



From Fintech to Ubiquitech: Accelerating the wider UK Digital Economy

Authored by a working group led by Dr. Ruth Wandhöfer

From Fintech to Ubiquitech: Accelerating the wider UK Digital Economy

Authored by a working group led by Dr. Ruth Wandhöfer

Mar 21, 2024.

Table of Content

Foreword - Rt Hon Lord Mayor of London Alderman Professor Michael Mainelli

Foreword - Chair, Ubiquitech Group

Executive Summary

1. Introduction: From Fintech to Ubiquitech

2. Rationale for this Report

3. Vision and Objectives

4. High-Level Recommendations

4.1 Cyber Security and Fraud Controls

4.2 Network, Systems and Processes

4.3 Digital Systems in Trade

4.4 Verification and Authentication of Users, Entities and Assets

4.5 Delivering Digital Skills Education and Inclusion

5. Legislative and Regulatory Backdrop

6. The role of the United Kingdom and its USPs in the Global Digital Economy

6.1 Enabling Legislation

6.2 From Open Banking into Open Finance and Smart Data

6.3 Common Law and Common Wealth

6.4 Global Financial and Insurance Centre

7. Conclusion and Next Steps

Annex A – Detailed Ubiquitech Recommendations

Annex B – In Depth Inhibitors to a successful transition towards the Ubiquitech Digital Economy

Annex C – The Ubiquitech Group

Foreword

My theme as Lord Mayor - "Connect To Prosper" - focuses on leveraging the City of London's strengths and connections to tackle global challenges and seize new opportunities. The shift from Fintech to Ubiquitech (i.e. Ubiquitous Technology) presents a golden opportunity for the City and the UK.

Home to 40 learned societies, 70 higher education institutions, 130 research institutes, and over 24,000 businesses, including some of the world's most innovative tech firms, the Square Mile is truly unique. We have world-renowned financial services, an enabling legal and regulatory environment and access to incredible talent and skills. And the UK has been a pioneer in the use of Open Banking, with adoption reaching almost eight million active users, including almost a fifth of the UK's SMEs.

Having established itself as Europe's Fintech hub - attracting more Fintech investment than the next 13 European cities combined - the City of London ecosystem can show new leadership as the global digital economy evolves to the point where smart data is used across all aspects of the economy.

The economy of the last 20 years has been driven by mobile, social platforms, and the cloud. The next 20 years will be driven by smart economic networks based on artificial intelligence, open data, and shared ledgers. Countries that embrace this next wave of efficiency and effectiveness will prosper by increasing productivity and trust, while reducing cost: creating a simpler, smoother, more secure system for customers and businesses that will make our lives easier and our money safer.

If flows of data are the lifeblood of our economy, standards are its beating heart. So, as part of "Connect To Prosper", we have launched the 695th Lord Mayor's Smart Economy Networks initiative, which is well underway and bringing together City and global institutions to kickstart the inception of international "open data" standards via development of prototypes.

As we outlined in our Vision for Economic Growth report, collaboration among government, industry, academia and international partners is essential for a fully integrated and inclusive digital society.

Building on the roadmap for the UK Fintech sector set out in the Kalifa Review (2021), From Fintech to Ubiquitech is a timely and welcome intervention outlining the steps we need to take to harness the full potential of digital innovations across all sectors. These include; building consumer and organisational trust in the digital economy; accelerating digital verification solutions across a range of products and services, which could benefit businesses and consumers up to £4.8 billion by 2030; and investing in education and infrastructure to ensure everyone can benefit from the digital transformation.

By drawing on the City's unique strengths and connections and collaborating across different groups, we can ensure London is at the vanguard of the fourth Industrial Revolution.

The Rt Hon The Lord Mayor of London Alderman Professor Michael Mainelli

Foreword

The digitisation of economies around the world changes how citizens engage with governments, how businesses operate, what types of products are being produced and how these all flow within and across markets.

Starting with the Fintech payments revolution, we have already seen how payments and money itself is transforming, bringing new opportunities and risks and impacting consumers, businesses and Government. This for me was the starting point. But we are at a point where we need to ask ourselves, how can we truly embrace a Digital Economy with digital money and a plethora of digital services being bought and sold, if we still lack ubiquitous network coverage, the ability to access services and in some cases the financial and digital education necessary to do so?

Taking the step from digital payments to the boarder Digital Economy is essential. With the Kalifa Review on Fintech we already have some key initiatives in play to support the sustainable growth of this new business class across the UK. However, against the backdrop of several new key legislations that have been adopted, the UK is now in a position where it needs to reflect on how to best embrace these opportunities of change and turn them into global leadership, moving from Fintech to Smart Data and into Ubiquitech (i.e. Ubiquitous Technology), across all aspects of the economy. And the Ubiquitech Report is there to help in taking those practical steps that will accelerate the transformation of the UK into a comprehensive Digital Economy that sets the standard for the rest of the world.

Let us all move forward into the Digital Age of Ubiquitech.

Dr. Ruth Wandhöfer

Chair of the Ubiquitech Group

Executive Summary

The future of the UK digital economy is at a critical juncture, demanding a paradigm shift in thinking and a call to action for investment and industry collaboration. To develop a positive, sustainable, inclusive, and accessible Digital Economy for all we need an urgent focus on digital investment and strategic cross industry collaboration to help deliver for the next generation of UK citizens. Following the Kalifa Review of 2021 into supporting the Fintech and Regtech markets building on Open Banking, we now stand at the juncture of all Smart Data taking this further forward be it in Healthcare, Agriculture or any other sector.

One of the recommendations of the Kalifa Review was the formation of a Centre for Financial Innovation and Technology (CFIT) and only in March 2024 CFIT's first report estimated efficiency savings for the UK of £ 30.5 billion should Open Finance be taken forward more widely.

Our central premise in this Ubiquitech Report is that the UK is now ready to move from a Fintech revolution to a Ubiquitech revolution as universal technologies reach maturity. Whilst this Report has not estimated the efficiency savings for the UK across the board, it would appear logical of these to be of even greater magnitude, particularly in areas such as Healthcare. Failing to act on this agenda puts the UK economy at strategic risk of falling further behind other nations with ambitious digital agendas, negatively impacting the standards of living of every citizen.

Key drivers for the paradigm shift are outlined, including the shift towards digital human interaction, the challenge to competitiveness posed by potential complacency and the essentiality of sustainability. We believe the Ubiquitech Report underscores the urgency for recent and forthcoming enabling legislation to leverage the digital future and the imperative need for enhanced security measures in the face of escalating fraud and cybercrime.

The arrival of Web3 and decentralisation furthermore necessitates a complete overhaul of existing digital operating models. This Report stresses the inadequacy of current systems and processes rooted in a paper-based past, calling for a radical shift towards real-time identity verification and authentication in the digital age.

The contributors of the Ubiquitech Report advocate for a new paradigm in data management and usage, emphasising the uniqueness engendered in digital representations and the need for a redefined approach to law. The future success of the UK Digital Economy hinges on embracing these transformative shifts in infrastructure, operations, and financial models to stay competitive in a rapidly evolving digital landscape.

Our Recommendations cover five key pillars and are summarised here below.

- **Cyber Security and Fraud Controls:** Consumer and organisational trust in the digital environment is of paramount importance and must be the Government's core concern.
- **Network, Systems and Processes:** It is axiomatic to note that for Ubiquitech technologies to thrive there is an underlying requirement that ubiquitous network coverage and connectivity is achieved.
- **Verification and Authentication of Users, Entities and Assets:** A crucial component of any trust framework is the confidence in identifying the relevant parties and the confidence in a liability framework when errors occur.

- **Digital Skills Education and Inclusion:** For the Digital Economy to be successful and comprehensive all areas of society should be comfortable in their understanding and abilities to exploit the benefits on offer.
- **Digitising International Trade Systems:** Moving beyond the purely Digital Economy, reforms to digitise and optimise the movement of physical goods are also necessary to streamline both financial systems and supply chains.

The Ubiquitech Report highlights how the UK, and the City of London ecosystem in particular, can take advantage of our world renowned legal, regulatory and standards environment, combined with our technological, scientific and knowledge expertise to drive the 4th Industrial Revolution from these shores. This is truly a Carpe Diem moment for the UK as a Global Trust Hub and Centre of Excellence in Innovation across the board.

1. Introduction: From Fintech to Ubiquitech

The Ubiquitech Report is focusing on how we can advance the UK Digital Economy by leveraging emerging legislation, industry initiatives as well as new funding models that would enable citizens, businesses and government to securely connect and transact in a ubiquitous and efficient way.

With fast-moving legislation on an international level, it is time for the UK to reinforce and expand its role as the Global Hub for future technologies and professional services, moving beyond current dominance in Fintech to leading the way to the future Ubiquitech ecosystem.

Whilst all nations are revising their legislation to take in to account the needs to regulate Artificial Intelligence, emerging cyber security threats and optimise transparency of international corporate structures to prevent sanctions circumvention, the UK has a unique opportunity in aligning the otherwise disparate legislative developments elsewhere as we discuss in great detail in the below section on legislation.

2. Rationale for this Report

The rationale behind the Ubiquitech Report is encapsulated in the key driver identified that have led to a complete paradigm shift from Electronic to Digital Economies with all the threats and opportunities that are associated to this for the United Kingdom.

This paradigm shift calls for coordination and appropriate action between different Government departments, industry and regulators. All of these stakeholders need to appreciate their role in influencing the economic growth opportunities that can be afforded by Ubiquitech. Too many piecemeal reviews and pilot activities have led to a disjointed and suboptimal approach from Government, industry and across consumer society to the detriment of delivering an operationally effective Digital Economy in the UK and the opportunity for the UK to deploy, leverage and export this model globally.

3. Vision and Objectives

Our vision is to create an inclusive and prosperous Digital Economy and society for the UK. In order to achieve this, we need to identify the current barriers that are holding the UK back, propose ways to remove these barriers as well as develop a digital infrastructure approach and model that can achieve these objectives. A common denominator will need to be found in order to truly enable ubiquitous access.

The ultimate benefits of a digitally connected UK society will deliver a significant boost to efficiency, the successful reduction and mitigation of financial crime and identity theft, highly secure access to a ubiquitous data infrastructure for individuals, businesses and government and the acceleration of new business models, which are all enabling factors for economic growth.

4. Key Recommendations

The Ubiquitech Report highlights how the UK, and the City of London ecosystem in particular, can take advantage of our pragmatic and well regarded legal, regulatory and standards environment, combined with our technological, scientific and knowledge expertise to drive the 4th Industrial Revolution from these shores. This is truly a Carpe Diem moment for the UK as a Global Trust Hub and Centre of Excellence in Innovation across the board. As the Kalifa Review identified, the Fintech industry in the UK has been seen globally as a great success and Ubiquitech has the capacity to extend this commercial success into all other technological field and sectors of the economy.

4.1 Cyber Security and Fraud Controls

- Ubiquitech will become the binding force across all Critical National Infrastructure (CNI) and as such the cyber security and fraud standards adopted to protect it must surpass any protections currently deployed to ensure that it thrives.
- With Smart Data under the DPDI building on Open Banking these new security and fraud controls, themselves enabled under DPDI ECCT et al, need to be actively promoted across Government, Regulators, Law Enforcement and the Private Sector. The City of London Corporation and the City of London Police (as lead authority) are well placed to play a catalyst role in the context of supporting industry's adopting of greater financial crime intelligence sharing.

4.2 Network, Systems and Processes Recommendations

- It is axiomatic to note that for Ubiquitech technologies to thrive there is an underlying requirement for ubiquitous network coverage and connectivity to be achieved. Network coverage and access form an integral part of what we call Ubiquitech, without which there will be no Digital Economy in the UK.

4.3 Digital Systems in Trade Recommendations

- With the dominance of English Common Law in global trade flows the UK's strengths in legal and professional services supporting such trade and the UK's first mover advantage in designing the 'Reliable System' to support it digitally, this is a natural area for the UK to exploit on the global stage.

4.4 Verification and Authentication of Users, Entities and Assets

- At the heart of the Digital Economy is the requirement for any systems to reliably assert that the individuals, entities and assets are actually as claimed in the fight against fraud and other forms of financial crime.
- Building on existing banking standards and integrating multi-modal biometrics, i.e. a combination of different biometric elements used in customer authentication, within a more robust strong customer authentication regime will enable us to not only crack down on existing abuses of the

financial systems around the world but provide consumers and organisations with the confidence to adopt digital services to enable them to take full advantage of the Digital Economy. Many believe that such measures could actually lead to Open Banking helping towards a cure for cancer.¹

4.5 Delivering Digital Skills Education and Inclusion

- Education, training and apprenticeships should always be future focused to ensure that society is appropriately skilled, for example currently Web3 skill-sets and education should be part of the training. Digital skills must form part of the school and university education, and also part of reskilling and upskilling of the existing workforce to address both pipeline and incumbent workers being dislocated in the current digital disruption.

¹ For further details see: 'Redecentralisation: Building the Digital Financial Ecosystem', Ruth Wandhöfer, H. Al-Nakib, Palgrave MacMillan, 2023 (ISBN 978-3-031-21590-2).

5. Legislative and Regulatory Backdrop

In this section we will provide an overview of what we consider to be the key legislative and regulatory building blocks that will assist in shaping the UK Digital Economy toward the state of a truly Smart Economy through the adoption of Ubiquitech.

a. Economic Crime and Corporate Transparency Act (ECCTA)

Whilst one focus of the ECCTA is to clamp down on loopholes left open in the earlier Economic Crime and Enforcement Act, perhaps the most important aspects of the ECCTA are the introduction of the new offence of 'failure to prevent' and the reform of Companies House. The former radically changes the motivation of businesses to more proactively engage in economic crime prevention, psychologically turning current reactive Suspicious Activity Reporting on its head. The latter, if implemented correctly, has the potential to take the best parts of the current Companies House regime, with its internationally renowned transparency and searchability that is of so much use to the economy as a whole, and to layer on top the probity and certainty that the information will be accurate and reliable. However, as with the rest of the UK's legislative stable this will require provisions of the Data Protection and Digital Information Bill (DPDI) to be dovetailed effectively. Whilst the DPDI could be called the 'One Bill to Rule them All', we cover it last in this section precisely because it is the glue that can enable the Ubiquitech vision to be optimally realised.

From a pure economic crime angle the 'failure to prevent' will promote more effective sharing of financial crime data and intelligence between organisations, and not just organisations within the traditional economic crime space, as we discuss under the Online Safety Act below. The provision of a 'recognised legitimate interest' to share data within the DPDI is a critical step forward and the position, explicitly, to link such recognised interest and failure to prevent will provide the certainty that is necessary for inter and intra industry confidence.

Within Companies House reform, the need to tighten Identity and Verification (ID & V) controls to ensure robust data are welcome, though at the same time Companies House statements on their intention as to how this will be carried out are disappointing, both in their timescale and security standards. Disturbingly in evidence to the Business and Trade Committee on 7th February 2024, it was noted that ID & V would be adopted in 'early 2025', giving organised crime a full year to continue exploiting the gaping hole that the Act was supposed to address. A further year before adoption for existing companies leaves even more time to exploit the loopholes. More disappointing still, however, was the reference to Companies House looking to work with the Government Digital Service and their One Log In for technical 'security' standards, which fall well short of current minimum standards for the financial services industry, themselves insufficient to adequately protect consumers payments, and, under Ubiquitech, all other forms of Smart Data that will build on existing Open Banking.

From a UK Plc perspective, the more robust adoption of controls at Companies House is an urgent operational requirement, as the Ministry of Defence might put it, so that identification and verification of Directors, Persons of Significant Control and Ultimate Beneficial Owners can be effectively managed to ensure a resilient global Corporate directory of directories, spanning all global trade.

As noted in the International Regulatory Strategy Group (a joint body comprising the City of London Corporation and The City UK) *'There is general agreement that an international register is a good idea, but the practicalities of actually effecting it are likely to be what becomes the issue. Therefore, while an international register is the desired end goal, an intermediate goal is to have standardised national registers which are similar.'*²

Following the central theme of this Ubiquitech Report, the provision of a reliable ecosystem to ease international trade and financial systems is within reach and the UK is uniquely well positioned to take advantage of this.

Again, to cite the IRSG report *'the building blocks for international coherence in the financial sector have already begun to be laid. The Legal Entity Identifier (LEI), for example, is the first global and unique entity identifier, created as a reference code to be used across markets and jurisdictions to allow for unique identification of legal entities that engage in financial transactions. Tools such as LEI are designed to enable regulators to identify parties to financial transactions immediately, and accurately. There is clearly an increasing awareness of the needed for consistency and global standards across multiple strands of the financial sector.'*³

With regard to identification of individuals and the ability to strongly authenticate customers, financial services again provide a lead, and as DPDI notes, all Smart Data applications such as those envisaged under other legislation can build on Open Banking.

b. Online Safety Act (OSA)

In the particular context of 'BigTech', the OSA outlines manners in which existing and potential threats and concerns can be reined in, in order to provide greater safety and security for users as well as sharing the burden across industry verticals for the damage frequently channelled through other platforms, in particular Social Media. During the FCA/PSR Authorised Push Payment (APP) Scam Tech Sprint in October 2022, every team on the sprint identified that it was less the sharing of information between financial institutions that needed to be streamlined, though this was of course a concern, and more important was the timely access to Social Media and Telco data. Access to Social Media and Telco data in relation to scams was deemed a higher priority and more effective approach.

Figures put forward at the time were that 80% of all Authorised Push Payment (APP) scams had involved Social Media platforms owned by Meta. More recent figures from one individual institution were lower, at 60%, but certainly evidence suggests that this is the majority of cases. Co-ordinating across industries, and availing ourselves of the 'failure to prevent' under ECCT, and the 'recognised legitimate interest' under DPDI, with sharing responsibilities across industry verticals has the potential to be a game changing approach to tackling not only financial crime, but ensuring the consumer trust that is essential for the Ubiquitech vision to be realised. The City of London Police, as the UK lead force in financial crime, have a unique role to play in fostering such developments, and the Lord Mayor's convening role again becomes a key enabler.

² Anti-money laundering (irsg.co.uk)

³ IRSG, Ibid

c. Electronic Trade Documents Act (ETDA)

The ETDA is arguably the most important piece of legislation that you have never heard of. Enabling electronic documents to have equal legal standing to paper documents in international shipping manifests, or 'Bills of Lading' may not prima facie sound like the most exciting legislative reform, but, the practical ramifications of it for the UK and its potential dominance of the forthcoming Ubiquitech revolution are unprecedented.

As one of the first Jurisdictions to give such equal legal standing, the UK is in position to drive Global Standards, not just by virtue of the British Standards Institution's renown in cyber security standards, but also due to the simple fact that 80% of all Bills of Lading globally are written under English Common Law. The ability to securely identify the 'Trusted Trader' through their Legal Entity Identifier, into the tracking of the goods in transit at sea, with the contents of those containers reliably tied into the financial system through, again UK originated Open Banking is estimated (International Chamber of Commerce) to be worth anything up to 10% of Global GDP. The UK previously led in global freight tracking projects such as the post 9/11 Smart and Secure Trade lanes initiative and delivery of materials to front line combatants in war situations.

d. Data Protection and Digital Information Bill (DPDI)

The 'One Bill to rule them All' is the DPDI, which has the potential to effectively become the glue to optimise all of the other recent Acts that have been passed.

Each of the above Acts and Bills essentially live or die according to the manner in which they can effectively handle data, and it is the provisions within the DPDI that must dovetail to allow effective and joined up Government and Governance.

As with the Digital Markets, Competition and Consumer Bill (DMCC), the Bill is currently in the House of Lords and started at Committee Stage on 20th March 2024. Recommendations within this Report will be shared with Parliamentarians to inform debate during Committee and subsequent stages in the passing of the Bill.

Without clarification on the data handling aspects within the DPDI, few of the aforementioned Acts can reliably enforce their own provisions, whether that be the nature of 'Identification and Verification' of Directors and PSCs within ECCT, the financial crime 'intelligence sharing' within the same Act, or the nature of a 'Reliable System' under ETDA.

Key clauses in the Bill, for example, include the provision of 'Recognised Legitimate Interest' in sharing data for purposes such as the fight against economic crime. Should the DPDI signpost explicitly to ECCT and the 'Failure to prevent' such crime, then the pendulum would swing from the current industry default position of limited sharing of intelligence to a far more effective position of increased sharing of intelligence becoming the default position, enabling more effective public private partnerships to flourish.

Equally, and by extension from the OSA, this public private partnership could extend across industry sectors, allowing Telcos and Big Tech to join law enforcement and financial services firms in the fight against organised crime.

Furthermore, with the ETDA offering opportunities for trade finance to more effectively leverage the currently illiquid assets stranded in the physical supply chain, the opportunity for Bills of Exchange to be raised from the newly digitised Bills of Lading provides a whole new asset class within trade finance. Whilst there has been debate as to whether such 'utility tokens' might be Regulated by the FCA, or international counterparts, the financial crime approach again provides a useful example. Given that such Bills of Exchange would now have an inherent and transferable value, then they would, as FinCen put it in their clarification on Cryptoassets back in 2021, be a transferable 'Store of Value' and thus be subject to US Anti-Money-Laundering (AML) controls.

The ability to release some of the currently estimated \$25 trillion of assets locked up in supply chains could likely be an attractive and lucrative market for the UK to explore.

The Bill explicitly states in its Regulatory Impact Assessment that Smart Data classes should build on the success of Open Banking Application Programming Interfaces (APIs), and as was covered extensively in the FCA Open Finance Policy Sprint in 2022 this will provide a requirement for a Consent Dashboard, as we discuss later in this White Paper. The Consent Dashboard will allow a consumer, newly empowered under the DMCC and further protected under OSA to realise both the monetary benefits and opportunities of their data rather than the current situation where this is generally realised only by current incumbent providers.

It has often been remarked that either 'Data is the new oil' or 'Identity is the new oil' etcetera, but what is indisputable is that this ability for consumers to realise the value of their data is likely to help drive adoption of digital. This in itself could create new asset classes every bit as ground-breaking as the ETDA's potential Bills of Exchange.

6. The role of the United Kingdom and its USPs in the Global Digital Economy

The UK has Unique Selling Propositions, especially the City of London's global advantages, which can play such a central role in moving the UK towards Ubiquitech. Whilst many of these points are well rehearsed, this Report believes that the existing in-built advantages can have a dramatic multiplier effect as Trust Services expand into new sectors.

6.1 Enabling Legislation

It is the combination of the new legislation, listed in the previous section, that will enable the United Kingdom and the City of London more particularly to take advantage of a coherent and streamlined regulatory approach to facilitate the balanced ecosystem that London has taken advantage of in the Fintech revolution and to reinforce that leadership and extend it into other sectors of the economy and overall society.

The fact that the DPDI will establish Open Banking data sharing standards for the wider economy demonstrates the foundational role of the UK's financial services industry and thus the City of London.

On 7 September 2023 the City of London Corporation launched its report *Vision for Economic Growth – a roadmap to prosperity*. Its focus is on the evolution of the financial and professional services sector. Its objectives are delivered through a series of Big Moves, or strategic reforms, that are designed to create transformational change over time. Economic growth identified within the report was estimated at being £225 billion (note that, whilst there will be some overlap with savings identified, the C4DTI report identified £224 billion in efficiency savings - the closeness of these figures is a coincidence). One of those Big Moves focused on investment in driving an innovation and growth mindset across government, regulation and industry. The report identified that the Digital Regulation Cooperation Forum (DRCF) is already working across silos more effectively, adding that the DRCF "should be given appropriate resources and an even stronger mandate to drive regulatory coordination for digital issues. It should focus both on strategic outcomes and operational efficiency, aligning reporting requirements across regulators." This move will serve as a key enabler for innovation across the UK, and support delivery of some cornerstone innovations

Specifically, we would like to see enhanced DRCF governance – to deliver greater regulatory clarity, reduce risk of duplication, and advance regulatory capabilities. This should include:

- Annual report including a plan for the year ahead
- Transparency around existing rules and role of DRCF
- Transparency around existing DRCF interface with Cabinet Office; Parliament; other financial services regulators
- A DRCF self-assessment of what a strong mandate would mean

6.2 From Open Banking into Open Finance and Smart Data

The UK has been a pioneer in the use of Open Banking, with adoption reaching almost 8 million active users, including almost a fifth of the UK's Small and Medium Enterprises (SMEs). The 2023 Autumn Statement demonstrates the Government's unwavering support to take full advantage of this innovation and will ensure we realise its full potential. As part of its commitment to unlock the full potential of Open Banking, the Government announced the intention to legislate Open Banking over the next year. This will enable the new regulatory framework to require firms beyond the largest banks to participate in Open Banking, effectively expanding Open Banking beyond the CMA 9. As noted earlier, CFIT have recently estimated GDP growth of £30.5 billion as a result of such Open Finance efficiencies, a boost of slightly over 1%.

Cited in the *End of the Implementation Roadmap Report: Recommendations for the Future of Open Banking*⁴, one of the impediments to progress has been the absence of a clear cross-department vision for developing the UK into a Smart Data economy, where people and businesses have rights to access their data, wherever it may be held, and benefit from a wide range of new choices and innovations.

We support the Government's commitment to unlocking the full potential of Open Banking-enabled payments and proposal to legislate this year to support this. The Government's intention for the new regulatory framework will require firms beyond the largest banks to participate in a sustainable and equitable commercial model through which the technology and necessary consumer protections will be developed, and with appropriate regulatory backstops. This provides some assurance to the future of Open Banking in the UK. We understand that HMT and the FCA sees this as the route to also advancing Open Finance. This is an important next step in policy. There should be clarity around the interface function between Open Banking and Open Finance and the 'Smart Data Big Bang' announced in the Autumn Statement 2023.

The role for the DPDI in advancing Open Finance is clear. The government will publish a National Payments Vision in 2024. Building upon the Future of Payments Review's findings⁵, this should include consideration of priorities for UK payments, working with the Payment Systems Regulator (PSR) and the Bank of England. This should also include a formal government acknowledgement of the role for Digital Identity in payments, and crucially the role of Strong Customer Authentication by Third Party Providers for access to accounts or other smart data sets. Despite UK leadership in the technical security aspects and the existence of specific British Standards in this regard, adopted by UK Finance⁶ as meeting their obligations to the PSR in 2018, these have not been fully implemented to date creating a significant security risk. The UK expertise in cyber security and biometric systems again adds to the UK USP, and needs to be fully realised in order to effectively protect data and support trust in data access and sharing.

⁴ Open Banking, "Trustee End of Implementation Roadmap Report", <https://www.openbanking.org.uk/wp-content/uploads/FINAL-Trustee-End-of-Implementation-Roadmap-Report-30-January-2023-Final-Searchable.pdf>

⁵ UK Government, "Future of Payments Review 2023", <https://www.gov.uk/government/publications/future-of-payments-review-2023>

⁶ September 2018, British Standards Institution Publicly Available Specification in Digital Identification & Strong Customer Authentication (PAS499)

Developing Open Finance as a branch (or branches) of a harmonised Smart Data Framework is a complex process. However, with the right structure, incentives, and governance in place, it has the potential to revolutionise the financial sector, offering consumers and SMEs more control, security, and choices. As Open Finance evolves, collaboration across stakeholders will be essential in addressing challenges and unlocking its immense potential. While barriers exist, the potential benefits of open finance in terms of innovation, competition, and consumer empowerment are significant. Overcoming these challenges requires collaboration between regulators, financial institutions, Fintech companies, and other stakeholders. The UK's experience with open banking offers valuable lessons and a foundation upon which to build.

The City of London Corporation's Vision for Economic Growth report underscores the significant economic potential of digital verification, projecting a £4.8 billion boost to the UK economy from 2024 to 2030 through digital service transformation and fraud loss mitigation. Widespread adoption is expected to not only safeguard against £3 billion in fraud losses but also to act as a catalyst for new financial and cross-sectoral services, adding further substantial value. Concerns have been raised over the years, including the Treasury Select Committee, that there has been a dramatic under-reporting of fraud historically, and given academic estimates that between 9-12% of the UK economy may be 'hidden' criminality, figures in single figure billions, whilst seemingly large, would be a very small proportion of a more than £200 billion black market if fraud is also believed to account for around half of all crimes.

Digital verification is pivotal for transitioning to a fully digital economy, enhancing security, streamlining transactions, reducing costs, and fulfilling KYC obligations. It's also foundational to AI assurance infrastructure. The global market for Digital Verification was valued at \$10 billion in 2022 and is expected to grow to \$29.3 billion by 2028, reflecting a compound annual growth rate (CAGR) of 19.6%. This growth is driven by key sector players through R&D and strategic collaborations, offering both single-factor and multi-factor authentication products.

In the UK, the financial services sector, as part of the global market, benefits significantly from digital verification, with the Banking, Financial Services, and Insurance sectors accounting for over 28% of the market revenue share in 2022. The shift towards digital banking services necessitates secure verification, critical for access control and enhancing customer experiences. The sector's use of digital verification varies, with regulatory compliance, technological advancements, and consumer preferences key drivers.

Regulators should adopt an innovation and growth mindset to provide collective leadership on priorities like secure authentication, and as financial sectors and institutions increasingly rely on such technologies, the need for agile, coherent regulatory responses becomes imperative to maintain competitiveness and resilience.

6.3 Common Law and Commonwealth

London's Commercial Courts remain a preferred destination for international dispute resolution. English law provides the legal basis for many international jurisdictions, comprising an estimated 40% of all governing law in global corporate arbitration. 77% of UK Commercial Court claims in 2019 involved at least one party outside England and Wales and 43% of claims involved parties all located outside England and Wales.

Most insurance, derivatives and commodities trading contracts globally are written in English law, covering trillions of pounds of financial transactions each year. English law supports business ambitions, it is visionary and progressive, and it has the support of a robust court, arbitration and disputes infrastructure. London is the home of English law, and companies based here have access to its top practitioners. Companies based in the UK also benefit from formation, restructuring and insolvency laws, and UK regulations. As previously noted, the IRSG AML report outlines that in the absence of a global register and a globally agreed approach the next best step is to build on agreed standards, such as LEIs, and the UK and London are uniquely well placed to provide such global common standards. However, we believe that the UK is well placed to unilaterally offer a Global Register, leveraging our reputation as a Trust Third Party in international law, arbitration, insurance, and standards.

6.4 Global Financial and Insurance Centre

Per data from *City of London Benchmarking (2024)* and the *State of the sector: annual review of UK financial services (2023)*, the UK's Financial Professional Services (FPS) industry is world leading and robust. It employs 2.4 million people, generates 13%, or £294bn, of UK GDP and contributes £100bn to UK taxes. Financial services (FS) workers generate an average of £177,000 in economic output, making them some of the most productive workers in the UK.

The 2024 City of London Benchmarking analysis shows that London is the top Global Financial Centre (GFC) in the world. London's overall competitiveness score in 2024 is the same as it was in 2023, but the score of each of the underlying dimensions has changed. For example, a decline in the 'reach of financial activity' dimension is offset by gains in the 'enabling regulatory and legal environment' and 'talent and skills' dimensions. Bottlenecks in business activity caused by Brexit and the COVID-19 pandemic have been cleared – regulatory efficiency, immigration policies and workers returning to the office have all improved London's business ecosystem. This position cannot be taken for granted, however. Some of the fundamentals driving the growth of financial services are in decline.

London also improved its score in the 'enabling legal and regulatory environment' dimension. The UK regulatory regime is highly regarded around the world and ranks second in our analysis. Singapore ranks in first place due to its proactive and market-aware regulatory approach. Although the UK and Singapore financial industries share similarities – both are international finance hubs – the UK is a far larger global market and also has a large sophisticated domestic market. Balancing domestic consumer protection with wholesale global finance players does not allow for a one-size-fits all regulatory regime however, something UK regulators must address to improve competitiveness.

The UK's FPS industry is an essential cog in one of the world's most innovative ecosystems. It drives growth and enables effective investment, while supporting innovative solutions to global challenges. FPS supports the tech industry and helps to achieve sustainability targets through capital allocation, deal-making, legal and accounting services, and providing the insurance necessary to drive ground-breaking projects. Businesses located in the UK benefit from a globally connected market, highly-skilled domestic and international talent, both domestically and from around the world, and a supportive and ambitious policy environment.

As Kalifa noted, the UK is at the cutting edge of Fintech developments, and has been a world leader in innovative payments systems, regtech, insurtech and cyber security and can now move

towards being the global leader in Ubiquitech. It is the leading Fintech centre in Europe – London attracts more Fintech investment than the next 13 European cities combined. The UK's FPS industry helps ambitious new companies to thrive by providing an established customer base, as well as the financing and services to succeed.

The UK is the world's largest net exporter of financial services. Net FS exports reached a record £72bn in 2022. The US comes in second with £59bn of net exports in 2022. However, these decreased by 2% year-on-year, as exports fell by 3% and imports fell by 4%. The US saw net FS exports fall by 13% in 2022 as exports fell by 2% and imports increased by 7%. The UK is a beneficiary of this trend as UK FS exports to the US increased by 4%. The US continues to be the largest market for UK FS exports, accounting for a 34% share.

The UK is the world's leading international asset management hub with £4.2tn managed for overseas clients, and Foreign Direct investment in UK FPS reached £2.1bn in 2022 and created 15,000 jobs. The UK is a top destination for FPS FDI with a 68% increase in capital invested compared to 2021, and 39% more projects.

The UK is still the largest centre for international bond issuance, but the value of outstanding international bonds in the UK fell 5% in 2022 to US\$3.2tn. The US was more than US\$800bn behind, in second place.

The UK is the world's leading financial centre in terms of cross-border banking activity. It had US\$5.3tn of cross-border banking claims (15% global market share) and US\$5.4tn of cross-border liabilities in Q4 2022. Japan ranks second with 12% market share, followed by France and Germany with 11% and 10%, respectively.

London remains the world's largest centre for FX and OTC derivatives trading. The UK uses its advantageous position between Asia and the US to be the world leader in FX trading. In 2022 London handled a daily average of US\$3.8tn in FX trades, double New York (the next largest centre) which saw daily average volumes of US\$1.9tn.

London is also a global insurance hub. The London Market is the largest specialist insurance market, and the UK is the third largest insurance market in the world. The US ranks top in the insurance world with 43.7% market share and over £2.5tn of premium volume in 2022, driven in part by the size of the domestic market. The UK is the third largest market, by total premium volume (£305bn in 2022). Insurance premiums in the UK fell by 2.8% in 2022, and market share dropped 0.1% points to 5.4%. The London Market for specialist insurance is world leading, however. It covers 42% of global marine, aviation and energy insurance, and is the market leader in direct insurance premiums. Solvency II reforms will make London's insurers more competitive as £100bn of capital is released over the next ten years.

7. Conclusion and Next Steps

We are at the beginning of a new era of economic development, which is taking us ever deeper into the digital realm. With many positive developments over the last decades the UK is now at the cusp of going truly digital. This Ubiquitech Report therefore makes the timely case for accelerating change across network, security, standards, trust and user centricity.

At the centre of the imminent next steps is the finalisation of the DPDI, which will be the linchpin of regulatory reform that opens that path to digital and economic leadership by the UK at a global scale.

The UK is only able to benefit by putting in place ubiquitous network to enable every citizen and business to connect to the Smart Data highway that is currently being built upon Open Banking. The setting up of a 'Reliable System', underpinned by secure verification and authentication of individuals, entities and assets, driven by multi-modal biometrics where applicable will also become a building block to creating global standards and leadership in trade, building upon the ETDA. In parallel, this will enable the UK to attract businesses from all over the world to register their businesses in the UK providing further synergies across the global trade supply chain and further lifting the UK's leadership role in the space of legal arbitration and insurance.

Now is the time to act. Ubiquitech has to become a reality, connecting data, people, businesses and assets across secure channels to create economic growth and prosperity for all.

Annex A – Detailed Ubiquitech Recommendations

The key recommendations called out in this report are further detailed with regard to the underlying rationale in the below section. These recommendations are designed to be practical and feasible, whilst at the same time encouraging various stakeholders to think beyond the immediate necessities in order to shape the future of the UK as a leading Digital Economy.

A.1. Cyber Security and Fraud Controls

- The first duty of any Government is to protect their citizens and in the digital economy the first requirement of Government and Industry is to protect consumers and organisations from online harm. Central to this is the requirement to ensure Trust in the system to give confidence in the effective functioning of the overall ecosystem.
- The digital economy in the modern world is a fundamental part of Critical National Infrastructure (CNI) in and of itself, but in the Ubiquitech context it links through to most other areas of CNI such as Healthcare, Energy, Telecommunications. Protection of CNI has long been prioritised over the resilience of other sectors, though we note that financial services, whilst part of CNI themselves, are exempt from network information systems regulations due to having stronger sector-specific security standards.
- Given the foundation for Smart Data is being built on Open Banking, this report believes that the cybersecurity and counter-fraud requirements for our Ubiquitech vision are appropriate albeit that further strengthening of security measures must always be kept front of mind.
- This report welcomes current initiatives as part of the Government's fraud strategy such as financial crime intelligence sharing between public and private sector, between players within particular industries and between different industries. This report recommends to further such work being undertaken as risks from fraud have been a constant theme of our research and have the potential to be an early win for the UK on the international stage.
- From our starting point of Open Banking placing all our financial eggs in one basket, it is evident that even more security steps will need to be put in place if all our other sectoral eggs are loaded on top. Security standards such as for cyber security and strong customer authentication will need to be enhanced and effectively implemented and closely monitored by regulators across the board, be it for financial or say Health applications.
- Failure to adequately achieve the necessary trust and security of systems not only jeopardises the eggs in our basket but puts at risk the golden goose that is the potential Ubiquitech industries of the future.

A.2. Network, Systems and Processes Recommendations

- It is axiomatic to note that for Ubiquitech technologies to thrive there is an underlying requirement for ubiquitous network coverage and connectivity is achieved.
- We believe that the value that can be unlocked from more optimal use of consumer and organisational data is such that the market should be incentivised without recourse to regulatory or legislative levers, though as with Open Banking and CMA 9 guidance on standards maybe required.
- Renewable energy powered networks and datacentres should be encouraged by Government as part of NetZero targets, though we note that inefficiencies in current methods of data handling and storage lead to unnecessary duplication of effort and energy requirements.
- Regulatory bodies across the numerous industry verticals impacted by Ubiquitech should be encouraged to stay involved in trials of future technologies to speed up regulatory acceptance, bearing in mind that different forms of Smart Data will require different combinations of regulatory oversight.
- The Government needs to be bold and collaborate fully with private investors, though the added value to mobile operators and communications providers should be sufficiently evident to drive greater adoption. Sectors which will only benefit from the Ubiquitech Infrastructure (such as Healthcare) if such connectivity is available, should also be encouraged to help fund its deployment.
- “Advertising Free” services could become the ‘norm’. The Data Protection and Digital Information Bill will be the key enabler for alternative funding models of infrastructure as consumers will be offered the opportunity to monetise their own data where they believe it appropriate, always bearing in mind that informed consent is imperative.

A.3. Digital Systems in Trade Recommendations

- In light of the Electronic Trade Documents Act (ETDA) the UK should leverage its global jurisprudential influence to ensure good legal alignment across all our trading partners. As the first major nation to give equal legal standing to electronic documents rather than paper bills of lading, the UK is uniquely placed to design the ‘Reliable System’ that global trade will depend upon in future.
- As we have discussed earlier, 80% of global trade is already operated under English Common Law. Arbitration is carried out within the UK and many of the technical standards such as the ISO 27000 family are international adoptions of earlier British standards.
- Noted by the IRSG in January 2024, a global register would be adopted in an ideal world, but that standards might have to suffice. However, given the opportunity for the UK to drive the ‘Reliable System’ and the potential for effective reform of Companies House, the UK is in a unique position to form the desired Global Register of companies through coordination of requirements for global supply chain standards.

- In the City of London, we have a world leading concentration of maritime international contract and dispute resolution legal expertise and firms that will have international reach through representation of major trading companies. CoLC should convene a group of legal experts from across the industry and governments to leverage commercial diplomatic and international organisation channels to promote our laws and ensure legal alignment thereof with those of our major trading partners as they consider adoption of Model Law on Electronic Transferrable Records (MLETR) legislation.
- It is essential to for a non-commercial collaborative entity to create the space in which end-to-end digital solutions can be tried tested and refined and adapted to suit the needs of the intended beneficiaries, the trading community themselves.
- Alongside the legal expertise mentioned above, CoLC represents and promotes the interests of our world leading tech provider community. With the market currently skewed towards a small number of large incumbents and limited scope for entry and scaling up of innovative, small firms, CoLC can play a major part in providing practical opportunity for innovation and constructive disruption in the market to the benefit of all users.
- In a similar manner to recommendations from the Kalifa Review and more recently from CFIT itself, we believe that to underpin and ensure work is in close alignment with the legal strand, we should emulate the successful 'Sandbox' approach of the FCA and the Bank of England in financial services. Likewise, we should look to create and enable access to a 'Scalebox' for international trade solutions to design test and develop business models, including appropriate governance for the development of reliable systems under ETDA terms.
- Working with the ICC and other interested and convening parties (e.g. UK Chamber of Shipping, Lloyds, IGP&I and ITFA), the City of London ecosystem should urgently establish a working group to undertake a series of short sharp and focused tests on developing the model for ETDA reliability and interoperation and the meeting of the practical requirements of its trade and trade finance communities – both MNEs and SMEs. Such a group (or groups if considered appropriate) could be established quickly based on existing supply chains (based on different commodities, financial instruments, geographic corridors and business processes) and real life, scalable and open solutions.
- The opportunities for the UK to establish the legal and technical 'rules of the road' for international trade need to be seized urgently, given the stars are currently aligned for the UK to set such standards including the ability to confidently authenticate the participants in the global supply chain from natural persons behind the legal entities, the legal entities themselves and the assets under ownership, which can now under a 'Reliable System' be incorporated within global trade finance flows.

A.4. Verification and Authentication of Users, Entities and Assets

- As noted above, at the heart of any 'Reliable System' will be assurance that the parties within the ecosystem are who they claim they are. This is of course not a new requirement, unique to international trade but has long been a fundamental requirement of banking and payment systems in the fight against fraud and other forms of financial crime.
- There has therefore been a long history of security developments to attempt to counter such threats, but as is evident from current fraud levels with roughly half of all crime being digitally committed fraud. As we move into the Ubiquitech environment and the opportunities identified through international trade, it is clear that organised crime will move into this field to exploit any ongoing vulnerabilities.
- It is critical therefore that confidence in the robust authentication of individuals, legal entities and assets can be assured and that liabilities can be assigned through the supply chain even where this may need to be subject to insurance, again a strength of the UK market.
- All held data relating to Individuals, Business/Government and Assets needs to be verified, rationalised and tied to a real person through ratified biometrics.
- Our 'Reliable Ecosystem' should operate on the basis of a "zero-trust" best practices principle alongside existing data minimisation and other privacy preserving technologies and techniques.
- KYC will have to include capture of multi-modal biometrics in order ensure uniqueness at enrolment to prevent false positives. The ability to cross-reference multi-modal biometrics ensures that falsely obtained genuine credentials cannot be utilised in the real world, helping to prevent injection attacks.
- The use of biometrics is essential in combating fraud – multiple biometrics have been proven to be better than one. A fingerprint may suffice for a low risk transaction or action, but having multiple modes of biometric available allows for seamless step-up authentication.
- Standards accreditation and benchmarking of the reliability of biometrics will be crucial to ensure that our ecosystem cannot be compromised by advancing threats such as deep fakes and injection attacks against the system. These components in the KYC process will need constant and controlled monitoring and regulatory oversight through trusted channels such as financial services, who already have the legal obligation to handle strong customer authentication robustly building the Smart Data onto Open Banking parallels from DPD1. This would appear to be a logical next step to be incorporated within our 'Reliable Systems', be they for trade, banking, healthcare or any other form of Ubiquitech.

A.5. Delivering Digital Skills Education and Inclusion

- In order to bridge the digital skills gap, Government and service providers should design digital services and platforms that are accessible and user-friendly, providing affordable and accessible digital infrastructure and promoting digital literacy and skills training across all age groups. Specific consideration should always be given to access to systems for users not able to use traditional controls, e.g. sight impaired.
- Collaboration between Government, private sector organizations, non-profits, and community organizations is crucial for effective inclusion efforts.
- Apprenticeship programs and centres for lifelong learning are necessary to ensure that educational skills remain fit for purpose and timely. Industry Co-operation and funding in the education programme should be encouraged.
- Education and training should always be future focused to ensure that society is appropriately skilled, for example currently Web3 skill-sets and education should be part of the training.

Annex B – In Depth Inhibitors to a successful transition towards the Ubiquitech Digital Economy

The key shortcomings on the UK's trajectory towards a Digital Economy, which form the underlying basis of the Ubiquitech Report Recommendations are identified and discussed here below.

B.1. The Challenge of Cyber Risks and Fraud Controls

Cyber Threats are having a dramatic effect on global stability and this is predicted to continue for the next 10 years⁷. The Cyber Threat has grown exponentially and the result is devastating attacks that threaten the very existence of businesses and government bodies. This happens despite billions of dollars spent by enterprises on cyber resilience and recovery from cyberattacks.

Cyber is the first-strike weapon of modern warfare, and the targets are economic, systemically important global supply chains and the critical infrastructures of production, distribution, and finance/exchange.

Commercial enterprises are now on the front-line of a global economic battlefield and they are not prepared to do anything else but close known vulnerability gaps and patch their castle walls. Commercial enterprises are thus at an inflexion point:

- Enterprises are unable to prevent cyberattacks beyond standards-driven hygiene measures and whack-a-mole security operations. They continue to invest in Logo Security Assets (and can't configure or drive them), Incident Response and Recovery and doing the same things faster and harder, with the same outcome (they are a Breach Headline News article). Reactive and Response-based security has had its day. What is required is proactive Cyber Threat Intelligence-led Cyber defences and foresightful cyber threat risk management.
- Legislation that legally restricts enterprises from taking certain actions (paying a ransom) has forced an existential choice for businesses. The road ahead is long and tortuous, insurance does not cover the full extent of this road. Businesses must make hard choices between disclosure and non-disclosure of attacks if they know about the attack. If they don't know, or haven't discovered the attack, which is more likely today than it ever was, how can they disclose? Example: The British Library completely devastated, and the cyberattack that devastated Government supply chain partner Capita.
- There is a gap between the nation state security services and international and local law enforcement, which impacts enterprises. This gap was realised in 2018 by the 5 Eyes, but it was always known about. Investigations and consequences for adversaries occur in only 0.00002% of cases reported to Law Enforcement. There are no credible forces available to execute prevention or enforcement on cybercrime of any type. There is also no means to act disruptively and offensively against the rising tide of enemy actions. Examples: countless victims of carding fraud and theft, and of course the public failure to recover The British Library.

⁷ 2024 World Economic Forum Global Risks Landscape and Interconnections Map.

- Cybercrime and fraud now account for around half of reported crimes yet it remains radically underfunded in relation to its global impact (see the WEF statements on the global economic risk landscape 2024).

Unless we conceive of a Prevention and Enforcement Action Plan for cyber and fund it independently of the budgeting process, we are at severe risk of economic failure, and importantly a loss of trust and reputation for the UK overall.

B.2. Inadequate Networks, Systems and Access

B.2.1 Inadequate Infrastructure: How this is hindering the growth of the UK Digital Economy

The development of a robust and reliable digital infrastructure is crucial in fostering the growth of any economy, particularly in today's digital age. However, the UK faces significant challenges in terms of digital infrastructure, particularly in the telecoms sector.

Insufficient connectivity, limited broadband access and unreliable telecoms networks restrain productivity of businesses. This results in reduced competitiveness in the global market and hampers innovation and digital transformation. SMEs are particularly affected, as they heavily rely on digital platforms and e-commerce for their operations and sales cycles.

Moreover, the lack of reliable infrastructure also affects the development of advanced technologies such as 5G, high-speed internet and Internet of Things (IoT) devices. These technologies have the potential to drive economic growth, enhance productivity, and facilitate the transition to a digitalised economy. However, without adequate infrastructure, the UK lags behind other countries and fails to fully capitalize on the opportunities presented by the digital revolution. Whilst Oxford University's Portulans Institute ranks the UK 10th (out of 130) in their global Network Readiness Index 2023,⁸ a measure of a nation's capacity to use information and communication technology to promote growth and social wellbeing, we believe that still more can be done to ensure universal coverage, both geographically and demographically speaking.

The UK has set a target to ensure nationwide coverage of gigabit-capable connectivity by 2030 and deliver gigabit-capable broadband to at least 85% of UK premises by 2025. Currently, around 75% of premises have gigabit-capable broadband, but we would recommend that policy and regulation must be enacted to encourage private investment in network investment and increase competition in this space to allow for challenge of existing providers.

For 5G deployment it is essential to follow a market-led approach with a focus on policy stability, pro-investment regulation and speeding up the planning system for major projects and infrastructure transition to remove barriers to change.

In the recent UK Tech Plan, TechUK called for the government to be bold and *"go further and work with the telecoms sector to devise a new strategy to complete the rollout of advanced connectivity across the UK and support the availability of high-speed connectivity across the country"*.⁹

⁸ Portulans Institute, "Network Readiness Index 2023", link: https://download.networkreadinessindex.org/reports/nri_2023.pdf

⁹ UK Tech Plan, link: <https://www.techuk.org/resource/second-national-infrastructure-assessment-outlines-key-role-of-digital-infrastructure-to-drive-sustainable-economic-growth.html>

B.2.2 The need for sustainable network infrastructure

As the UK strives to achieve its net-zero and United Nations Sustainable Development Goals (UNSDG) commitments, it is essential to transition to more sustainable operating systems and power sources in the telecoms and cloud-based data distribution services sector. The current infrastructure heavily relies on energy-intensive processes and non-renewable resources, contributing to carbon emissions and environmental degradation. By adopting sustainable practices, the UK can reduce its carbon footprint and mitigate the adverse effects of climate change. If we carry on with an “as is” approach to infrastructure funding and development due to the greater connectivity and the huge increase in data use, traffic and streaming, this will not come without environmental consequences: for every bit of data that travels across such networks from data centres to end-users, another five bits of data are transmitted within and among data centres, all of which use energy (mostly electricity). It is estimated that energy demand from data centres and transmission networks accounts for around 1-1.5% of global electricity use in 2019.¹⁰ Whilst this may sound like a small proportion IDC Global Datasphere analysis had projections of data proliferation expanding at almost 25% per annum, suggesting up to 4.5% this year, and up to 17% by 2030, substantially threatening Net Zero targets without a fundamental mind shift in the storage and transmission of data.

Now more than ever we need new models of impact capital to be deployed by private investors to provide an adequate transition fund for UK Digital infrastructure so we can put in place more sustainable operating systems for the UK to achieve its development goals.

Transitioning to sustainable operating systems, such as renewable energy-powered networks will reduce greenhouse gas emissions, thereby supporting the UK’s commitment to achieving net-zero carbon emissions. Additionally, sustainable operating systems can improve energy efficiency and reduce operational costs for telecoms and cloud services infrastructure providers, enabling them to invest in network expansion and further technological advancements.

Furthermore, sustainable infrastructure development can attract green investments and stimulate economic growth. Investors and businesses are increasingly prioritizing sustainable practices, and a digitally advanced, environmentally conscious UK can become an attractive destination for such investments. This, in turn, would create new job opportunities, foster innovation, and strengthen the UK’s position as a global leader in the digital economy.

The World Economic Forum estimates that the combined global value of digital transformation to society and industry will exceed \$100 trillion by 2025. These financial benefits can be appropriately mapped to the United Nations’ Sustainable Development Goals (SDGs). Investment in technology enhances social and development outcomes in a country through several channels: internet access and enhanced telephone communication can improve access to information on employment and education, which will increase the chances that people can lift themselves out of poverty (SDG 1); digital infrastructure and Internet of Things technologies can stimulate agricultural sustainability and improve food security (SDG 2); and telecommunication can aid income inequality by connecting remote areas with cities and providing less developed countries and rural communities with work opportunities and free access to knowledge (SDG 10). By seeing investment in digital infrastructure as a core pillar for any future digital strategy we can envisage a brighter and more inclusive economy for all where no one is digitally excluded.

¹⁰ International Energy Agency, <https://www.iea.org/reports/data-centres-and-data-transmission-networks>, June 2020

B.2.3 The case for Broadband

Fibre optic broadband has been seen as the workhorse for data transmission for many decades yet under-investment has left the UK struggling to keep up with many other countries. Lack of Government vision has held investment back and as a result many other sectors of the economy have suffered. For example, the early 1980s Government stopped Mercury rolling out free fibre to every house through its water pipes with the, then publicly owned, water company. Later, in the early 1990's, whilst stopping BT's Fibre to the Home (FTTH) initiative, Government allowed over 200 (primarily American) cable TV companies to dig up UK roads and install obsolete coaxial cabling. The latter are now consolidated under the Virgin network and provide fibre-like services where fibre still has not reached.

For the last decade many new fibre companies have entered the market and are, at last, delivering new fibre infrastructure. The pricing and economics of this now generally work in urban and semi-rural areas for both business and consumer markets, but FTTH coverage is still relatively low. True rural areas still suffer from poor coverage. Wireless and Mobile Broadband are penetrating these areas however.

The City of London, unlike the rest of the country, has a fibre density issue. The concentration of so many businesses with high data needs into such a small area restricts the delivery of new fibre. In 2016 Zak Goldsmith, in his mayoral campaign, mentioned TfL resistance to his plan for fibre installation in the underground. Similar resistance was experienced with the deployment of mobile phone services. These have only recently been overcome. Where investment has been provided and fibre laid, subsequent ownership and regulatory change has left much of it unused.

For high end business use there are ten fibre networks offering good but expensive services. For smaller companies, provision of cheaper services is barely adequate. The City Property Advisory team (CPAT) has however worked with broadband operators in the Square Mile to deliver improved, faster broadband services at affordable prices for small businesses and residents. Attention and further development in this area will provide huge benefits for a thriving and evolving business community. In greater London over half the population can now access full fibre to the home as a result of new deals with the operators and the Boroughs.

Wireless broadband use has suffered primarily because of the building density. Some wireless frequencies do not penetrate buildings very well, so even efficient services like 5G are suffering in this context. WiFi roaming and coverage in-building largely fills the gaps in mobile coverage. The recently introduced 6GHz band works well for Mobile and WiFi. It is being fought over by Mobile operators who want to extend their 5G services and large cloud service providers wishing to increase delivery capacity through better WiFi. Strong leadership in the City and across the country with support from Ofcom and Government would be able to resolve this and enable the business use of this new opportunity to be maximised, thus enabling productivity growth as well as levelling-up.

B.2.4 Low Earth Orbit Satellites

Older satellite data services like Very Small Aperture Terminals, or VSATs, have been providing global coverage for decades. The 'regional' footprint is adequate for many applications and services where poor latency is not an issue. The economics of these are now being challenged by the deployment of Low Earth Orbit (LEO) satellites. These are offering global streaming at medium data rates and at much lower latency, which will be essential for Web3 (~100MBPS). Starlink currently has over 5,289 satellites in LEO (at an altitude of around 500km) and has approval to launch 7,500 more within the next three years. Until recently, all these satellites provided services via satellite user terminals – antenna dishes deployed by the customer, which act as a middleman for communications between the satellites and user devices, like smartphones. Newer satellites are now being launched with the capability to communicate directly with the user phone. BT are contracted with the UK-owned LEO company OneWeb for services through antennae and have just started trials with the SpaceX Starlink satellites for phone connectivity. Starlink's direct-to-mobile services will begin with text messaging capabilities, with voice and data coverage to come in the following years. This seems trivial but it will be global, direct to person communications.

B.2.5 Moving forward to Web3

Unlike the earlier internet, Web3 is based on decentralisation, self-sovereign identity and Distributed Ledger Technology (DLT).

The underpinning connectivity described above is being used for the delivery of pioneering Web3 services. Emerging LEO Satellites are particularly suited to host these services due to the low latency. Web3 is distributed and based on DLT, which favours high transaction rates and low latency.

People will be able to use Web3 technology to communicate and make transactions without revealing their personal information. This can protect people from identity theft and fraud. It can also help promote free speech and open communication. Because it is decentralised, meaning that no single entity controls it, data is spread out across many different computers. This decentralisation makes it very difficult for hackers to get access to data.

Web3 will allow people to communicate directly without the need for intermediaries. In addition, because Web3 is decentralised, it is more resistant to censorship and manipulation.

B.3. Inefficiencies of Paper-Based Systems in Trade

Few areas of human activity remain as paper-based as international trade. The ICC estimates that some 25 billion bits of paper are created each year globally in this context. At the same time CBP estimates that there is some \$2tn of Trade Based money laundering each year, while WEF also estimates there to be a trade finance gap of some \$1,7tn not because lending is risky or because there is significant default, but because there is insufficient data available for lenders to make regulatorily compliant decisions to make capital available. At any given time, it is estimated that some \$0.5tn of capital is tied up simply in delayed settlement of liabilities within global supply chains, capital that could easily be released and used by viable businesses for increased growth and productivity through increased international trade.

A typical international transaction now can involve up to 40 documents and some 5,000 separate data points. Each document requires not just the repetition of data that will almost certainly have been generated by the originating transaction, but the separate creation of bilateral trust relationships between actors in supply chains.

As the risks involved in international trade – geopolitical, climatic and commercial – all show signs of increasing, it is clear that the current way of doing things – much of which remains fundamentally unchanged since the Bill of Exchange Act 1883. With the passage of the ETDA the UK has a unique and once in a generation opportunity to change things for the better

B.4. The Lack of Verification and Authentication

The organisational costs of ID Verification (IDV), whether performed manually, or digitally, amounts to £billions per year.¹¹ However, the direct costs do not include the people training, processes development, record keeping, regulatory reporting and numerous additional organisational costs also incurred each year. This is to be expected given the current cacophony of IT systems, all layered on top of each other, all satisfying specific niche needs, but also leaving gaps, cracks and holes to be exploited by criminals or other malicious actors across the economy. As these deficiencies are identified and fixes are developed and deployed, organisational costs for IDV continue to rise. The 2023 Lexis Nexis Risk Solutions report into ‘The Cost of Compliance’ also estimated that UK businesses spend £7.8 billion on such compliance costs each year, though as we can witness from continued fraud losses, spending it with very little impact on the issue the compliance is supposed to address.

In the current state the following symptoms exist:

People	<ul style="list-style-type: none"> • Data not shared or sanitised • Multiple “truths” • Out of date data, out of date information • Personae of individuals in their role, linking individual as a Director, PSC, etcetera within a Legal Entity, or as a private citizen, etc
Entity	<ul style="list-style-type: none"> • Government departments are siloed • Prompt Companies House Reform as a current opportunity • Adoption of Legal Entity Identifiers as an enabler within the ETDA ‘Reliable System’ • Storing and processing old, or conflicting data, or correcting data errors. Information is stale, analysis using aged data is fundamentally flawed • Some data not available, or processes not capable of adequate verification. e.g. Beneficial Owner(s) and Ultimate Beneficiary Owner(s) are not fully traceable to companies and vice versa
Asset	<ul style="list-style-type: none"> • No referenceable and verified repositories or digital verification processes exist for assets

¹¹ According to an internal study by Barclays of 2022, KYC cost in Retail Banking alone (globally) averages \$65 (Singapore Dollars), roughly £52. There is a total of circa 180 Million accounts in the UK held by people over 18 which includes 50 Million current accounts. KYC needs to be performed every 2-5 years (averaging 3.5) depending upon perceived risk putting the UK KYC in Retail Banking at circa £2.6Bn per annum – for just one small sector of the business world.

The results of the current state are evident:

- UK financial fraud (2022) of over £1.2B, although a significant amount of fraud remains unreported. Of this, financial fraud in the UK Finance and Insurance sector totalled over £790M.
- In addition, in this sector alone, a further £1.1B of financial fraud was successfully prevented (source www.ukfinance.org.uk).

The current ID&V data sources and ID&V processes should be absorbed into the new framework and the legacy processes, IT systems and data stores decommissioned. With the millions of current data sources and ID&V processes, this adoption will take many years. Only when completed, with supply chain and other process loopholes systematically closed, and process analytics enabled, will APP and other types of financial fraud be significantly reduced.

B.5. The Issues with Digital Skills Education and Inclusion

Digital financial exclusion imposes significant costs on individuals and society as a whole. In the UK, there are over eleven million people who lack the basic digital skills they need to participate fully in our digital economy. There is a clear digital divide in our nation, which is harming those who are left behind and holding our economy back. By 2028 the UK economy could arguably be missing out on almost £22 bn of value as a direct result of digital exclusion – see report from The Good Economy Foundation.

While the UK government has taken steps to improve digital financial inclusion and access to financial and basic banking services and we commend the work and efforts documented in HMT's Financial Inclusion 2021-2022 Report¹², much more work is to be done to bridge the digital financial divide.

For example, some of the costs associated with digital financial exclusion include:

Limited access to essential services: Individuals who are digitally and financially excluded may face difficulties in accessing essential services such as banking, healthcare, education, and government services. This can result in higher costs, inconvenience, and a reduced quality of life.

Financial disadvantage: Lack of access to digital financial services can lead to higher transaction costs and limited financial options for individuals. This can result in exclusion from certain financial products and services, making it harder to save, invest, and manage finances effectively.

Reduced economic opportunities: Digital and financial exclusion can limit employment opportunities and hinder career advancement. Many jobs now require digital skills, and online platforms offer opportunities for entrepreneurship and income generation. Without access to these resources, individuals in lower income households may find it difficult to participate in the modern economy.

Increased social exclusion: Being digitally and financially excluded can lead to social isolation and exclusion from social networks. In an increasingly interconnected world, digital exclusion can limit social interactions, access to information, and participation in social and community activities.

¹² HMT Financial Inclusion Report 2021-2022: https://assets.publishing.service.gov.uk/media/639c91f4d3bf7f37618b5c5d/Financial_Inclusion_Report__002_.pdf

Digital exclusion and the lack of digital skills have a significant impact on the UK economy and our ability to move to transition to a smarter and greener digital economic operating base. As more and more essential services move online, such as banking, healthcare, and government services, those without digital skills or access to technology are left behind. This creates a digital divide between those who can easily access and navigate these services and those who struggle to do so. Moreover, digital exclusion undermines productivity and innovation. Businesses that lack digital skills and tools cannot fully leverage the benefits of technology to streamline their operations, reach wider markets, or develop innovative products and services. This limits their competitiveness and growth potential, ultimately affecting the overall productivity of the UK economy.

Digital exclusion and a lack of digital skills has several consequences on the UK economy:

Limited economic participation: Digital exclusion prevents individuals and businesses from fully participating in the digital economy. This means they miss out on opportunities for online business transactions, e-commerce, and digital marketing. As a result, their economic potential remains untapped, leading to a loss of productivity and growth.

Increased inequality: Digital exclusion creates a digital divide, exacerbating existing social and economic inequalities. Those who lack access to digital tools and skills face barriers in accessing online services, employment opportunities, and educational resources. This further widens the gap between the digitally excluded and the digitally connected.

Reduced productivity and innovation: Businesses that are digitally excluded struggle to adopt digital technologies and leverage their benefits. This hampers their ability to streamline operations, automate processes, and enhance productivity.

Impacted job market: The digital economy is creating new job roles and transforming existing ones. However, those without digital skills are at a disadvantage when it comes to job opportunities. They may face limited employment options, lower wages, and increased vulnerability to job displacement by automation.

Inefficient public services: Digital exclusion hinders the delivery of public services that have shifted online. Those who are unable to access online government services, such as filing taxes or applying for benefits, are left with limited options, leading to inefficiencies and increased costs for both individuals and the government.

Reduced digital innovation and entrepreneurship: Digital exclusion limits the pool of potential innovators and entrepreneurs. Individuals who lack digital skills or access to technology may be deterred from pursuing digital business ventures or developing innovative solutions. This hampers the entrepreneurial ecosystem and slows the pace of digital innovation in the country.

To mitigate these consequences, it is essential to invest in initiatives that promote digital inclusion, such as providing affordable internet access, offering digital skills training programs, and ensuring that digital services are accessible to all.

Annex C – The Ubiquitech Group

Group Chair:

Dr. Ruth Wandhöfer, Member of the City of London Innovation and Competitiveness Advisory Board, NED, Author, Adviser, Visiting Professor Bayes Business School (formerly CASS).

Members:

Vivienne Artz, OBE FCSI (Hon) CMgr CCMI, Intelligent Data Advisory Limited

Rick Chandler, Professor of Statistics, University College London (UCL)

Andrew Churchill, Founder and CEO, Technology Strategy

Nick Davies, Director, ICC Centre for Digital Trade & Innovation

Chris Hurst, CTO (CIO CSO CISSP), Blackwired.Pte

Rob McBratney, CEO, Sietech

Victoria Thompson, Founder and Director, Orora; Chair, Whitechapel Think Tank; Lecturer Financial Regulation & Policy, University College London (UCL)

With support from Leighton Hughes, Fintech Policy Adviser, Innovation & Growth, City of London Corporation

