Red Tape and Costs for both SMEs and Financial Institutions:** Digital Company ID reduces regulatory and administrative burdens on businesses, especially SMEs, cutting compliance costs for financial institutions by £1.7 billion annually and generating significant improvements in productivity for businesses. Our POC found the Digital Company ID could deliver the following benefits:
    - Over a 50% drop in the current costs associated with business verification and bank KYB procedures for financial institutions.
    - Over 60% reduction in the time required for verifying and onboarding businesses during bank account openings.
    - 33% improvement in drop-off rates, attributed to the more efficient bank onboarding process.
- **A Robust Governance Framework Empowers the Private Sector to Scale a Digital Company ID:** Establishing governance structures and standards is essential for ensuring interoperability and accountability across sectors. A robust framework empowers the private sector to scale Digital Company ID services nationwide to ensure they meet both commercial and compliance requirements.

Recommendations for Action:

To unlock the full potential of Digital Company ID, the Government, regulators and the financial services industry need to collaborate to put in place the right market and regulatory frameworks and initiatives. Here are seven recommendations proposed by our Coalition:

1. **Develop a Prototype for Digital Company ID:** CFIT, in collaboration with industry, should test and launch a fully functional Digital Company ID prototype preferably with the support of the Financial Conduct Authority (FCA) Innovation services. This will gather user feedback, validate functionality, and ensure regulatory alignment.

2. **Enable Reciprocal and Secure Data Sharing:** The Government must consider mandating all relevant organisations across the Financial ecosystem to share data on economic crime. This could be achieved in part via a Digital Company ID. In addition, industry should work with the Government to understand the different models for sharing that data, including who provides the permission to share the data.

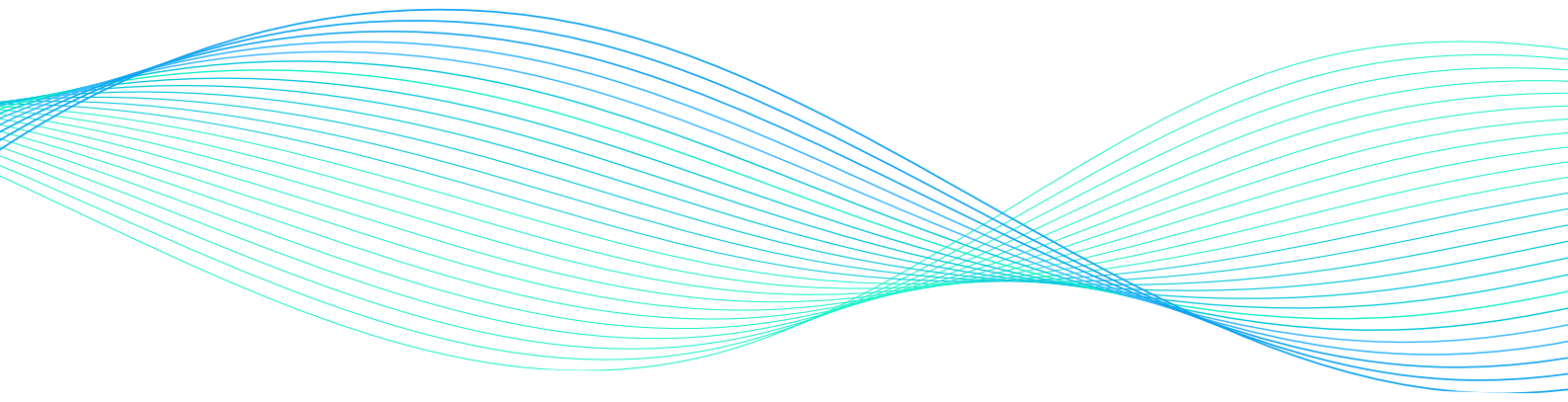
3. **Appoint a Lead Authority:** To address market coordination failures, the Government should consider appointing a lead authority to oversee the accreditation and governance of Digital Company ID. Industry, with the support of CFIT, should drive forward implementation and scaling, ensuring the future lead authority stays informed as necessary.

4. **Promote Standards for Interoperability:** CFIT is committed to collaborating with industry to establish standards that ensure domestic and international interoperability, accountability, and secure adoption of Digital Company ID. These standards will reduce compliance costs and foster trust across sectors. Further, these standards should take into consideration the work already significantly underway regarding personal digital identities.

5. **Create a Multi-Stakeholder Taskforce:** Establish a taskforce to identify, prioritise, and develop high-value use cases for Digital Company ID within financial services. This includes tackling deceptive practices in areas such as supply chain validation and fraud prevention in public procurement.

6. **Review the Regulatory Framework:** Policymakers, working closely with industry, must review the regulatory framework for Digital Company ID, ensuring it is fit for purpose in order for firms to rely on Digital Company ID from a regulatory perspective. This review should focus on addressing gaps and ensuring alignment with evolving market needs.

7. **Drive Market Confidence Through Government Adoption:** Government departments must lead by example, adopting Digital Company ID for critical interactions such as procurement, confirmation statement filings and tax filings, aligning to the Government's vision for Making Tax Digital. This will help create support for private sector investment and build trust in the system.



Conclusion

Fraud continues to pose a significant and evolving threat to the UK economy, undermining trust, financial stability, and economic growth. However, by embracing Digital Company ID, we have a practical and effective solution that can strengthen our financial ecosystem, enhance regulatory compliance, encourage innovation, and drive greater transparency across sectors.

The implementation of Digital Company ID offers a crucial opportunity to address longstanding vulnerabilities in business verification and fraud. By establishing a standardised, interoperable, and trusted system, businesses, financial institutions, and policymakers can streamline processes, reduce friction in onboarding, and remove the loopholes that bad actors exploit.

Crucially, this initiative aligns with the Government's broader strategy for economic growth, as outlined in the Department for Science, Innovation and Technology's (DSIT) Blueprint for Modern Digital Government and the commitment to a Smart Data economy, as evidenced by the Data (Use and Access) Bill. This Bill will help put in place the building blocks to unlock the potentially transformative benefits that Digital Company ID can offer. Furthermore, it supports the UK's ambitions to lead in digital innovation, unlocking private sector investment, fostering a more competitive and inclusive business environment, and ensuring that the financial sector remains resilient in an increasingly digital world.

Our blueprint lays out a clear, actionable path for policymakers and industry leaders to drive this transformation. By implementing these recommendations, we can not only mitigate fraud but also unlock efficiency and productivity, reduce compliance costs, and create a more secure and prosperous economic landscape for businesses of all sizes.

Now is the time to act.

"The coalition has offered a viable means for Smart Data to be used in the battle against fraudulent bad actors. The coalition's recommendations will be reviewed by the Government, which includes the potential for a Digital Company ID solution to be deployed across our economic ecosystem, which will help provide a strong foundation for better data sharing."

Agnieszka Scott, Head of Smart Data, Department for Business and Trade

"Financial crime harms consumers, costs businesses and impedes economic growth. That's why fighting it is a priority for the FCA.

Fraud is continuously evolving, so we welcome innovations, including developments such as Digital Company ID, which can help combat it.

We look forward to continuing to work closely with CFIT and industry."

Steve Smart, Joint Executive Director of Enforcement and Market Oversight, FCA

"We are encouraged by the Centre for Finance, Innovation and Technology (CFIT)'s second Coalition that is aimed at diminishing the scourge of economic crime. This impacts negatively on businesses and consumers alike, damaging trade and ultimately UK economic growth. The suggested counter measure, found in the widespread usage of Digital Company ID, will hamper the efforts of fraudsters, enable businesses to trade securely, and lessen the bureaucracy that they encounter on a daily basis. Digital Company ID is key to unlocking the potential of a Smart Data economy, and the City Corporation's commitment to advance these innovative initiatives is clear through support for CFIT as a co-founder alongside HM Treasury, but also active participation in this Coalition. I congratulate CFIT's Coalition on its hard work, dedication, and effort in advancing this important work."

Chris Hayward, Policy Chairman, City of London Corporation

Chapter 1

The Changing Face of Fraud in the UK

In 2023, over 1.2 million acts of fraud were committed in the UK, equivalent to nearly two fraudulent acts every minute and costing individuals £5.4 billion[4]. This excludes fraud offences that are not reported to the police or Action Fraud. According to a report published by the Home Office in 2023, the overall estimated direct cost of fraud to the UK was £6.8 billion[5] per year.

Excluding the local peak in fraud due to Covid, financial fraud appears to be growing steadily[6]. In the first half of 2024, an increase of 15% of cases was filed to the National Fraud Database. Whilst Artificial Intelligence (AI) can help fight fraud, advances in AI are also expected to accelerate fraud unless decisive action is taken. We are supportive of a regulatory framework that addresses these risks whilst supporting innovation as recommended in the Government's AI Opportunities Action Plan. Financial loss is only part of the broader societal cost of fraud. Significant resources are devoted to preventing, prosecuting, and assisting victims of fraud. In 2022/23, the financial sector spent an estimated £34.2 billion on regulatory compliance[7], much of it aimed at combating financial fraud. Despite these efforts, fraud that occurs within the financial sector undermines trust in institutions and impacts UK economic growth.

Fraud is constantly evolving. According to Action Fraud, it was estimated that at least 86% of fraud reported nationally is now cyber-enabled[8]. Most fraudulent activities will be amplified by digital tools powered by emerging technologies. In recent years, bad actors have been adopting advanced tools to increase their scale of operation, penetration, and sophistication. For example, scammers can use AI to fabricate high-quality fake identities and documents to gain financial advantage or use deepfake technology to set up video and voice calls and initiate money transfers. In fact, identity fraud is one of the most common case types filed to the Cifas National Fraud Database and accounted for 64% of all filings in 2023[9].

Fraud generates negative economic sentiments by raising risk perceptions across the economy. This affects business activity and damages the reputation of entire trading markets. The impact of fraud also extends beyond the real economy. It also undermines social cohesion. High-trust societies are often associated with numerous socially beneficial outcomes, such as stronger support for wealth redistribution and welfare policies. The widespread presence of fraud undermines these qualities, weakening societal structures.

Anti-fraud measures, especially those that use identity-based solutions, can improve trust, transparency, and market functioning and reduce economic crime. The economic benefits of improved market functioning, driven by more trustworthy data about participants, have been estimated to add between £3 billion and £25 billion annually to GDP[10]. Evidence suggests that high-trust societies tend to have greater market efficiency because they enjoy lower transactions costs[11]. While much of this is not directly related to legally defined fraud, any reduction in fraudulent activity contributes to these positive outcomes.

> "Digital Company ID reduces friction at onboarding. Up to an astounding 150 questions are asked to businesses opening a new bank account. Reducing these touchpoints means banking customers can access facilities quicker and easier. Improving the customer journey without compromising anti-money laundering procedures is vital for a successful, thriving business. Digital Company ID supports a trusted ecosystem where increased data sharing would help combat fraud and foster economic growth."

Grant MacDonald, Director – Fraud and AML Strategic Initiatives, Experian

> "Digital Company ID addresses the growing challenge of fraud by ensuring reliable, real-time data for risk decision-making. This innovation will significantly improve efficiency of risk decisioning and build trust in businesses and financial institutions alike. It is a critical tool in preventing bad actors from entering the system. By adopting Digital Company ID and seeing Government leading by example as a first user of Digital Company ID for specific use cases, we stand to strengthen the foundation of our economy by promoting trust and transparency and in turn help drive economic growth."

Nina Kerkez MBA CAMS, Senior Director, Market Planning, Platforms, LexisNexis Risk Solutions

> "We welcome the coalition's work and recommendations. Digital Company ID will help protect UK Financial Services businesses from financial fraud and economic crime. Dun & Bradstreet can support the Digital Company ID, providing live business identity data to help businesses avoid potentially fraudulent situations."

Edgar Randall, Managing Director, Dun & Bradstreet UK

Chapter 2

Preventing Fraud with Digital Company ID

Effective fraud control relies on the timely identification of bad actors, either before a fraud is committed or as rapidly as possible after to limit the extent of repetitions. To enable a systematic approach to combat fraud, Digital Company ID is necessary to improve the accuracy of identification, facilitate high quality information sharing, enable timely fraud intervention, and empower existing fraud intelligence networks.

The increasing digitisation of administrative processes has allowed the proliferation of companies engaged in fraudulent activities, and at the same time made identification harder. This is exacerbated by the digital proliferation of inconsistent, poor quality, lightly checked and out-of-date information about companies, helping them to hide for long enough to commit fraud.

Let us use the following example on push payment fraud to explain a current, and future Digital Company ID enabled scenario. Today, the transaction might be blocked by the internal systems of one payment service provider and reported to counter-fraud intelligence networks like Cifas or other fraud databases. Further investigation would then be carried out on the fraud case as a single, independent event.

With Digital Company ID, better fraud intelligence and analysis could be enabled, including examining the linkages of this fraudulent company with other individuals (directors, shareholders and named employees as contained in the Digital Company ID), related entities, physical addresses, websites and telephone numbers. Real-time intelligence sharing of these connected parties, under lawful basis, could be used to place fraud risk markers onto the accounts of the same entity at other payment service providers, or of different but related entities throughout the financial system.

In this push payment fraud example, the use of Digital Company ID, coupled with real-time intelligence and fraud alert systems, could create an extensive data sharing network in the financial system. This contributes to a critical piece of counter-fraud infrastructure because better intelligence is at the heart of it. Sharing markers of fraud risk requires a consistent identifier and exchange of high-quality and standardised data. Both could be achieved effectively through Digital Company ID, while minimising the risk of false positive identifications which could result in damaging legitimate businesses[12].

Our work within the Coalition has revealed limited analytical research on fraud and counter-fraud initiatives, both in the UK and internationally, restricting the ability to conduct quantitative modelling on the impact of Digital Company ID. The absence of detailed, consistent, and up-to-date fraud data in the UK hinders a systematic approach to fraud prevention and the development of effective, system-wide countermeasures.

By integrating verified and standardised company data with real-time fraud intelligence, Digital Company ID strengthens fraud detection, disrupts fraudulent networks, and enhances regulatory compliance. This creates a trusted mechanism for businesses and financial institutions to verify company identities and their authorised representatives. The next section explores what Digital Company ID is, how it works, and the essential components that make it a transformative innovation.

Chapter 3

What is Digital Company ID?

Digital Company ID is a unique digital representation of a business entity for the purpose of digital verification. It enables the integration of verified and trusted information about a company, including their registration documents, company credentials, business activities and financial records, and proves that the company is "real".

These verified data points and credentials can only be changed at the source - not within the Digital Company ID. Depending on the use case, the Digital Company ID can also contain other information about the business, like their suppliers, trading partners, and credit profiles. It enables a company to prove their identity for various business activities without presenting physical documents.

To enable efficient and seamless use, Digital Company ID is linked to validation of the people authorised to represent the company. This linkage can be achieved through the use of a Digital Identity Service Provider, certified under the UK digital identity and attributes trust framework (UKDIATF), both at the point of creation of Digital Company ID and when a transaction is being requested by an authorised company representative.

To maximise its impact on economic crime, Digital Company ID needs to be constantly updated which requires it to be regularly used by the company. To achieve this, Digital Company ID needs to be secure, reusable, scalable and adaptable to many use cases within and beyond the financial services sector.

Digital Company ID consists of three key components:

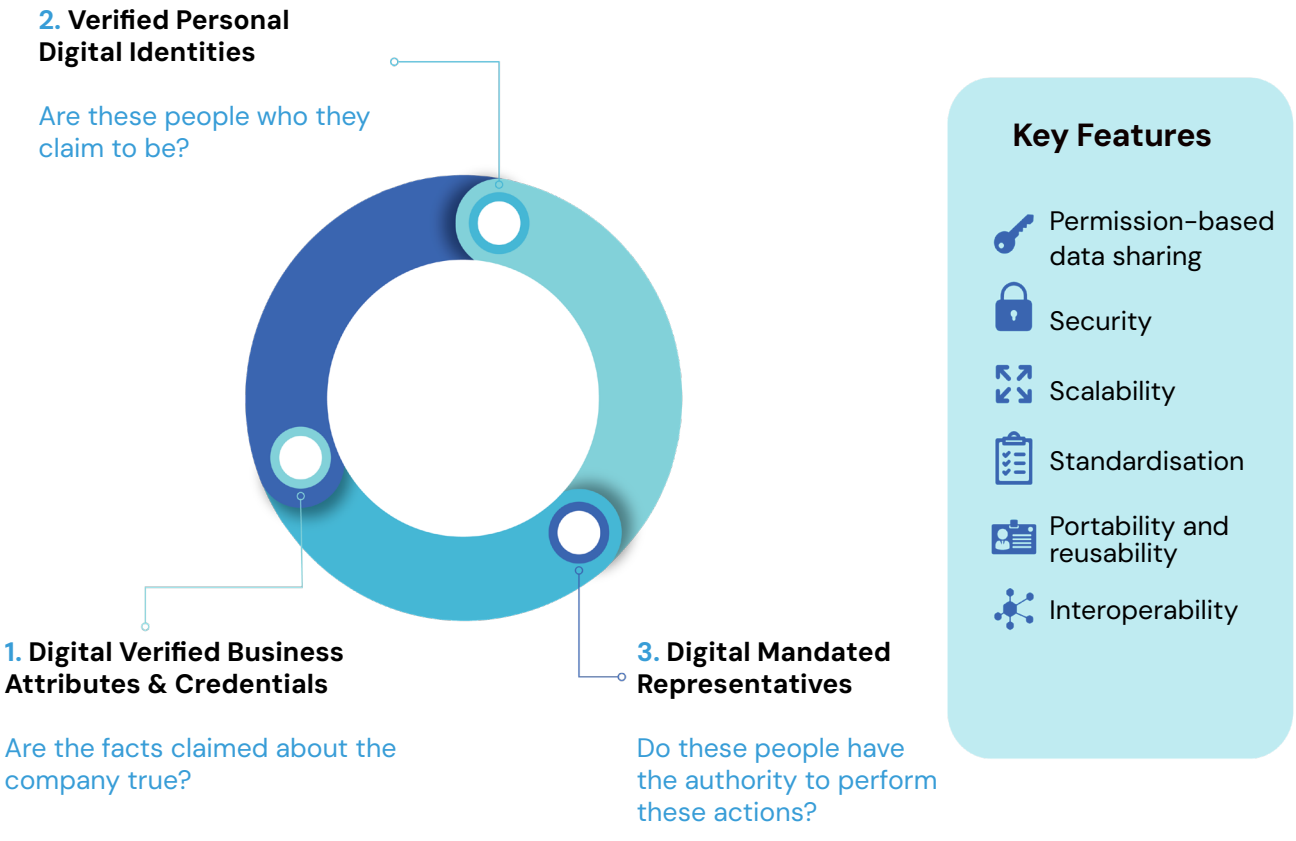


Figure 1: The 3 components of a Digital Company ID

Component 1: Digital Verified Business Attributes and Credentials

Purpose: Are the facts claimed about the company true?

- These are the foundations of Digital Company ID. They refer to specific and verified facts known as "verified attributes" about a company, together they act as a baseline for business verification. These verified attributes should be provided in the form of standardised and machine-readable data, enabling automation in a process.
- Examples of verified attributes may include company registration number verified by Companies House, or VAT registration number and tax status verified by HMRC.
- Companies may also add additional self-attested data to supplement their Digital Company ID, for different use cases.

Component 2: Verified Personal Digital Identity

Purpose: Are these people who they claim to be?

- These are verified personal digital identities for directors, shareholders and those individuals acting on behalf of the company. Verified personal digital identities are created and maintained in a similar way to Digital Company ID: they are a set of verified personal information and attributes.

Component 3: Digital Mandate

Purpose: Do these people have the authority to perform these actions?

- A digital credential that represents the authority and context to which an individual or a related entity has a mandate to act on behalf of a company, e.g. able to authorise a payment. These credentials can only be created, amended and verified by the company.
- Used in conjunction with the above digital verified business attributes and credentials, users can rely on Digital Company ID to effectively verify 1) the individual's identity and 2) whether the said individual has the delegated authority to perform certain actions on behalf of the organisation, such as requesting and approving transactions, filing tax returns, and signing commercial contracts.

Real-life Applications of Digital Company ID

Any improvement in fraud prevention through the implementation of a robust and well-functioning Digital Company ID will have far-reaching positive effects across the broader economy, liberating productive resources through increased efficiencies, and enabling reassignment to growth activities. Digital Company ID enables seamless access to financial services and credit where financial institutions can quickly verify a company's credentials, making it easier to secure loans, credit lines, or investment funding. It also enhances trust and credibility with customers, investors, and business partners. This can be particularly valuable for e-commerce, international trade, or companies expanding into new markets.

Here are some examples of real-life applications:

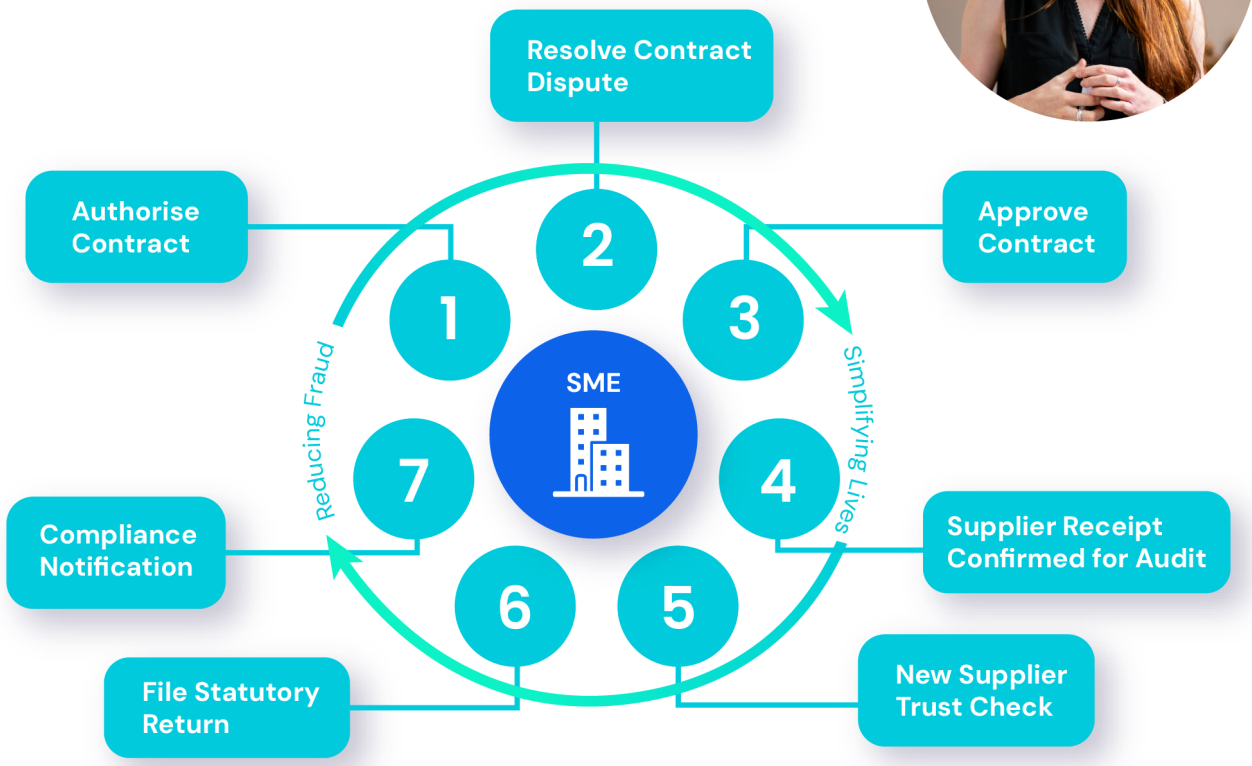
- An SME who is purchasing from another SME for the first time might routinely use a "trust-check" service based on Digital Company ID to validate their suppliers, similar to how they might perform a credit check.
- An individual customer who is purchasing goods from an online marketplace for the first time may want additional assurance by requesting a retailer verification, facilitated by Digital Company ID.
- A payment service provider may leverage Digital Company ID to automatically run identity checks in the background before processing a high-value or unusual transaction. This would enable timely notifications on potential scams, such as impersonation fraud, and alert the payer to stay vigilant without overwhelming them with too much complex information.
- A financial institution may apply Digital Company ID to their ongoing monitoring of account activities. For example, Digital Company ID will enable automated flags and triggers if there are key changes to the business nature, company ownership or risk profile, ensuring timely reviews of customer profiles. This can prevent bad actors from using fake or shell companies to exploit services, secure loans, or engage in other fraudulent activities. It will also facilitate better assessment of anti-money laundering (AML) risk by identifying and verifying the ultimate beneficial owner of the business.

On the next two pages, we will demonstrate how an SME Director and a Bank Manager can use Digital Company ID to support their daily operations. The first case study below serves to illustrate the seamless use of Digital Company ID across multiple operational activities which have been compressed into one day of Sophie's work life, who is the COO and Director of an SME. It demonstrates how Digital Company ID could be integrated into the business to prevent fraud, streamline operations, improve transparency and maintain compliance. Digital Company ID allows Sophie to focus her available resources on strategic leadership, having the confidence that the business is dealing with legitimate counterparts.

The case study also highlights the variety of activities where Digital Company ID can create value for users. High levels of trust are needed to carry higher levels of risk such as those illustrated in Activities 1, 2, 3, and 5 in Figure 2 below. These require the support of a clearly defined liability framework to provide users with the necessary protection and confidence. Whereas Activities 4, 6, and 7 involve far less, though not zero, risk. Their value lies more in convenience. These lower risk activities support more specialised Digital Company ID providers. Together, this further points to a market-shaping approach enabling an ecosystem of Digital Company ID providers, each addressing specific use cases. Some will naturally be delivered by larger organisations, while others may be better suited to market specialists.

Digital Company ID

A Day in the Life of Sophie: SME COO & Director



1	Authorise a Contract	The director logs into the company portal using their verified personal digital identity, prioritising tasks and authorising a flagged supplier contract.
2	Resolve Contract Dispute	At the office, they host a secure video meeting authenticated via their Digital Company ID, discussing sensitive documents and resolving a contract dispute.
3	Approve Contract	Using their Digital Company ID and verified personal digital identity, the director reviews and approves the contract, which is securely logged for compliance.
4	Supplier Receipt Confirmed for Audit	A notification confirms the supplier's receipt of contract, automatically recorded for audit. The director updates the CFO securely via messaging.
5	New Supplier Trust Check	Perform a 'Trust Check' with a certified Digital Company ID provider on a new supplier before paying their invoice.
6	File Statutory Return	The director files a statutory return via a Government portal, verified and logged by their company and verified personal digital identities.
7	Compliance Notification	Compliance notifications confirm secure logging of the day's activities, ensuring regulatory adherence and enabling focus on leadership.

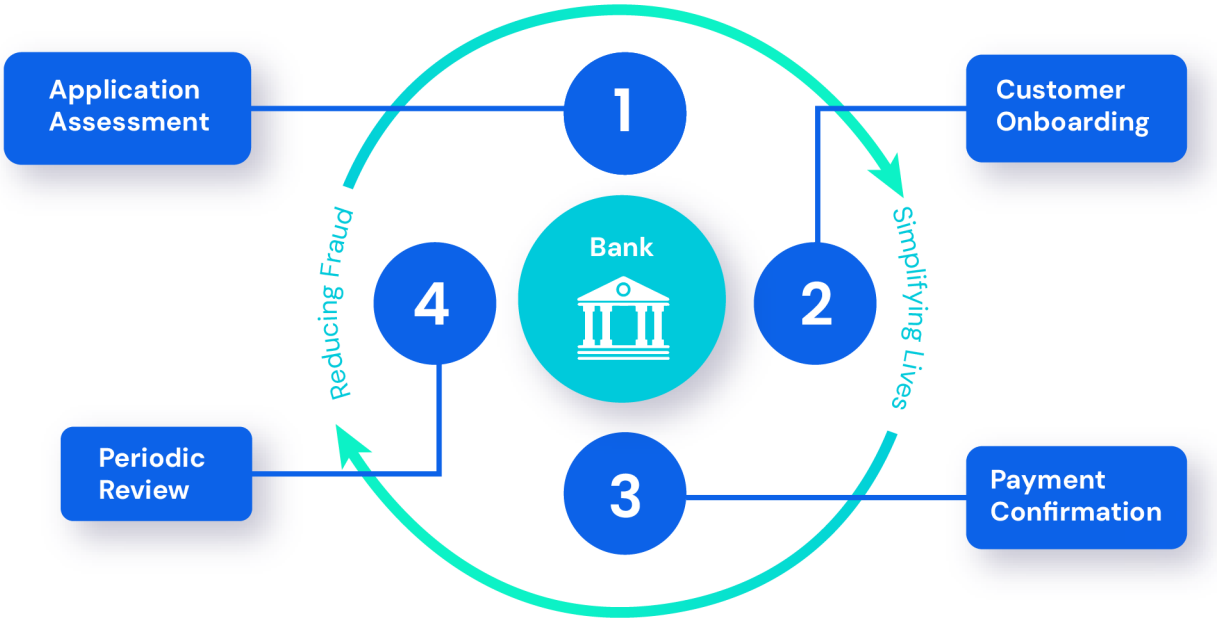
Figure 2: A Day in the Life of Sophie, SME COO and Director

To gain sight of the breadth of these opportunities, we recommend that industry takes the lead and develop other priority use cases beyond onboarding and KYB compliance processes. Digital Company ID will promote trust and transform the way SMEs interact with their counterparts, including their suppliers, business partners and customers. By identifying market opportunities and propositions that could deliver the most value for SMEs, the market can improve their operational efficiency and support their growth.

The second case study of a business bank account manager, Figure 3, serves to illustrate how Digital Company ID can be used in different daily scenarios in a bank to better protect customers and strengthen fraud detection. Digital Company ID provides the vital means to enhance ongoing monitoring. It enables banks to effectively validate the identities and business profiles of their customers, reconcile outdated information and investigate suspicious activities, supporting them to deliver better services and outcomes. Digital Company ID also provides a holistic picture of the business, its usual trading patterns, and supplies key insights for detecting and preventing fraud on an ongoing basis.

Digital Company ID

A Day in the Life of David: Bank Account Manager



1	Application Assessment	The bank reviews a business's Digital Company ID and cross-references it with trusted databases to confirm registration details, authorised representatives and risk profiles.
2	Customer Onboarding	Using a Digital Company ID, David approves the application, onboards the business, and works with monitoring teams to set account parameters based on the business's risk profile.
3	Payment Confirmation	The transaction monitoring team flags a high-value payment and uses Digital Company ID to verify the payee, transaction purpose, and the authorising director.
4	Periodic Review	During a routine review, the bank is notified that XYZ Ltd's business profile has changed. After verification, the Digital Company ID provider updates the bank, ensuring accurate and trusted information across the network.

Figure 3: A Day in the Life of David, Bank Account Manager

> “The coalition has proven that digitising how banks undertake know your customer obligations will help make compliance checks more user friendly for Britain’s small businesses and support the UK’s fight against financial crime. Delivering easier and quicker access to bank accounts and finance will also enable businesses to secure greater investment for growth and deliver more jobs for people across the UK.”

Elyn Corfield, CEO, Business & Commercial Banking, Lloyds Banking Group

> “Driving innovation and supporting initiatives that make life easier for SMEs is in our DNA – so we’re incredibly excited to be at the forefront of delivering a Digital Company ID solution. This will enable quicker access to financial services for legitimate businesses and ensure that key business information lives in one place. This will also make it harder for fraudsters to set up fake companies and ultimately help prevent people falling victim to fraud.”

Jordan Shwide, General Manager, Monzo Business

> “Financial crime is one of the most pressing crimes in the UK, which is why cross industry collaboration is vital to protect consumers, businesses and the overall economy. The proposed Digital Company ID highlights the role technology plays in protecting the financial system and customers, whilst supporting UK economic growth.”

Phalé McMillan, Head of Financial Crime Risk Management/Deputy Group MLRO, NatWest Group

Chapter 4

Our Proof of Concept

The Coalition chose a proof of concept (POC) to demonstrate Digital Company ID and its potential value in a single use case. The POC is a first step in helping define the data requirements, test the concept and its value with potential users, and identify areas of focus for further development.

Having identified various use cases to combat fraud, the Coalition chose a POC focused on using Digital Company ID to prevent bad actors from entering the financial system when opening new bank accounts. Since a bank account conveys trust and legitimacy, restricting fraudulent access has the potential to significantly impact the fraud landscape.

With the emergence of AI image generation and voice manipulation, there is a pressing need for better solutions to effectively detect and prevent fraud at the point of onboarding. In addition, by integrating Digital Company ID into the financial system, good actors such as genuine businesses are better supported through streamlined processes and enhanced trust and transparency.

A well-designed Digital Company ID will also take a lot of the cost and friction out of this onboarding process. For instance, businesses are being asked up to an astounding 150 questions when opening a new bank account, which forms a part of the KYB compliance process. Digital Company ID can incorporate a significant amount of this data along with its verification and offers the opportunity to automate all or part of this costly information exchange. This will reduce the load on businesses, improve the user experience and make the banking process more efficient.

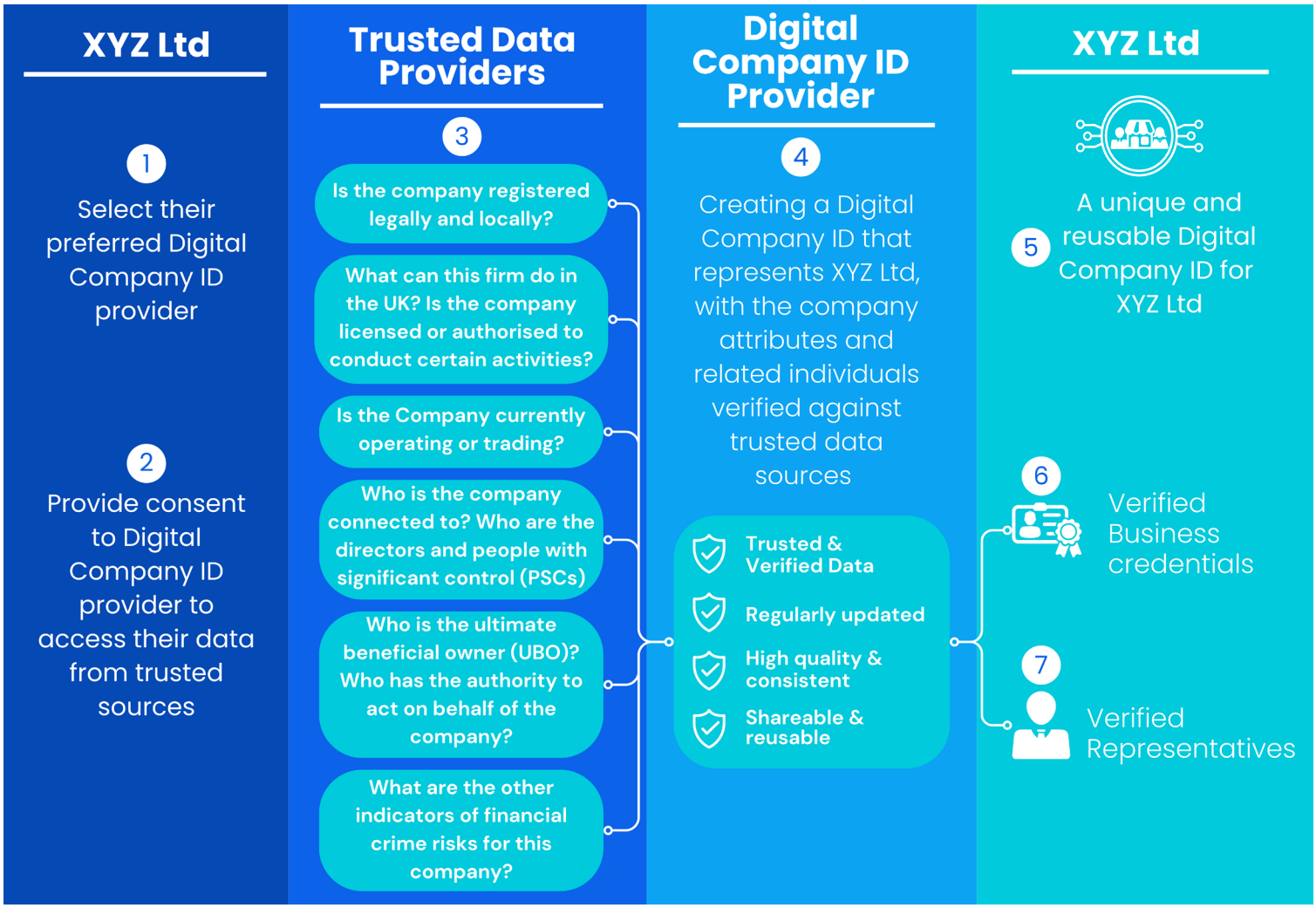


Figure 4: Use of Digital Company ID in opening a bank account

This diagram illustrates the journey of a small business, XYZ Ltd, in creating their Digital Company ID.

1. XYZ Ltd chooses their preferred Digital Company ID provider.

2. XYZ Ltd provides consent for the Digital Company ID provider to establish its digital profile.

3. The Digital Company ID provider then gathers information directly from trusted data sources to ensure their validity and credibility.

4. Once the business attributes and related individuals of XYZ Ltd have been verified by the Digital Company ID provider, it can issue time-stamped digital certificates, like verification badges, to the business and its representatives. These digital certificates are created to a common standard and are regularly updated by the Digital Company ID provider. They are shareable and reusable.

5. XYZ Ltd can now use their unique and reusable Digital Company ID to interact with financial institutions, business partners and their customers.

6. For example, XYZ Ltd can apply and reuse the digital certificates individually or combined whenever required to prove their verified business credentials, e.g. their business license.

7. XYZ Ltd can also reuse the digital certificates that are issued to verified company representatives in daily operations, e.g. COO who can sign contracts on behalf of the company.

In developing the POC, the Coalition focused on the context within which Digital Company ID would be used, set clear objectives which guided the development and testing of the POC and supported strong results to further guide the development of Digital Company ID.

The POC context:

Led by our three POC partners, Lloyds, Monzo and NatWest, the POC has been designed to seamlessly integrate into the customer journey and workflow, starting with the formation of a new company at Companies House. It incorporates the creation of Digital Company ID using trusted data, which is then utilised in the POC partners' bank onboarding process.

CFIT's POC objectives:

- Understand the challenges in order to find solutions and provide recommendations to stakeholders including policymakers.
- Evaluate whether Digital Company ID can create efficiencies and reduce friction in the bank onboarding process.
- Assess whether Digital Company ID can sufficiently address all but complex cases of KYB compliance process for bank account onboarding.
- Determine if the quality of the current in-house solutions can be improved by ensuring that information is dynamically updated through trusted sources.
- Demonstrate a user experience flow that will deliver lower drop-out rates.
- Evaluate the growth potential of Digital Company ID in broader application.

What the Coalition did:

The Coalition built a prototype journey for a SME, featuring key steps in the creation of Digital Company ID, its interaction with personal digital ID, and its application at the bank account opening process.

The prototype journey demonstrates:

- How secure integration of trusted and verified data through Digital Company ID can support better business verification and therefore reduce fraud.
- That Digital Company ID presents a comprehensive picture of the business, including its related individuals and key company attributes.

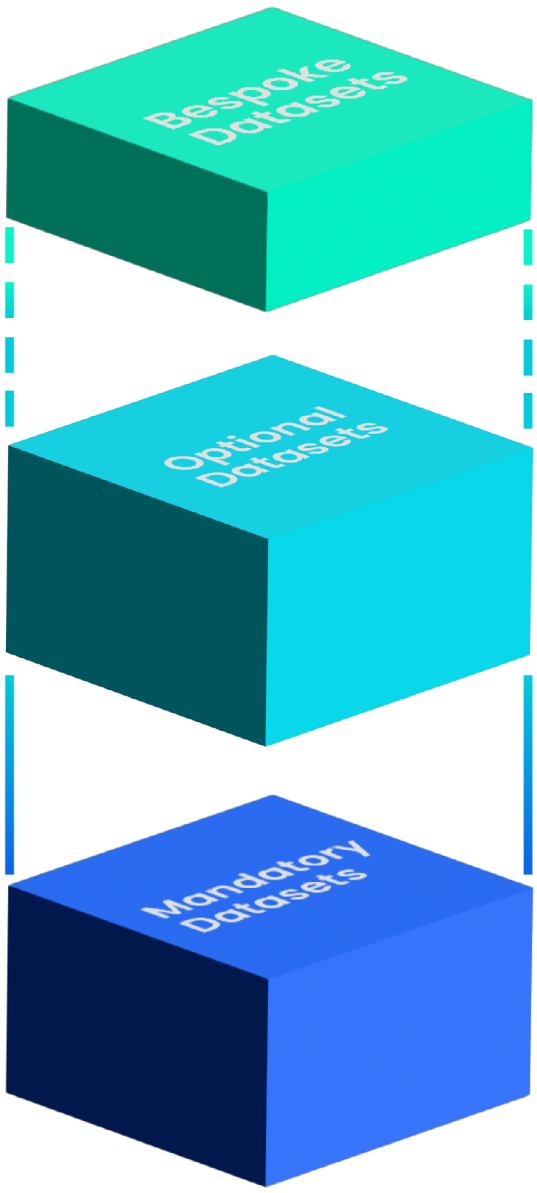
The results:

The POC enabled the Coalition to:

- Estimate that, by integrating the Digital Company ID POC into the banks' existing onboarding process, around 50% of KYB compliance processes and verification costs could be eliminated, drop-out rates could be reduced by 33% and onboarding verification could be sped up by over 60%.
- Reach a consensus on the core data elements required for a useful Digital Company ID in the financial sector; this is sufficient for onboarding and includes official and self-reported sources, consented and non-consented attributes.
- Reach an alignment that the Digital Company ID model could be used either with Digital Company ID aggregators collecting and maintaining the data records, or via a digital wallet held by the SME.
- Reach an agreement that the SME must be provided with a measure of control over how its data is being shared, and who has access to this information. The data shared must be proportionate to the risk and requirements of the use case.
- Explore key enablers for Digital Company ID, including the need for scalability and interoperability across use cases and sectors. The Coalition agreed that consistent standards should be in place to allow for data portability of the Digital Company ID between SMEs, certified ID providers and third parties.
- Identify best practice and assess the opportunities for leveraging existing established identity trust and governance framework in the UK and Europe to ensure alignment.

Critically the development of the POC also enabled the identification of the Digital Company ID Data Stack in Figure 5 below which illustrates the mandatory, optional, and bespoke datasets. This enables further testing of the viability of the Company Digital ID, and the data sets available, and lays the foundation for identification of data partners for the development of a Digital Company ID designed for onboarding purposes.

Digital Company ID Data Stack:



Bespoke Datasets

Example of reciprocal and secure data sharing:

Cifas – fraud risk data
City of London Police – fraud risk data and offloaded accounts
NCA – fraud and AML confirmed database
Others – sanctions and watch list checks, adverse media checks, etc.

Optional Datasets for SMEs

Example of data input:

HMRC – tax status
Registers for Authorisation, Licenses, and Certifications – business licenses and regulated activities
Open Banking – transaction records
Open Finance – loans, mortgages, insurance, pension data, etc.
Cloud Accounting Companies – financial and accounting information
Home Office - criminal records
LEI Database

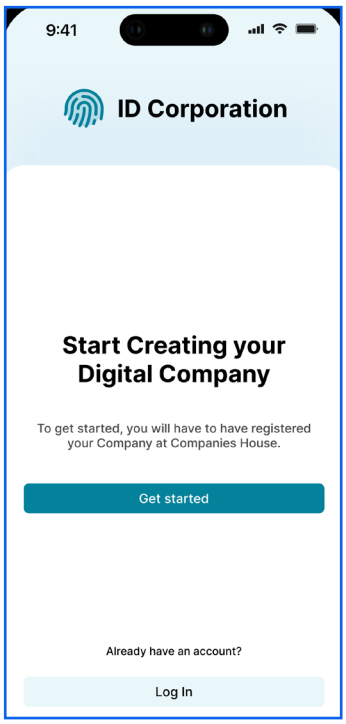
Mandatory Datasets

Example of data input:

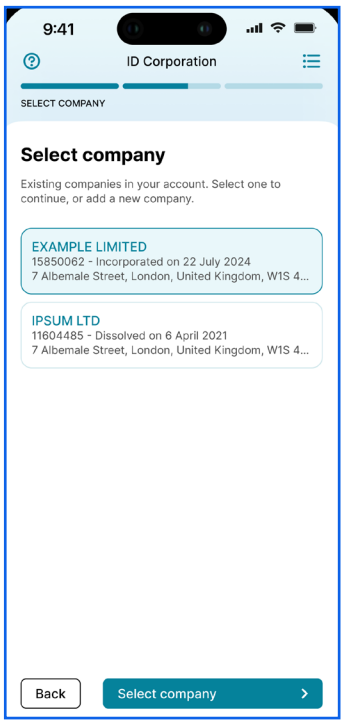
Companies House – company registration
Credit Reference Agencies – credit scores
Personal ID&V data – identity verification for related individuals
Social Media and E-commerce Platforms – online business presence

Figure 5: The Digital Company ID Data Stack

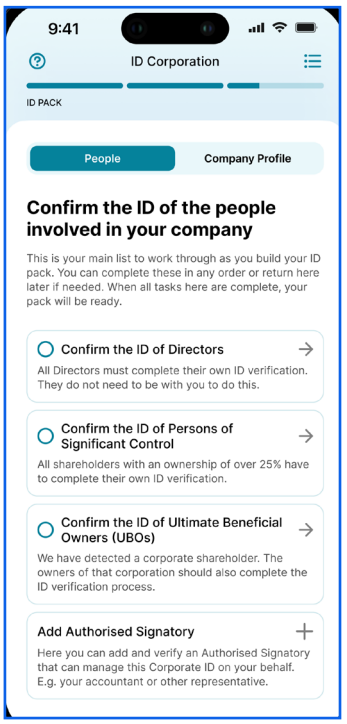
The Coalition's POC takes the user through the process of creating a Digital Company ID, accessing the data required for set up, integrating these data from trusted sources to form a single view, and showing its application in the bank onboarding journey, see sample screens below.



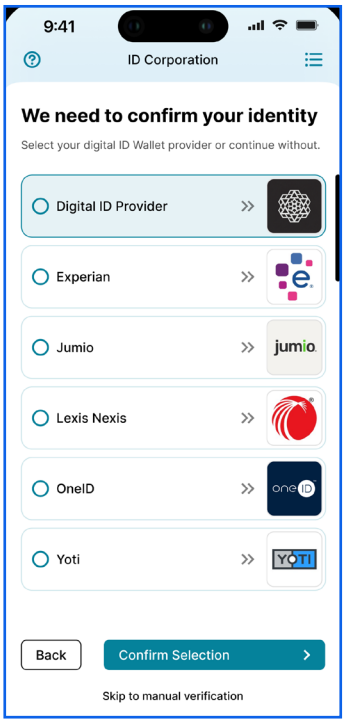
Digital Company ID providers will help SMEs create a reusable and sharable Digital Company ID.



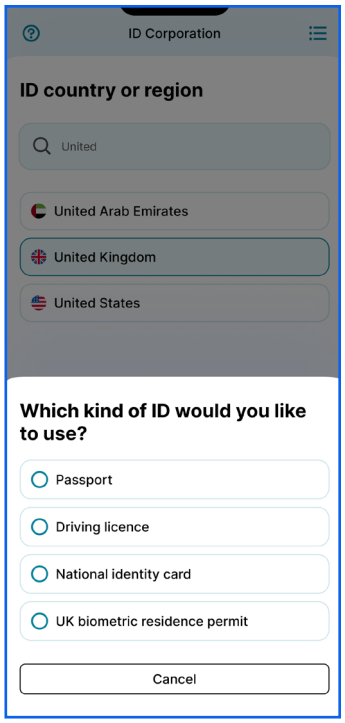
Start by confirming the name, location and purpose of the business by automatically linking information from Companies House registration to the Digital Company ID.



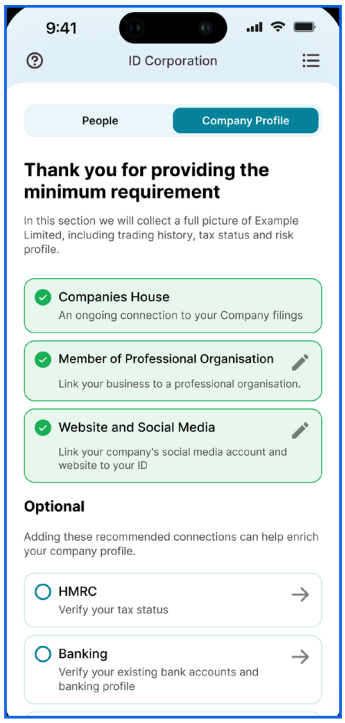
Confirm the identities of the Directors, Persons of Significant Control (PSCs) and Ultimate Beneficial Owners (UBOs)



Share identity information from an existing personal identity wallet

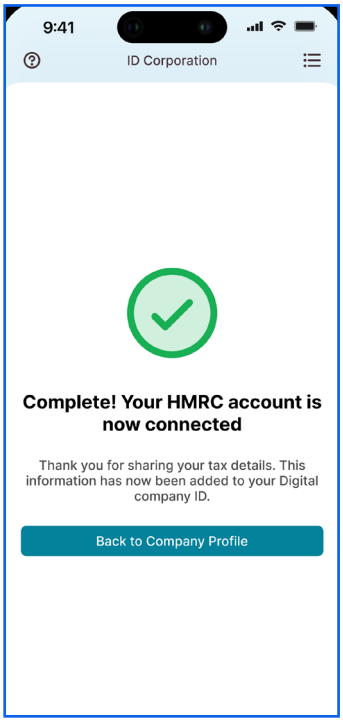


Or confirm the identity using photo ID and biometric verification

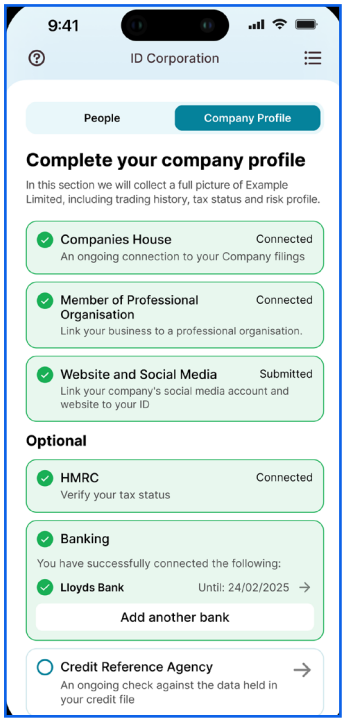


Confirm the business credentials using data from Companies House, public registers, website or other relevant sources

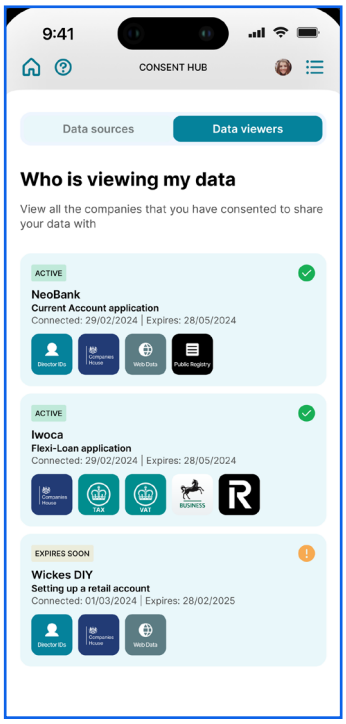
To verify tax status, link the company's HMRC account to Digital Company ID



Once connected, Digital Company ID can be used to maintain tax records



Add credit score, bank transaction data and other useful information to enrich the company profile, which can be used to obtain financial services



Manage permissions on data shared including the parties who are connected to the Digital Company ID and the dates when the connection goes live / expires

Figure 6: Sample screens for creating Digital Company ID

Key Findings from SME Research:

To better understand user need and perspective, CFIT commissioned Opinium to conduct independent qualitative research with 29 SMEs from various industries, locations, and sizes (5–50 employees, turnover below £10 million). Over half had opened a bank account recently. Participants were invited to test the POC developed by the Coalition and share their views on the potential application of Digital Company ID in their daily operation. Here are our key findings:

Key finding 1 **Benefit and value**	SMEs understood how Digital Company and personal ID can unlock powerful longitudinal value in saving time on administrative tasks, simplifying verification, and improving transparency in supply chains. Many appreciated the idea of securely storing data in one place, considering it safer than current systems like filing cabinets or personal devices.
Key finding 2 **Barriers and concerns**	Smaller SMEs, particularly those with fewer bank account transactions per year, perceived limited value in adopting Digital Company ID. They felt the solution was better suited to larger enterprises with higher transaction volumes. Privacy, security, and trust were recurring concerns, with many preferring banks to manage their data. They questioned why legitimate businesses should repeatedly verify their information, which is a key issue that the Coalition tried to address with Digital Company ID.
Key finding 3 **Fraud and usability**	While fraud is a top concern for smaller SMEs, many trust banks to mitigate the risks. Larger SMEs, with more robust systems recognised the advantages of a single source of truth. The data sharing capabilities of Digital Company ID were seen as more valuable than the ID itself, but the frequency of use and upfront data requirements were perceived as potential hurdles.

Overall, SMEs appreciated the potential to reduce administrative burdens and streamline processes using Digital Company ID. Larger SMEs had more appreciation of its value in fighting fraud. Some of the participants highlighted the need for clearer management and data protection assurances. These will be explored further in our recommendations and the Coalition's next phase of work.

> "Enabling modern digital verification services for individuals and organisations is key to helping to reduce fraud, by removing opportunities for imposters to misrepresent who they are. We welcome the CFIT work and are excited to create implementable and scalable new secure services and products that will enable corporates to protect themselves from economic crime."

Paula Sussex, CEO, OneID

> "CRIF has been a core partner within this coalition. We look forward to the coalition's recommendations being taken forward and, in particular, to the creation of a prototype that can be deployed across the financial ecosystem. CRIF is committed to delivering this with other coalition and industry partners."

Glen Keller, Chief Product Officer, CRIF UK

Chapter 5

Emerging Design Considerations of Digital Company ID

The Coalition, in developing the POC, highlighted critical design considerations across three key areas:

- The essential features of Digital Company ID.
- The governing frameworks needed to ensure trust and security.
- The market dynamics required to drive adoption and innovation.

Among these, the Coalition believes that alignment with the UKDIATF is the most crucial factor. Ensuring compatibility with the UKDIATF will provide a structured, interoperable, and secure foundation for Digital Company ID, leveraging the UK's existing personal digital identity ecosystem and reinforcing fraud prevention efforts across financial services and beyond.

Compatibility with the UK Digital Identity and Attributes Trust Framework

To play an effective role in fighting fraud, Digital Company ID needs to be paired with a sophisticated, pre-existing verified personal digital identity[13]. The greatest advantage lies in deterring individual bad actors from entering the financial system in the first place or, if they do gain access, identifying and stopping them quickly.

We expect that personal digital identity, as already defined in the Government's UKDIATF, will be widely adopted and that Companies House will rely on these verified personal digital identities in establishing the authenticity of directors and PSCs for all UK corporate entities. The existence of a well-functioning personal digital identity market is an essential component of Digital Company ID. The UKDIATF provides a structured approach for the creation and management of personal digital identities. We anticipate that Digital Company ID will follow a similar approach, with standards and guidelines set out to ensure its security, interoperability and robustness. Organisations adhering to this framework can obtain certification, demonstrating their commitment to maintaining high standards in digital identity management and promoting trust in the market[14].

Other Design Considerations

To support a usable, scalable and trusted Digital Company ID across different sectors requires the development of service design principles. These are crucial to the development of the market, supporting a repeatable foundation that enables low friction and in turn, ease of adoption and use. We expect these to be explored further as industry develops a minimum viable product of Digital Company ID and validates the solution with real customers.

Emerging Service Design Considerations

Key Features of Digital Company ID

- **Every Digital Company ID should have a common core.** which represents the standardised verified, minimal data that is sufficient to do a first pass risk assessment for onboarding and KYB compliance process.
- **Digital Company ID must be extensible** beyond the bank onboarding use case and beyond the financial services market.
- **An extensible data architectural design** to support an ecosystem of value-added services across sectors. In other words, certified providers can incorporate additional validated / attested data to further inform risk assessment in other use cases, such as used car auctions.
- **Digital Company ID must maximise the opportunity for reuse and interoperability** of all data within agreed terms. In other words, it should support the ability for a company or an authorised representative to reuse the verified credentials or underlying data, for example when they switch their Digital Company ID to another provider.

Governing Frameworks

- Digital Company ID should be a solution that is **compatible with the UKDIATF** and other relevant global open standards.
- Where **validation of an individual** is required, say a company director, this will be performed by an Identity Provider / Holder Service Provider that is certified under the UKDIATF including at record creation or when enacting a contract, etc.

Market Development

- Digital Company ID should support the **creation of a contestable market of company ID providers**, promoting competition and enabling a robust and responsive ecosystem to address and service niche and emerging use cases.

Chapter 6

Essential Enablers of Digital Company ID

The UK is well positioned to rapidly mature its Digital Company ID market due to its well-established regulatory frameworks, a highly developed financial and legal ecosystem, a robust digital infrastructure, and strong Government support for initiatives such as Smart Data and trusted digital identity, which collectively create an environment conducive to innovation and adoption.

The Coalition has identified the critical enablers spanning regulation, infrastructure, and commercial frameworks with some of these already in place or actively under development. Together, these elements are essential for creating the right market conditions and incentives for Digital Company ID to scale. To establish a robust and agile Digital Company ID ecosystem, it is essential to align the legal and regulatory framework in parallel with the technology standards and architecture. These establish the foundation and trust for the provision and deployment of Digital Company ID.

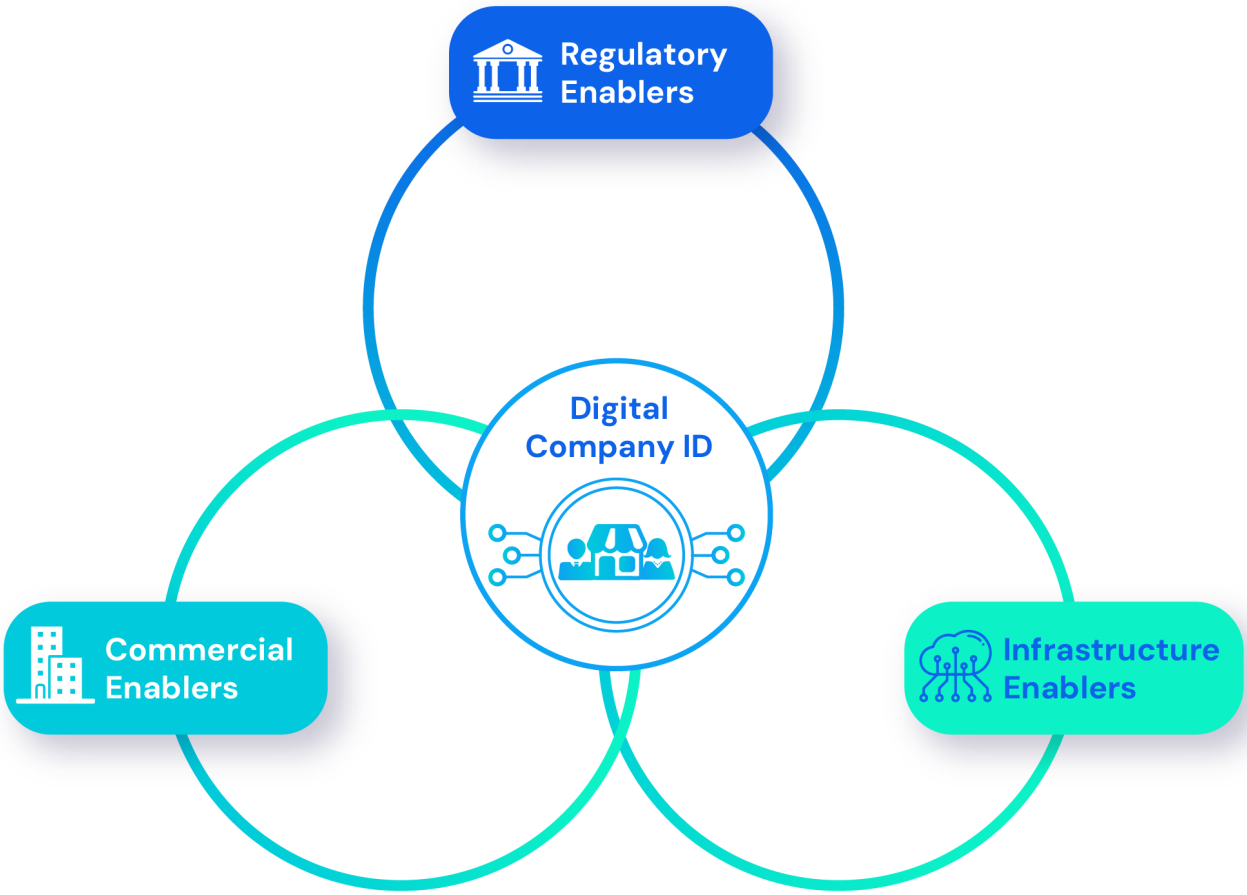


Figure 7: Essential Enablers of Digital Company ID

Regulatory Enablers

For instance, the **Data (Use and Access) Bill** and **Smart Data Schemes** enable secure data sharing and operational efficiencies, delivering significant benefits for businesses. At the same time, reforms under the **Economic Crime and Corporate Transparency Act (ECCTA)** and new verification rules introduced by the Companies House ensure access to reliable company data. Government initiatives like the **Digital Regulation Cooperation Forum (DRCF)** and **Regulatory Innovation Office (RIO)** encourage collaboration across sectors, aligning new innovation such as Digital Company ID with emerging market needs and regulatory priorities.

Infrastructure Enablers

Other enablers provide the technical infrastructure and governance necessary for scalability and trust. The **FCA innovation services** provide essential tools to test Digital Company ID in a controlled environment. The **Digital Securities Sandbox** supports the testing and refinement of Digital Company ID within the capital market, while various **governance and trust frameworks** ensure data quality, reliability and interoperability across sectors. By facilitating secure and innovative data usage, **system-level fraud data sharing rules** and **Smart Data Schemes** strengthen fraud prevention through harnessing better fraud intelligence. **Sustainable commercial models**, underpinned by these enablers, ensure that value propositions are clear and viable for long-term success.

Commercial Enablers

To further drive adoption, **optimal user experiences**, **priority use cases**, and **international demand** enhance trust, usability, and integration across sectors and borders as global interest in Digital Company ID grows. Together, these enablers not only support the implementation of the recommendations, set out in the next chapter, but also deliver economic and operational benefits, fostering a secure and innovative digital economy.

Detailed description and level of maturity of each enabler can be found in Appendix 3.

Regulatory Enablers		
1	Data (Use and Access) Bill	The UK Data (Use and Access) Bill enables Digital Company ID, strengthening data protection, driving innovation, and supporting economic growth alongside the Economic Crime and Corporate Transparency Act (ECCTA).
2	ECCTA & Companies House Reform	Companies House reforms under the ECCTA enable Digital Company ID by requiring identity verification and enhancing fraud prevention.
3	Anti-Money Laundering	UK AML regulations reinforce the need for robust digital verification, strengthening the Digital Company ID market and combating economic crime.
4	FCA Innovation Services	The FCA innovation services offer a range of market facing tools and support for firms launching innovative products and services. Testing Digital Company ID in the FCA innovation services would help provide clarity regarding regulatory requirements and support delivery.
5	Digital Securities Sandbox	The FCA and Bank of England's Digital Securities Sandbox supports innovation in capital markets and explores digital verification, advancing the role of Digital Company ID in financial market infrastructure.
6	Digital Regulation Cooperation Forum (DRCF)	The DRCF fosters collaboration among regulators (FCA, ICO, Ofcom, CMA) on digital identity, advancing efforts to develop Digital Company ID.
7	Digital Markets, Competition and Consumers Act (DMCC)	Digital Company ID, alongside digital personal identities, provides an essential tool for all businesses to take advantage of the opportunities that the DMCC enables.
8	Regulatory Innovation Office (RIO)	The Regulatory Innovation Office reduces regulatory barriers, aligning priorities, and fostering collaboration, ensuring swift adoption of innovative solutions.

Infrastructure Enablers		
1	Digital Personal ID	Digital personal identities are integral to Digital Company ID, enabling directors and company representatives to verify their identity securely. Supported by the Data (Use and Access) Bill, digital personal identities and Digital Company ID will modernise verification processes.
2	Digital Company ID Governance	Trust frameworks like the UKDIATF ensure secure ecosystems, laying the foundation for a Digital Company ID governance framework that is fit for purpose and tailored for the UK market.
3	Sustainable Ecosystem Commercial Model	A sustainable commercial model and liability framework are key to the widespread adoption of Digital Company ID, ensuring scalability and addressing evolving risks in the digital identity market.
4	Smart Data Schemes	Smart Data schemes enable secure data sharing, and streamline business processes, essential for creating and using Digital Company ID.
5	System Level Fraud Data Sharing	System level fraud data sharing amplifies the value of Digital Company ID by enabling fraud intelligence across organisations. Industry collaboration is essential to enable and establish reciprocal and secure data sharing networks.

Commercial Enablers		
1	Priority Use Cases & Value Creation	The Coalition's POC highlighted Digital Company ID's broader potential, including boosting SME productivity and capturing accurate business data. Identifying key use cases and frameworks will boost market adoption and investment.
2	Optimal User Experience	Optimised user experiences and standardised features are key to adopting Digital Company ID, enabling seamless, secure use across markets.
3	International Demand	The international digital identity market is evolving with common standards. Aligning Digital Company ID with these developments is key to unlocking export potential for UK businesses and promoting global trades.

Chapter 7

Next Steps for Digital Company ID

This section outlines targeted recommendations that enable Digital Company ID to scale and fight fraud. The recommendations build on our key findings and focus on secure data sharing, governance, regulatory alignment, scaling and interoperability. This is a call to action for policymakers, industry leaders, and regulators to collaborate and drive forward Digital Company ID, reinforcing the UK's position as a leader in digital innovation and financial security.

CFIT Recommendations: A Call to Action

1. **Develop a Prototype for Digital Company ID**
   CFIT, in collaboration with industry, should test and launch a fully functional Digital Company ID prototype to gather user feedback, validate functionality, and ensure regulatory alignment.

2. **Enable Reciprocal and Secure Data Sharing**
   The Government must consider mandating all relevant organisations across the ecosystem to share data on economic crime, while industry collaborates to define data sharing models and permissions.

3. **Appoint a Lead Authority**
   To address market coordination failures, the Government should consider appointing a lead authority to oversee the accreditation and governance of Digital Company ID.

4. **Promote Standards for Interoperability**
   CFIT is committed to collaborating with industry to establish standards that ensure domestic and international interoperability, accountability, and secure adoption of Digital Company ID.

5. **Create a Multi-Stakeholder Taskforce**
   A taskforce should be established to identify, prioritise, and develop high-value use cases for Digital Company ID within financial services.

6. **Review the Regulatory Framework**
   Policymakers, working closely with industry, must review the regulatory framework for Digital Company ID, ensuring it is fit for purpose in order for firms to rely on Digital Company ID from a regulatory perspective.

7. **Drive Market Confidence Through Government Adoption**
   Government departments must lead by example, adopting Digital Company ID for critical interactions. This will help create support for private sector investment and build trust in the system.

Figure 8: CFIT Recommendations: A Call to Action

1. Develop a Prototype for Digital Company ID

To unlock the full potential of Digital Company ID in fighting fraud and driving economic growth, we recommend developing and testing a fully functional prototype. Building on the Coalition's POC, this solution will integrate real-time data from trusted sources into a user-friendly and secure system. Testing the prototype in the FCA innovation services would help provide clarity regarding regulatory requirements. It would also support the delivery of a practical solution that is robust and adaptable to the needs of businesses.

During this process, CFIT, policymakers, regulators and industry would work together to gather user feedback, refine the solution to incorporate necessary safeguards, and assess regulatory implications. This should take into consideration latest legislative developments like the Data (Use and Access) Bill and global initiatives. By validating the prototype in a controlled environment, stakeholders can address potential challenges including identifying necessary policy changes and mitigating risks against misuse. Further, it will help upskill the involved stakeholders on Digital Company ID.

2. Enable Reciprocal and Secure Data Sharing

Criminals exploit gaps in data sharing between financial institutions, allowing them to commit fraud elsewhere after being discovered and offboarded by previous institutions. Reciprocal and secure data sharing, enabled in part by Digital Company ID, offers a new set of tools in combatting the growing threat of fraud in the UK. Improved intelligence across the market will enable swift detection of bad actors and stop criminals who have been offboarded by one firm committing fraud in others.

To address the increasing sophistication of fraud, the financial ecosystem must implement reciprocal and secure data sharing. This effort should be reinforced by the adoption of Digital Company ID, which, when combined with the expanding availability of data through various Smart Data initiatives, presents a unique opportunity to enhance fraud prevention and combat economic crime. Digital Company ID acts as a bridge between fragmented intelligence sources, enabling more efficient fraud detection and mitigation.

To achieve this, we recommend that the Government considers:

- Mandating all relevant organisations across the ecosystem to share data on fraud and other types of economic crime. This will incentivise timely reporting and intelligence sharing across relevant stakeholders, including financial institutions, payment operators, BigTechs, and telecommunication companies.
- Conducting a market study to review the economic crime data sharing landscape in the UK, and consider ways to join up different national and sectoral intelligence networks, such as the National Fraud Intelligence Bureau, National Fraud Database, National Hunter, National SIRA, etc.
- Assessing the potential role of Digital Company ID in linking both fraud and economic crime data to help provide insights that could guide counter-fraud efforts.

As part of the study, industry should collaborate with Government and regulators to:

- Identify and prioritise the types of data that would be the most effective in combating fraud.
- Understand the different models for sharing data, including who provides the permission to share the data.
- Consider any implications on data protection, privacy and competition.

3. Appoint a Lead Authority

To address market coordination failures and ensure the successful implementation of Digital Company ID, the Government should consider appointing a lead authority. This body will provide clear ownership and accountability within the Government and oversee the governance and accreditation of Digital Company ID in the UK.

The appointment of a lead authority is critical to creating a structured approach to the governance of digital identities, including personal digital identities (an area that has progressed due to the UK digital identity and attributes trust framework) and Digital Company ID. Clear accountability will enable industry to drive implementation and scaling, while avoiding fragmentation that could slow progress. A sector-agnostic, central governing body will streamline decision-making, foster stakeholder collaboration, and build trust across industries. CFIT stands ready to help drive forward implementation and scaling by convening key industry stakeholders.

4. Promote Standards for Interoperability

Interoperability is essential for fostering widespread adoption of Digital Company ID. We recommend the development of standards that promote interoperability, ease of access, and reuse across various customer journeys. Having clear and consistent standards will ensure that Digital Company ID is user-friendly, scalable, adaptable and widely applicable. The standards should consider cross border initiatives and reflect other international frameworks, such as the EU Digital Identity Wallets, where possible. By driving market-wide consistency, these standards will enable easy creation and application of Digital Company ID across use cases, sectors and borders.

To facilitate the creation of these standards, CFIT will convene a cross-industry, diverse stakeholder working group. The working group will evaluate and define appropriate governance protocols and produce practical insights that can be used to guide the development of standards and trust frameworks, ensuring the outputs are effective, implementable, and reflective of user needs. This collaborative effort will establish a robust foundation for interoperability, enabling seamless use of Digital Company ID across industries to deliver market-wide benefits.

5. Create a Multi-Stakeholder Taskforce

To drive the development and adoption of Digital Company ID, a taskforce should be established to identify, prioritise, and develop high-value use cases in financial services and other sectors. This taskforce will bring together industry leaders, policymakers, regulators, and other key stakeholders to address critical challenges such as supply chain validation and fraud prevention in public procurement. The taskforce will evaluate the market opportunity and commercial viability of priority use cases and create actionable strategies for implementation.

For instance, the taskforce will explore new applications of Digital Company ID that promote trust, deliver tangible benefits and improve SME productivity, such as validating supplier and customer interactions, and improving access to financial and non-financial services. It will establish scalable commercial models and liability frameworks that underpin sustainable, high-quality data sharing across sectors. Policymakers, acting as observers, will remain informed of market developments and key trends, supporting alignment with legislative and regulatory objectives.

6. Review the Regulatory Framework

Whilst the UK benefits from a well-developed regulatory environment, the current framework was predominantly written over thirty years ago, without emerging technologies, new players and innovative use cases in mind. Further, the sheer volume and complexity of regulations that interact with Digital Company ID may put immense pressure on firms to innovate and embrace new solutions, which hinders adoption.

To support ongoing innovation of the Digital Company ID in a fast-changing, global market, UK policymakers and regulators should undertake a comprehensive review, in collaboration with industry, to ensure existing frameworks are fit for purpose, close gaps and remove overlapping or duplicative requirements. Regulatory clarity will provide businesses with the confidence to adopt Digital Company ID.

This review is essential for building trust, reducing complexity, and ensuring regulatory frameworks are fit for the rapid change in the digital era. It will also clarify the roles of Government departments and regulators in this space.

7. Drive Market Confidence Through Government Adoption

To accelerate adoption, Government departments should lead by example and adopt Digital Company ID for government services, such as procurement, tax filings and confirmation statements submission. Early adoption by the Government will build trust in the system and inspire confidence and investment among private sector stakeholders.

By adding Digital Company ID as a reliable proof of identity for government services, businesses will be encouraged to integrate Digital Company ID into their operations. This will also improve user experience, simplify verification, and create efficiencies in the provision of government services.

Moreover, Government could explore additional levers to encourage the adoption of Digital Company ID, such as introducing tax incentives and public procurement compliance requirements. These measures will promote the utility of Digital Company ID across various sectors and accelerate the transition to a Smart Data economy through wider and improved data sharing.

> “The adoption of Digital Company IDs has the potential to drive growth and foster greater economic prosperity. For UK SMBs, which make up 99% of the business landscape, this presents an opportunity to drive productivity while reducing compliance costs and cutting through admin. Overall, an important step towards a more digitised economy.”

Steve Hare, CEO, Sage

Appendix 1

The Face of Financial Crime in the UK

In 2023, over 1.2 million incidents of fraud were committed in the UK — equivalent to over two fraudulent acts every minute[15]. Financial fraud is growing at an alarming rate, and advances in AI are expected to accelerate this growth unless decisive action is taken. The economic and social harm caused by fraud is profound. According to the Home Office, fraud targeting individuals resulted in a direct cost of £4.4 billion in 2019/20, with each incident causing an average financial loss of around £4,000[16].

However, this direct impact on victims is likely only a part of the broader societal cost of fraud. Significant resources are devoted to preventing, prosecuting, and assisting victims of fraud. According to an estimate by LexisNexis Risk Solutions and Oxford Economics, in 2022/23, the financial sector spent an estimated £34.2 billion on regulatory compliance[17], much of it aimed at combating financial fraud. Despite these efforts, fraud that occurs within the financial sector undermines trust in institutions. This is particularly concerning at a time when financial institutions are expected to play a leading role in adopting and deploying future technologies for both anti-fraud efforts and economic growth.

The FCA has three key operational objectives: protecting consumers from misconduct, safeguarding the integrity of the UK financial system, and promoting effective competition[18]. Fraud impacts all three:

- It is the most direct form of "bad conduct" harming consumers.
- Fraudulent activity undermines fair competition by rewarding firms engaged in deceptive practices.
- Fraud erodes the systemic trust and integrity of the financial system, which the FCA recognises as crucial to the UK's international competitiveness and sustainable growth[19].

The fight against fraud is integral to maintaining a robust and trustworthy marketplace. The FCA emphasises that firms' business models, controls, and activities must uphold market trust and prevent financial crime, systemic risks, or market abuse. Fraud generates negative externalities by raising risk perceptions across the market, affecting overall business activity and damaging the reputation of entire marketplaces.

Fraud also has broader implications beyond its legal definition. Criminologists describe it as part of a continuum of deceptive behaviour—acts involving lying, deception, or false pretenses to gain financial advantage[20]. Activities like posting fake reviews or concealing negative feedback may not meet the legal definition of fraud but still fall within this spectrum of deceptive practices. Anti-fraud measures, especially those that leverage identity-based solutions, can play a critical role in addressing both outright fraud and other forms of deceitful behavior.

The economic benefits of improved market functioning, driven by more trustworthy data about participants, have been estimated to add between £3 billion and £25 billion annually to GDP[21]. Evidence suggests that high-trust societies tend to have both less regulation and greater market efficiency[22]. While much of this is not directly related to legally defined fraud, any reduction in fraudulent activity contributes to these positive outcomes. Anti-fraud tools, particularly identity-based solutions, are likely to be effective in addressing even forms of deceit that might be legal, like the exaggeration of commercial reputation through highly selective presentation of online reviews.

However, the impact of fraud extends beyond economics. When trust is eroded by fraud, it undermines social cohesion as well. High-trust societies are often associated with numerous socially beneficial outcomes, such as stronger support for redistribution and welfare policies. The widespread presence of fraud undermines these qualities, weakening the foundations of social solidarity[23].

Fraud is constantly evolving. Combating it has always been akin to a "Red Queen race," as described in ***Alice Through the Looking Glass***[24], where everyone must run faster and faster just to stay in the same place. Bad actors leverage technology to its fullest advantage, and those fighting fraud must remain at the cutting edge of innovation simply to keep up. The rise of AI and digitisation marks a new chapter in this ongoing battle.

AI is widely acknowledged to make many types of fraud easier to execute[25]. A chilling example that made headlines in early 2024 involved a deepfake video call where a fraudulent CFO of a multinational company instructed the Hong Kong office to urgently and secretly transfer $25 million[26]. The employee, reassured by the apparent presence of familiar colleagues on the call, complied. This incident illustrates the dangers posed by voice synthesis, video synthesis, and the large-scale exploitation of compromised personal and corporate credentials. Once the building blocks of Digital ID are in place, innovations can be developed that will reduce the risk of these sorts of fraud.

If even a multinational corporation can be deceived by such technology, it is not difficult to imagine the devastating effects as these tools are deployed against tens of millions of less technologically savvy individuals and organisations across society.

The economy is riddled with countless fraud attack surfaces, ranging from bank transactions and emails to pension scams, dating fraud, deceptive social media ads, investment schemes, and more. Each of these areas represents an opportunity for bad actors to exploit, and the capabilities of generative AI (GenAI) make it easier for them to operate across multiple domains. With 86% of all fraud being cyber-enabled, the majority of fraudulent activities will likely be amplified by GenAI's ability to automate processes and convincingly impersonate individuals or entities[27].

Society's vulnerability to cyber-enabled fraud is precisely what makes the issue well-suited to digital counter-fraud strategies. Fraud and anti-fraud efforts are locked in a constant cycle of evolution, each side leveraging the same technologies to outpace the other — a dynamic often referred to as the ***Red Queen Race***. This report focuses on the potential of a well-designed Digital Company ID to play a significant role in this ongoing battle. While digital personal IDs are widely recognised as vital tools in combating fraud, an effective Digital Company ID will also be essential. Crucially, Digital Company ID and digital personal ID must be equally sophisticated—if one lags behind, bad actors will inevitably target the weaker link.

With both Digital Company ID and digital personal ID, the most significant advantage lies in preventing bad actors from entering the financial system in the first place or, if they do gain access, identifying and stopping them quickly. The financial system — particularly banking — is almost indispensable for executing cyber-enabled fraud. Without a bank account, the only alternatives for profiting from fraud are cash and cryptocurrency. Cash typically limits fraud to face-to-face scenarios, while cryptocurrency, except in cases like cyber-extortion, remains relatively niche. A bank account is therefore a critical tool for most bad actors, making it a natural focus for fraud control.

Appendix 2

Driving Economic Growth in the UK with Digital Company ID

Digital Company ID, once fully deployed, will be a very valuable piece of digital infrastructure which will make a meaningful contribution to the UK's economic growth. In this section, we offer some order of magnitude calculations for the impact of Digital Company ID. Some of the quantified benefits come from reduced cost of compliance and some from impact to the wider economy. These efficiency gains can be used to reduce fraud, and in those cases, the benefits can be seen in fraud reductions.

We build up the figures from three distinct sources of benefit:

1. Digital Company ID will reduce the cost of banks' SME onboarding operations. Our POC work has provided us with quite detailed figures for this saving, and we have a good degree of confidence that this number can be extrapolated to the rest of the banking sector. This figure provides a resource cost saving, and, by the standard assumption that these resources are redeployed in the economy at the same rate of value add, this is taken to be an annual increase in GDP of £45 million.

2. The cost of banks' ongoing monitoring, compliance and due diligence will be reduced. We use an estimate of this cost in relation to the cost of onboarding provided by a detailed "Cost of Compliance Review" by Oxford Economics and LexisNexis Risk Solutions to extrapolate from our onboarding savings. This method suggests a further increase of annual GDP of £129 million.

3. The above two figures have considered the impact on banks' operations. However, we can expect Digital Company ID to have resource cost impacts in many other parts of the economy. First, there are other financial service and professional sector products like insurance, asset management (including real estate), accountancy and law where fraud control is almost as important and impactful as in banking.

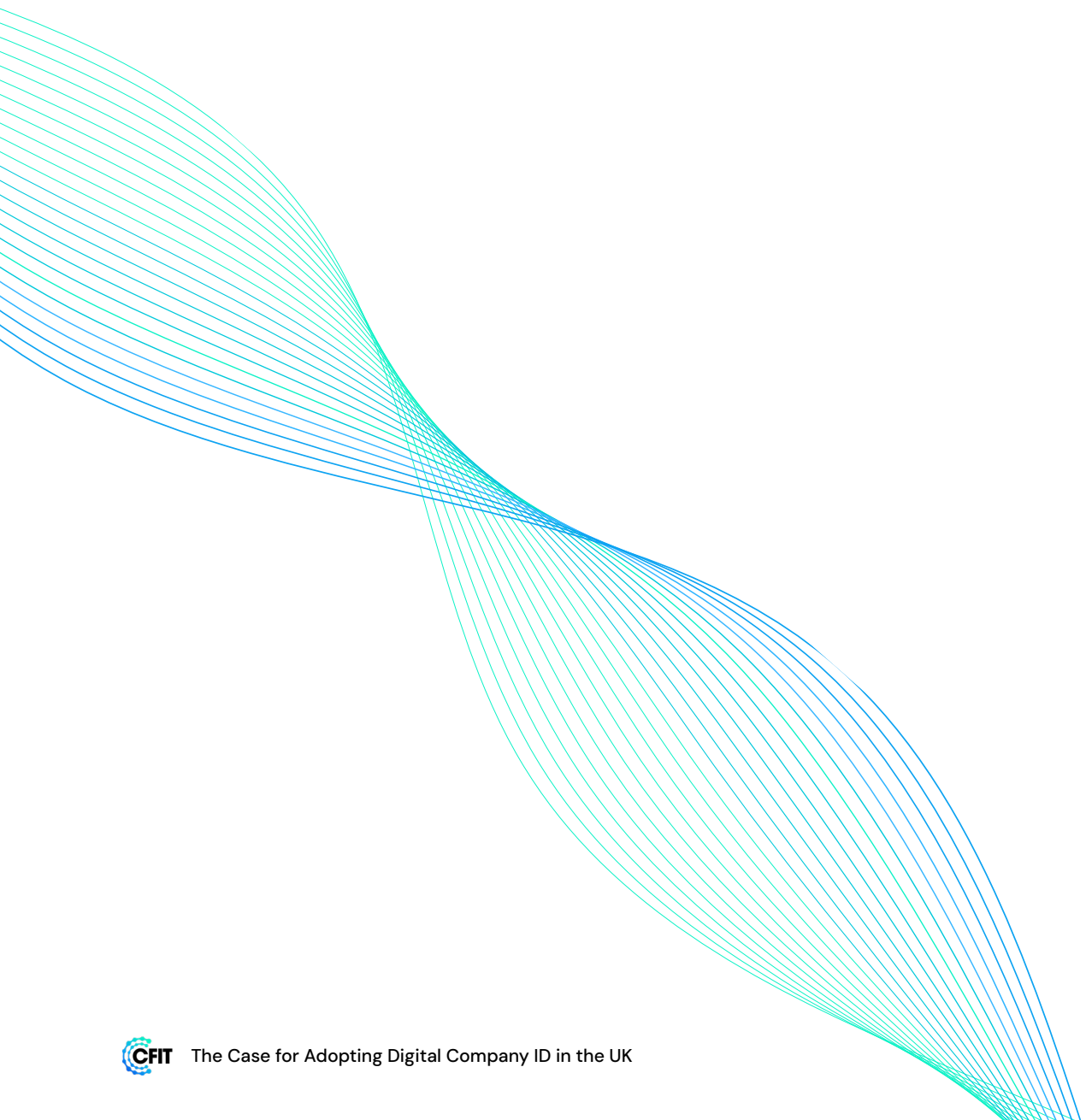
   We extrapolate our banking estimates to the rest of the financial sector using the Oxford Economics / LexisNexis Risk Solutions work, and reach a figure of approximately £1.7 billion annual GDP addition. The allocation is based first on the number of SME accounts versus personal accounts. We derive this from two sources: the FCA's statement that 97.9% of UK adults have a bank account, and Experian's report that there were 5.2 million SME accounts in 2022. Having used this proportional allocation (approximately 10% of total compliance costs to SMEs), we use the results of the POC estimate that Digital Company ID could reduce compliance costs by 50% to find an estimated resource cost saving.

   That, however, is not all when it comes to impacts on the wider economy. Many other parts of the economy are subject to fraud - for example waste management, some areas of public procurement, used car sales, branded consumer goods, food and agriculture, etc. Anti-fraud regulation is typically less stringent than in the financial sector, because fraud in these sectors is less enabling of fraud overall. However, we can expect Digital Company ID, with the increase in ease of use that it delivers, to have an impact in these sectors.

   Estimating these wider-economy effects is clearly difficult and subject to a wide range of uncertainty. We offer two methodologies to estimate an order-of-magnitude. The first is based on an

extrapolation of a figure modelled by McKinsey estimating that personal digital ID could contribute 0.5% of GDP in 2030. The second is an extrapolation of a figure estimated by the Behavioural Insights Team's analysis of the potential to "de-shroud" the economy with more accurate information and thereby improve the operations of competition. These two extrapolations are used as independent ways of establishing an order of magnitude for these diffuse wider economy effects, and both are consistent with a magnitude of approximately £1 billion per year.

The economic analysis highlights the significant financial and operational efficiencies that Digital Company ID can unlock, from reducing fraud-related costs to enhancing SME productivity and driving broader market confidence. However, realising these benefits at scale requires a strong foundation of regulatory, technical, and commercial enablers. Establishing a robust governance framework, ensuring interoperability with existing digital identity systems, and fostering industry-wide adoption are critical to transforming Digital Company ID from a concept into a widely accepted market standard. The following section outlines the essential enablers that will drive the successful implementation and scalability of Digital Company ID, providing the necessary infrastructure, regulatory alignment, and industry coordination to maximise its economic impact.



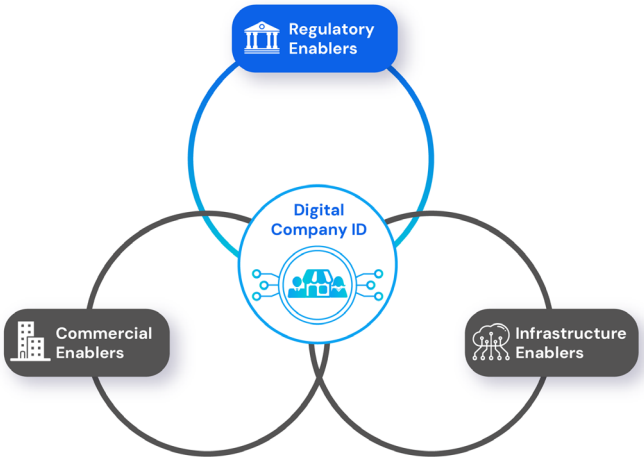
Appendix 3

Enablers of Digital Company ID

The Coalition has identified the critical enablers spanning regulation, infrastructure, and commercial frameworks to support the development of Digital Company ID. These enablers are essential for building a robust, agile and trusted digital infrastructure, and creating the right market conditions for Digital Company ID to scale. As the market matures, these enablers may evolve, and new enablers may emerge.

Regulatory Enablers

For Digital Company ID, these foundations are already being laid, with new or amended regulations and Government bodies in place or under development for the rapidly evolving markets where Digital Company ID will play a crucial role across the economy.



Regulatory Enablers		
1	Data (Use and Access) Bill	The UK Data (Use and Access) Bill enables Digital Company ID, strengthening data protection, driving innovation, and supporting economic growth alongside the Economic Crime and Corporate Transparency Act (ECCTA).
2	ECCTA & Companies House Reform	Companies House reforms under the ECCTA enable Digital Company ID by requiring identity verification and enhancing fraud prevention.
3	Anti-Money Laundering	UK AML regulations reinforce the need for robust digital verification, strengthening the Digital Company ID market and combating economic crime.
4	FCA Innovation Services	The FCA innovation services offer a range of market facing tools and support for firms launching innovative products and services. Testing Digital Company ID in the FCA innovation services would help provide clarity regarding regulatory requirements and support delivery.
5	Digital Securities Sandbox	The FCA and Bank of England's Digital Securities Sandbox supports innovation in capital markets and explores digital verification, advancing the role of Digital Company ID in financial market infrastructure.
6	Digital Regulation Cooperation Forum (DRCF)	The DRCF fosters collaboration among regulators (FCA, ICO, Ofcom, CMA) on digital identity, advancing efforts to develop Digital Company ID.
7	Digital Markets, Competition and Consumers Act (DMCC)	Digital Company ID, alongside digital personal identities, provides an essential tool for all businesses to take advantage of the opportunities that the DMCC enables.

Regulatory Enabler 1: Data (Use & Access) Bill

The UK Data (Use and Access) Bill (DUA Bill)[28], introduced to the House of Lords on 23 October 2024, is central to the development of the Digital Company ID market. Designed to "unlock the secure and effective use of data for the public interest," the Bill focuses on reforming data sharing and standards to drive innovation, improve public services, and strengthen data protection. The Bill supports the development of Digital Company ID by establishing the legal framework for digital identities, enabling Smart Data Schemes, and supports the Economic Crime and Corporate Transparency Act.

By establishing Digital Verification Services (DVS), the Bill provides the legal framework for secure and trusted personal digital identity products, enabling services such as pre-employment checks, age-restricted purchases, and moving house. This statutory footing will accelerate the implementation of the UKDIATF which forms the governing structure for Digital Identities and fosters a secure, investment-ready digital identity ecosystem.

By integrating Smart Data schemes, the DUA Bill creates a robust governance structure for broader data sharing. Together with digital personal and company ID the Bill lays the foundations for secure and scalable data sharing and with it, economic growth.

The DUA Bill's provisions also underpin broader legislative efforts, ensuring reliable enforcement of identification and verification requirements, as outlined in the ECCTA, and supporting data-sharing mechanisms in the fight against financial crime.

Regulatory Enabler 2: The Economic Crime & Corporate Transparency Act (ECCTA) & Companies House Reform

The reforms introduced by Companies House under the ECCTA[29] are critical to the development of the Digital Company ID market. These measures strengthen corporate verification by requiring all individuals registering or managing companies, such as directors and PSCs, to verify their identities via GOV.UK One Login or an Authorised Corporate Service Provider (ACSP). Additional requirements, such as verifying lawful purposes for company activities and providing more shareholder details, enhance the accuracy and reliability of data on the companies register. These changes not only improve transparency and trust in the UK business environment but also make it harder to use fictitious or fraudulent identities in company formation and operations.

These reforms are foundational for the Digital Company ID market, enabling reliable KYB compliance process and creating a trusted framework for data sharing and corporate verification. Coupled with provisions for a "recognised legitimate interest" in sharing data, these changes will bolster inter-industry confidence and improve the fight against economic crime. The CFIT-chaired taskforce on SME finance echoed the importance of these reforms, recommending accelerated implementation to standardise and verify company information. By linking identity verification with fraud prevention measures, the reforms further pave the way for a secure, transparent, and scalable Digital Company ID market, essential for tackling financial crime and supporting UK economic growth.

Regulatory Enabler 3: Anti-Money Laundering

The UK's anti-money-laundering (AML) regulations, based on the Financial Action Task Force (FATF)[30] recommendations, are critical to the development of the Digital Company ID market. These regulations require due diligence to prevent money laundering and terrorist financing, reinforcing the need for robust digital verification systems. Recent efforts, such as HM Treasury's 2024 consultation on improving the Money Laundering Regulations (MLRs), aim to strengthen defences against economic crime by targeting priority threats. Digital verification for businesses plays a vital role in supporting a risk-based approach, improving the effectiveness of AML measures, and ensuring a secure foundation for the Digital Company ID market to thrive.

Regulatory Enabler 4: FCA Innovation Services

The FCA innovation services offer a range of market facing tools and support for firms launching innovative products and services. These include the FCA regulatory sandbox, innovation pathways, digital sandbox, etc. Since 2014, the FCA has helped almost 1,000 firms develop and test their ideas through their innovation services. Testing a fully functional prototype of Digital Company ID in the FCA innovation services would help provide clarity regarding regulatory requirements. It would also support the delivery of a practical solution that is robust and adaptable to the needs of businesses.

Regulatory Enabler 5: Digital Securities Sandbox (DSS)

The FCA and Bank of England (BoE) launched the Digital Securities Sandbox (DSS) on 30 September 2024, the first Financial Market Infrastructure sandbox enabled by the Financial Services and Markets Act 2023. The DSS allows firms to test emerging technologies like Distributed Ledger Technology in the issuance, trading, and settlement of securities under a temporary, modified regulatory framework. This flexible environment supports innovation in UK capital markets while safeguarding market integrity and cleanliness. Running until December 2028, with applications closing in March 2027, the DSS aims to transition successful participants into a permanent regime, shaping the future of UK financial market infrastructure.

Regulatory Enabler 6: Digital Regulatory Reform

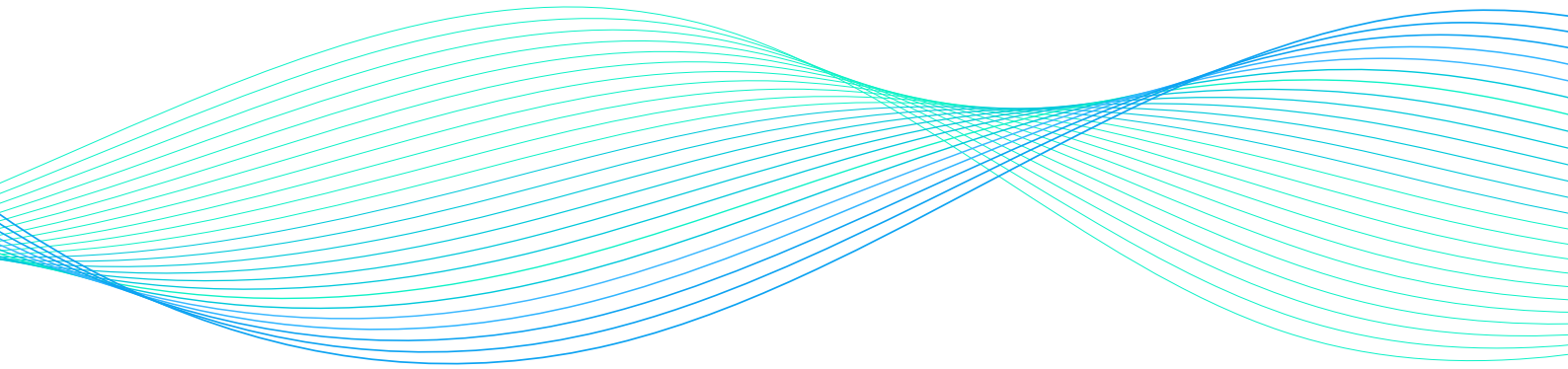
A key policy enabler is the Digital Regulation Cooperation Forum (DRCF), which ensures clear communication and transparency between its member regulators (FCA, Information Commissioner's Office (ICO), Ofcom, the Competition and Markets Authority (CMA) and avoid duplication of efforts. These regulators are actively working on digital identity, both collaboratively and within their areas of focus. The DRCF has already conducted horizon scanning into the future of digital identity.

Regulatory Enabler 7: Digital Markets, Competition and Consumers Act (DMCCA)

The DMCCA, with wide-ranging reforms, came into effect on 1 January 2025 and makes provision to reform digital markets, protect consumers and increase competition. While large technology firms are the primary focus of the Act, all UK businesses must understand the implications of the new rules and the opportunities enabled. The CMA will publish draft guidance on exercising its new powers, helping businesses prepare for the upcoming regime. Digital Company ID, alongside digital personal ID provides an essential tool for all businesses to take advantage of the opportunities that the DMCCA enables.

Regulatory Enabler 8: Regulatory Innovation Office (RIO)

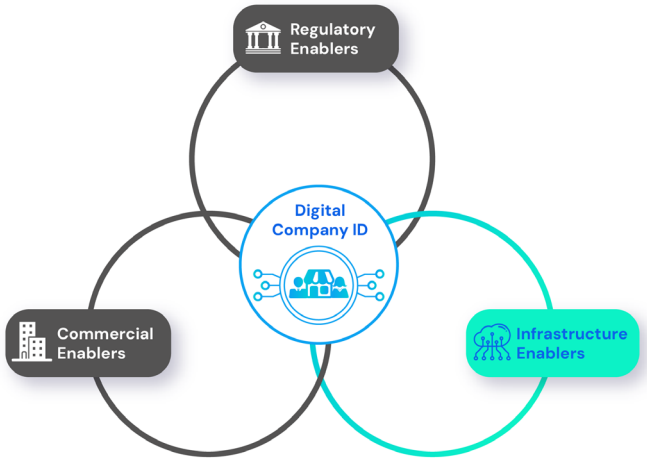
The new Regulatory Innovation Office (RIO) aims to reduce barriers for businesses by supporting regulators in updating regulations, speeding up approvals, and fostering collaboration among regulatory bodies. The RIO will align regulatory priorities with Government ambitions to drive innovation and economic growth. For the development of Digital Company ID RIO is well positioned to play a critical role in ensuring rapid market development, particularly where sector-specific regulation or amendments are required. This has been demonstrated in the age verification use case, where trials began in 2019, legislative consultations were completed in early 2024, and Government-backed digital ID for alcohol sales are expected by 2026. By tackling regulatory barriers, the RIO will be essential in addressing the rapidly evolving fraud landscape and enabling Digital Company ID adoption.



Infrastructure Enablers

Key components that enable individuals and entities to verify and authenticate identities online while maintaining privacy and control over personal data.

The infrastructure enablers for Digital Company ID build on those already developed for the digital personal ID including governance structures, ecosystem commercial models, data access schemes. Additionally, system level fraud intelligence sharing lays an infrastructural foundation in the fight against economic crime.



Infrastructure Enablers		
1	Digital Personal ID	Digital personal identities are integral to Digital Company ID, enabling directors and company representatives to verify their identity securely. Supported by the Data (Use and Access) Bill, digital personal identities and Digital Company ID will modernise verification processes.
2	Digital Company ID Governance	Trust frameworks like the UKDIATF ensure secure ecosystems, laying the foundation for a Digital Company ID governance framework that is fit for purpose and tailored for the UK market.
3	Sustainable Ecosystem Commercial Model	A sustainable commercial model and liability framework are key to the widespread adoption of Digital Company ID, ensuring scalability and addressing evolving risks in the digital identity market.
4	Smart Data Schemes	Smart Data schemes enable secure data sharing, and streamline business processes, essential for creating and using Digital Company ID.
5	System Level Fraud Data Sharing	System level fraud data sharing amplifies the value of Digital Company ID by enabling fraud intelligence across organisations. Industry collaboration is essential to enable and establish reciprocal and secure data sharing networks.

Infrastructural Enabler 1: Digital Personal ID

Digital personal ID is a key component of Digital Company ID, allowing directors to verify their identity when acting on behalf of a company. The UK's development of a digital personal ID system marks a significant step toward modernising identity verification, balancing technological advancement with privacy considerations. The DUA Bill aims to establish a secure and efficient framework, certifying approved identity verification products to build trust and simplify processes for both individuals and businesses.

Digital personal ID are also laying the groundwork for public recognition of the value the digital ID offers and an adoption path. Public support for digital identities is growing, with a recent survey showing 53% of the public in favour of a universal digital ID system, backed by prominent political figures[31]. Currently, 52 pre-certified personal digital identity providers are awaiting the finalisation of the Data Bill to be able to move forward.

Infrastructural Enabler 2: Digital Company ID Governance

Trust and governance are central to the development of digital identities, with Trust Frameworks playing a critical role alongside regulatory powers. These Frameworks address issues beyond the scope or granularity of regulations, such as API schemas and commercial models. Today UKDIATF supports the digital personal ID market by providing governance for a trusted and interoperable ecosystem. Under development since 2020, it has evolved through policy planning, consultation, stakeholder engagement, and iterative refinement.

The UKDIATF's development included the release of an alpha version in 2021, public testing in 2022, and a beta version in 2023, which introduced a trust mark for certified providers. Continued refinements in 2023-2024 have laid the groundwork for a Digital Company ID Trust Framework, which is likely to adopt foundational elements from the personal DIATF, adapting them to suit the specific data, context, and governance requirements of the Digital Company ID market.

Infrastructural Enabler 3: Sustainable Ecosystem Commercial Model

A sustainable commercial model for the provision of Digital Company ID is critical for the solution to scale and to ensure its long-term viability. The commercial model is essential to align the incentives between Digital Company ID providers, data owners (i.e., SMEs), data providers (i.e., credit reference agencies) and data users (i.e., lenders and financial institutions). It also fosters the development of a healthy, competitive ecosystem.

Establishing common foundations for liability models is equally essential to ensure alignment with commercial frameworks, integration with trust and governance structures, and adaptability to the unique risks of each use case. As the Digital Company ID market continues to develop, further work will need to be undertaken to establish the appropriate commercial and liability frameworks, to be reflective of evolving market needs and emerging use cases.

Infrastructural Enabler 4: Smart Data Schemes

To gain access to the wider economic opportunities from Digital Company ID, Smart Data schemes are key enablers. They enable secure, efficient, and regulated data access for seamless economy-wide use in business processes and digital services.

Smart Data schemes enable secure sharing of digital data from multiple sources and sectors, ensuring interoperable use across systems, fostering accuracy and trust in various applications. Smart Data schemes are crucial for unlocking the value of Digital Company ID, as demonstrated by the Coalition's POC development process. The Coalition identified a set of data needed for the creation of Digital Company ID and additional data requirements for bank onboarding and KYB compliance process, much of which could be made available via Smart Data schemes.

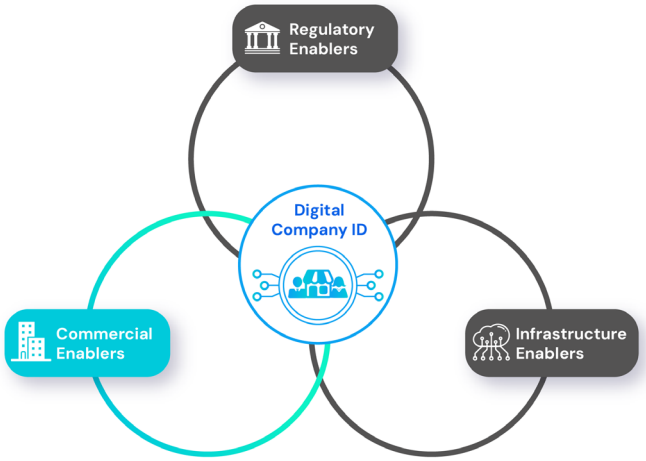
The UK Smart Data Team, under the Department for Business and Trade (DBT), is developing a strategy to establish these schemes, with planning already underway. CFIT is looking forward to providing support where required to advance the progress.

Infrastructure Enabler 5: System Level Fraud Data Sharing

System level sharing of data about frauds multiplies the value from Digital Company ID by enabling fraud intelligence sharing. Fraudulent activity can be shared across multiple organisations. Industry must come together to drive this opportunity forward and implement voluntary data sharing networks and update their products to make the most of Digital Company ID.

Commercial Enablers

Commercial enablers for company ID support a thriving market and foster innovation, competition, and consumer trust, opening domestic and global economic opportunities.



Commercial Enablers		
1	Priority Use Cases & Value Creation	The Coalition's POC highlighted Digital Company ID's broader potential, including boosting SME productivity and capturing accurate business data. Identifying key use cases and frameworks will boost market adoption and investment.
2	Optimal User Experience	Optimised user experiences and standardised features are key to adopting Digital Company ID, enabling seamless, secure use across markets.
3	International Demand	The international digital identity market is evolving with common standards. Aligning Digital Company ID with these developments is key to unlocking export potential for UK businesses and promoting global trades.

Commercial Enabler 1: Priority Use Cases and Value Creation

The bank account onboarding use case that the Coalition POC developed has enabled an increased level of clarity and understanding of the potential applications of Digital Company ID. The Coalition SME research highlighted further broader use cases which can support SME productivity through its ongoing use such as mandatory filing, supplier verification and payment authorisation. This echoes the National Payments Vision[32] which has welcomed the Coalition's work and will in due course consider any findings that emerge.

To encourage the adoption of Digital Company ID, it is important to identify a set of priority use cases within and beyond the financial sectors, establish the value propositions and the appropriate commercial and liability models that underpin each use case. This will promote the market's understanding of, engagement with, and investment in the value made available by Digital Company ID, and as a result, enhancing and realising the economic benefits.

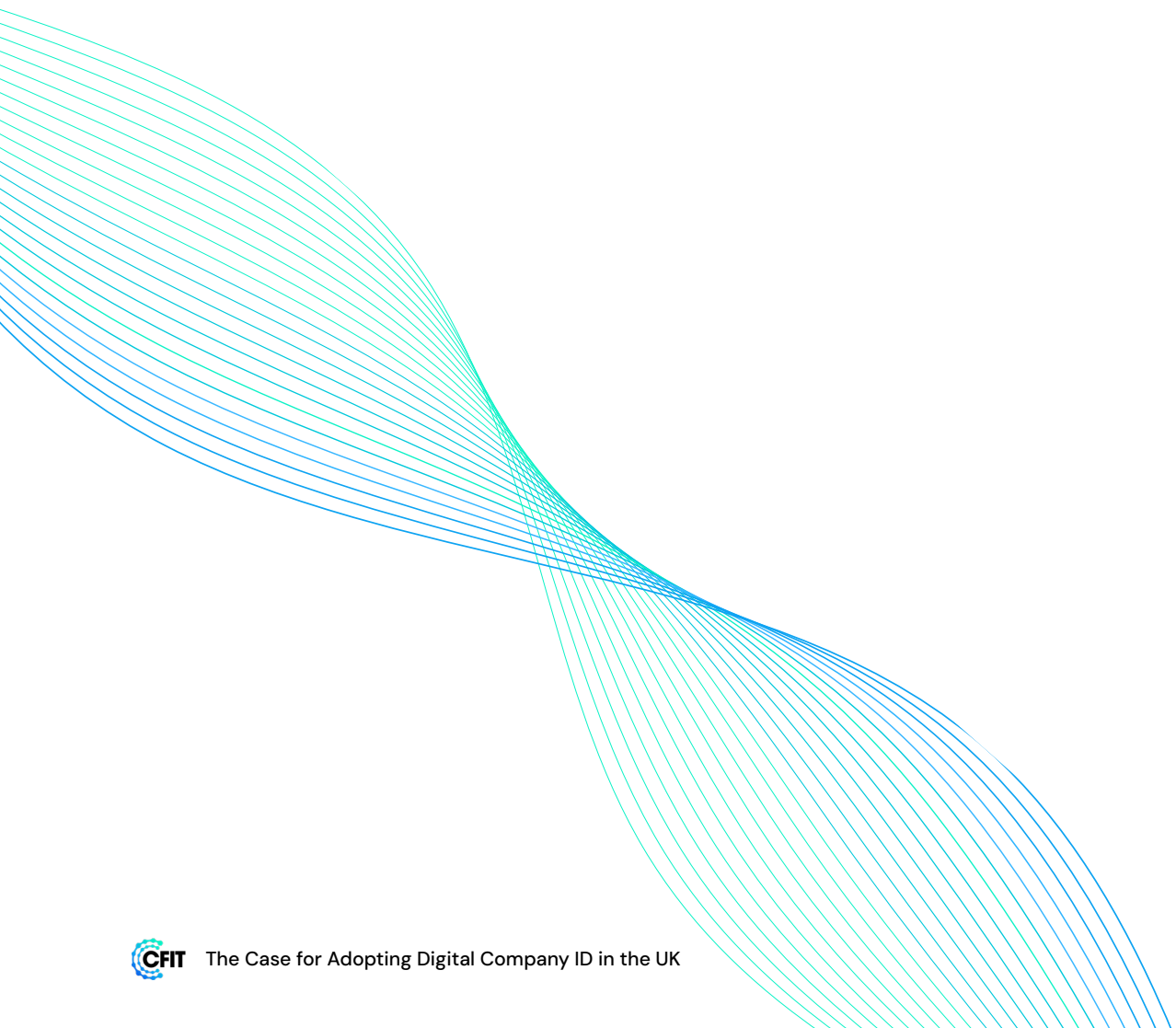
Commercial Enabler 2: Optimal User Experience

The development of optimal User Experiences is critical to accelerating the adoption of Digital Company ID and in strengthening the fight against economic crime. Essential features, such as how IDs are initiated, integrated into online customer journeys, and designed for safety and data sharing, require standardisation to ensure seamless use at scale and pace.

Achieving this in a competitive market with multiple Digital Company ID providers depends on users easily recognising and adopting these features, which rely on common "design patterns". These patterns require careful crafting to blend naturally into daily life and across multiple markets and use cases, enabling widespread adoption.

Commercial Enabler 3: International Demand

The international digital identity market is progressing across multiple jurisdictions, and common standards are beginning to emerge. Unlocking export potential for UK businesses will require the ability to efficiently and competitively operate in these jurisdictions. The alignment of Digital Company ID with international digital identity market developments will be an essential enabler.



Appendix 4

International Case Studies

Many countries have adopted digital verification (DV) schemes, reducing fraud and enhancing financial security. While Estonia, Sweden, and India lead with public-sector models, Canada and the Nordic countries rely on private-sector solutions. The UK, however, has yet to implement Digital Company ID, leaving it more vulnerable to fraud and falling behind in global efforts to combat digital financial crime.

Members of this Coalition, in answer to the question: "What other jurisdictions should the UK look to for good models or lessons in ID and data sharing initiatives for the financial sector?" singled out: Canada, Estonia, Netherlands, India, and Sweden. In each country, action is already being taken to meet the need for verification of corporates, either by the public sector or by private companies. India, and Estonia all have public sector digital verification (DV) schemes in place. The Nordic countries and Canada have established private sector DV schemes. Netherlands has a hybrid model. Below, we have set out detail on the DV schemes utilised in each of these jurisdictions, as well two core markets for the UK: the United States (U.S.), and the European Union (EU).

Key Takeaways:

- Global Leaders: Estonia, Sweden, and Norway are standout examples of high adoption and seamless integration.
- EU Integration: The EU leads in interoperability with the electronic identification, authentication, and trust services (eIDAS) framework, ensuring cross-border utility.
- Developing Systems: Canada and the U.S. are advancing through private-sector innovation, while India's Aadhaar showcases biometric-based success.
- Fraud Reduction: All systems report significant fraud prevention, particularly in finance and government services.

1. Canada

This section explores how corporate verification in Canada is facilitated by its e-system, a digital identity system tailored for business use. This system is part of the broader Pan-Canadian Trust Framework, ensuring secure and interoperable identity verification processes.

- In Canada, corporate verification can be conducted through several systems depending on the specific needs such as verification of corporate status, validation of corporate information, or verification for legal compliance. Key systems include:
  - Corporations Canada: This is the federal body responsible for the incorporation and maintenance of federal corporations. It offers an online database where you can search for federally incorporated companies.
  - Each province and territory in Canada have their own corporate registry. These registries maintain records of all incorporated businesses within their jurisdiction, including registration information and compliance status. Examples include the Ontario Business Registry, BC Registry Services, and Registraire des entreprises in Quebec.

- Canada Revenue Agency (CRA): The CRA's Business Number (BILLION) is a unique identifier for businesses in Canada, used for various tax and program accounts.

- For most corporate verification purposes, businesses and individuals will check through the federal Corporations Canada database or the relevant provincial registry.
- Canadian businesses leverage SecureKey's Verified.Me, which aligns with international identity standards. This facilitates secure transactions with global partners and integrates Canadian systems into international digital identity frameworks.
- There is a moderate to high usage of corporate verification across various sectors, particularly finance and regulated industries such as healthcare.
- The value chain involves public sector agencies (such as government business registration), banks, and private entities that offer services to corporations.
- These entities collectively contribute to a streamlined process for secure and verified corporate onboarding and interactions.
- Key providers include SecureKey and Verified.Me. Additionally, provincial government systems like BC Services also play a role in the corporate verification ecosystem.
- The digital ID systems enhance fraud prevention capabilities within the value chain, notably during the onboarding of corporate entities and their ongoing transactions.
- This improved security is expected to yield noticeable benefits in areas such as online financial transactions (46% improvement), online account openings (38% improvement), and eCommerce transactions (33% improvement)[33].

2. Estonia

This section explores Estonia's corporate verification approach, which is primarily enabled by the e-Business Registry and e-Residency program. These provide digital ID for corporates, especially beneficial for foreign business owners. The X-Road platform facilitates secure data exchange for corporate transactions, enhancing the management of companies remotely.

- The e-Residency program enables corporates to easily access EU markets and is aligned with the eIDAS framework, promoting interoperability with EU digital systems.
- There is substantial adoption of Estonia's e-Residency, with over 109,000 e-residents resulting in the establishment of more than 29,000 companies globally. [34]
- This shows a strong preference among global corporates for using Estonia's digital systems for company formation and management.
- The value chain includes government agencies that issue e-Residency ID and private banks and service providers that support the business operations of these digital entities.
- This integration ensures a seamless process for establishing and operating companies within Estonia and across the EU.
- Key providers include the Estonian government and tech providers like Cybernetica, who support the infrastructure and technology behind the e-Residency and corporate verification systems.
- Estonia's e-Residency and corporate verification systems enhance transparency and security in corporate operations.[37]

- Because of these transparent systems, although specific fraud reduction statistics are not detailed, the outcome is known to reduce fraudulent filings and unauthorised access through strong authentication and verification processes.

3. Netherlands

This section highlights the effectiveness of the Netherlands' approach to digital identity and corporate verification, demonstrating a strong model that supports secure and efficient business operations both domestically and across the EU.

- The Netherlands employs eHerkenning, a business-focused digital ID system that facilitates secure access to government services, management of tax filings, and interactions with private entities like banks.
- This system is designed to ensure that corporate identity verification is robust, secure, and streamlined for various corporate activities.
- eHerkenning is fully interoperable under the eIDAS regulation, enabling Dutch businesses to securely interact and verify identities across the EU. This ensures smooth cross-border corporate transactions and compliance within the European Union.
- eHerkenning is widely adopted among Dutch businesses for both government-related transactions and increasingly in the private sector.
- This high level of adoption reflects the trust and efficiency of the eHerkenning system within the Dutch corporate landscape.
- The value chain involves a government-managed issuance of digital ID and integration with private banks and service providers, facilitating a comprehensive ecosystem for corporate verification.
- This setup ensures a seamless operation for businesses, from tax compliance to secure data exchanges.
- Providers include the eHerkenning system itself and private ID verification providers that support the infrastructure and enhance the security protocols.
- eHerkenning significantly reduces fraud in tax compliance and corporate transactions through its secure verification protocols.[36]
- Although specific fraud reduction figures are not provided, the system's design and integration into both governmental and private sectors indicate a robust impact on minimising tax fraud and unauthorised access to sensitive systems.

4. India

This section provides detail on how India utilises the Aadhaar-based eKYC system for corporate verification, which in turn supports the onboarding of businesses and corporate entities.

- The design integrates with India Stack APIs to enable secure, paperless processes for corporate identity verification, enhancing the efficiency and accessibility of verification services.
- The interoperability of India's corporate verification systems with international standards is currently limited but is progressively aligning with global requirements, especially in the financial sector for compliance purposes.

- There is high adoption of Aadhaar-based eKYC in the banking and telecom sectors, where it's primarily used for verifying corporate customers.
- The widespread application of Aadhaar eKYC is further supported by the significant number of transactions and interactions it facilitates. For instance, in April 2023 alone, over 250 million eKYC transactions were recorded, contributing to a cumulative total exceeding 14.95 billion transactions. This volume underscores the critical role of Aadhaar eKYC in enhancing transparency and improving customer experience across essential service sectors.[37]
- The value chain includes Aadhaar authentication APIs which are integrated with private platforms like the Goods and Services Tax Network (GSTN).
- This setup facilitates a robust system for corporate transactions and tax compliance, linking corporate entities directly with verified individual identities.
- Key providers involve the Unique Identification Authority of India (UIDAI) and various private technology firms that support the framework and ensure its functionality across different sectors.
- Aadhaar's integration into corporate verification significantly reduces tax evasion and the prevalence of shell companies by ensuring that corporate entities are directly linked to verified individual identities.
- By linking corporate entities directly to verified individual identities through Aadhaar, the government has strengthened the mechanisms to ensure transparency and accountability in business operations.
- The initiative has been part of broader efforts to tackle the challenges posed by shell companies, which are often used for illegal activities such as tax evasion. The Indian government has been active in identifying and striking off shell companies from the registrar. For example, between 2018 and 2021, a large number of companies identified as shell companies were struck off, indicating the scale of the government's crackdown on entities involved in obscuring ownership and facilitating tax evasion.[38]
- Moreover, the mandatory linking of Aadhaar for filing income tax returns was specifically implemented to prevent fund diversion to shell companies, aiming to curb the misuse of such entities for tax evasion and other fraudulent activities.[39]

5. Sweden and Norway

This section underscores how Sweden's and Norway's approach to digital identity and corporate verification through systems like BankID, Buypass, and Commfides provides a secure, efficient, and highly adopted framework that integrates seamlessly with international standards, significantly enhancing corporate operations and security.

- Corporate verification in Sweden and Norway is primarily facilitated through BankID, which provides businesses secure access to banking, tax, and government services. Norway also employs Buypass and Commfides for specialised corporate sectors, enhancing the security and specificity of services offered.
- This system design focuses on robust authentication mechanisms for financial transactions, tax compliance, and regulatory filings.
- BankID in Sweden boasts a high adoption rate, with 98% of the population using the service, which encompasses over 8 million users. This extensive adoption underlines the trust and reliability perceived by users and institutions alike.[40]

- Both countries' systems are integrated with eIDAS, ensuring interoperability for cross-border corporate transactions within the EU/EEA. This alignment supports seamless international operations and compliance.
- There is extremely high adoption of BankID in both countries, making it central to corporate interactions and essential for daily business operations.
- The widespread use reflects the system's efficiency and the trust it commands among corporates in Sweden and Norway.
- The value chain involves banks that manage ID issuance and integration with both government and private platforms. This ensures a streamlined process for corporate verification and authentication.
- The integration of these systems across public and private sectors ensures a comprehensive approach to managing corporate identities and transactions.
- Key providers include the BankID consortium, Buypass, and Commfides, which deliver the technology and infrastructure necessary for the robust functioning of these systems.
- Strong authentication protocols inherent in systems like BankID significantly reduce risks of tax fraud and unauthorised business activities.
- This enhanced security not only protects against fraud but also bolsters the overall security and reliability of corporate transactions within and across borders.

6. United States (U.S.)

This section highlights the decentralised nature of corporate verification in the U.S., which allows for innovation but also presents challenges in terms of interoperability, standardisation, and fraud prevention.

- Corporate verification in the U.S. is decentralised, with private-sector solutions such as ID.me and Clear playing a significant role in identity proofing for specific sectors (e.g., healthcare and banking).
- Some state-level initiatives exist for business verification, adding further layers to the system's fragmented nature.
- The U.S. has limited interoperability with unified international digital ID frameworks. The focus is instead on compliance with global financial standards for cross-border transactions and regulatory requirements.
- Moderate adoption overall, with around 50% of large firms prioritising digital identity authentication to streamline processes and enhance security.[41]
- Adoption is mainly driven by large corporations and financial institutions for regulatory compliance and onboarding.
- The value chain includes private providers (ID.me, Clear) and federal agencies like the IRS, which handles business verification, particularly for tax purposes.
- This structure reflects the reliance on private innovation and state-specific approaches to corporate verification.
- Key providers include private companies like ID.me and Clear, as well as state-level business registries and federal agencies.

- Enhanced fraud prevention is evident in corporate tax and financial transactions due to secure KYC practices.
- Despite these advancements, challenges remain; 84% of organisations experienced identity-related breaches in the past year, indicating ongoing vulnerabilities in fraud prevention.[42]

7. European Union (EU)

This section demonstrates how the European Union's strategic approach to digital identity and corporate verification provides a strong framework for secure corporate activities, ensuring interoperability and compliance both within the EU and in relation to global standards.

- The EU employs a cohesive design for corporate verification using eIDAS-compliant systems, including national eID and the upcoming EU Digital Identity Wallet, which will integrate additional corporate functionality.
- This system is designed to streamline corporate compliance, facilitate secure cross-border transactions, and enable digital signatures across member states.
- The EU's corporate verification systems are fully interoperable across the EU and are aligned with international data protection standards, enhancing global cooperation and compliance.
- There is high adoption in countries with established eID systems such as Estonia, with moderate adoption observed in others.
- The eIDAS framework has promoted secure cross-border corporate transactions, encouraging widespread uptake across the EU.
- The value chain includes public sector registration agencies, private banks, and service providers, all playing integral roles in the authentication and verification processes.
- This comprehensive approach ensures that all aspects of corporate identity verification are robustly managed.
- Providers include national overnments and trust service providers like Thales and Signicat, which support the underlying infrastructure and security protocols of the eID systems.
- The standardisation of authentication processes under eIDAS significantly reduces corporate impersonation and fraudulent activities, thereby enhancing the integrity and security of corporate operations within the EU.
- The specific impact on fraud reduction, while not quantified with precise data points, is noted as significant due to the uniform standards enforced across member states.
- It is also worth highlighting that the use of Legal Entity Identifier (LEI) as an identifier is mandated by a number of EU directives[43]. An LEI is a universal identification code unique to that legal entity or structure. When an LEI code is allocated to an entity, the code is included in a global data system. This enables every legal entity or structure that is a party to a relevant financial transaction to be identified in any jurisdiction. Global LEI adoption underpins improved risk management in firms and supports better assessment of micro and macro prudential risk. It also promotes market integrity, contains market abuse and financial fraud, and supports higher quality and accuracy of financial data overall.

Sources

1. Source: Home Office: Tackling fraud and rebuilding trust
2. Source: Home Office: Tackling fraud and rebuilding trust
3. Source: LexisNexis Risk Solutions: UK Firms Spend £21.4k Per Hour Fighting Financial Crime and Fraud
4. Source: Home Office: Tackling fraud and rebuilding trust CFIT has updated a Home Office 2019/20 figure of £4.4 billion for the estimated direct cost of fraud to the UK taking into account growth in fraud between 2019/20 and 2022/23 as well as inflation (ONS GDP deflator). See The Payment Services (Amendment) Regulations 2024 IA for fraud trends.
5. Source: Home Office: Tackling fraud and rebuilding trust Repeating the adjustments described in the footnote above produces a 2022/3 cost of £8.37 billion.
6. The proximity of Covid makes fraud trends unusually hard to interpret and CFIT has low certainty in extrapolations in the current environment.
7. Source: LexisNexis Risk Solutions: Tackling Financial Crime: The costs of inefficiency within the UK
8. Sources: The Little Book of Cyber Scams 2.0 and Action Fraud
9. Source: Cifas: Fraudscape 2024 - Cifas
10. Source: The Behavioural Insights Team / Nesta
11. Sources: Social Capital: The hidden wealth of nation (Haldane and Halpern 2025) and Trust, regulation, and market efficiency
12. Source: This is also the main harm identified from fraud reduction through derogation of same-day payment requirements in the impact assessment of that measure. See The Payment Services (Amendment) Regulations 2024
13. Source: A verified digital identity for individuals as defined under the UK digital identity and attributes trust framework.
14. Source: Enabling the use of digital identities in the UK - GOV.UK
15. Source: ONS: Crime in England and Wales - Office for National Statistics
16. Source: Fraud Strategy, Home Office 2023
17. Source: LexisNexis Risk Solutions: UK Firms Spend £21.4k Per Hour Fighting Financial Crime and Fraud
18. Source: FCA: What we do
19. Source: FCA: Enhancing market integrity
20. Source: The Liminality of Fraud: Reimagining Fraud Theory to Inform Financial Crime Prevention
21. Source: The Behavioral Insights Team
22. Source: Springer Nature: Trust, regulation, and market efficiency
23. Source: Bowling Alone: The Collapse and Revival of American Community 2000
24. Source: Lewis Carroll, Alice in Wonderland
25. Source: Deloitte: "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking"
26. Source: CNN World: Finance worker pays out $25 million after video call with deepfake 'chief financial officer'
27. Source: Action Fraud: The Little Book of Cyber Scams 2.0
28. Source: Data (Use and Access) Bill
29. Source: Gov UK: Economic Crime and Corporate Transparency Act: outline transition plan for Companies House
30. Source: FATF: United Kingdom
31. Source: The Times: More than half of public support digital ID cards
32. Source: HM Treasury: National Payments Vision
33. Source: Regula: The New Imperative: Digital IDs
34. Source: Republic of Estonia Government: e-Residency factsheet
35. Source: Republic of Estonia e-Residency: Do business securely
36. Source: Government of the Netherlands: Tackling tax evasion
37. Source: Ministry of Electronics & IT: Aadhaar authentication clocks 1.96 billion transactions in April

38. Source: Taxguru: Government identified 2,38,223 companies as shell companies
39. Source: Oneindia: Made Aadhaar mandatory to prevent fund diversion to shell companies
40. Source: Innovatrics: "We enabled a whole digital ecosystem in Sweden – from eGovernment to a cashless society," claims Jonas Brännvall from BankID.
41. Both the Directive 2014/65/EU (MIFID 2), which entered into force on January 3, 2018, and the directly applicable Article 26 of Regulation (EU) No. 600/2014 (MIFIR) require all investment service providers to report on transactions with publicly traded securities. The European Commission's Implementing Regulation (EU) 2017/394 requires securities registrars to identify all legal entities via an LEI code.
42. Source: PYMNTS: Half of Large Firms Are Focused On Digital Identity and Authentication
43. Source: IDSalliance: New Study Reveals 84% of Organisations Experienced an Identity-Related Breach in the Last Year

CFIT | Centre for Finance Innovation and Technology

cfit.org.uk

X.com/CFIT_UK

linkedin.com/company/cfituk