IRSG
INTERNATIONAL REGULATORY STRATEGY GROUP

International Regulatory Strategy Group (IRSG)

DEPARTMENT FOR SCIENCE, INNOVATION & TECHNOLOGY CALL FOR EVIDENCE

SMART DATA OPPORTUNITIES IN DIGITAL MARKETS

Introduction

The International Regulatory Strategy Group (IRSG) is a joint venture between TheCityUK and the City of London Corporation. Its remit is to provide a cross-sectoral voice to shape the development of a globally coherent regulatory framework that will facilitate open and competitive cross-border financial services. It comprises practitioners from the UK-based financial and related professional services industry, who provide policy expertise and thought leadership across a broad range of regulatory issues.

The IRSG welcomes the opportunity to respond to the Department for Science, Innovation and Technology's (DSIT) call for evidence on 'Smart Data opportunities in digital markets'. Overall, we support steps to bolster the UK Smart Data ecosystem. The government should leverage the new legislative framework for Smart Data schemes, which the Data (Use and Access) Act (DUA Act) establishes, to facilitate secure and transparent data sharing across our digital markets. Implementing Smart Data, where service providers can share customer data securely with authorised third-party providers (TTPs) at the customer's request, could unlock £149bn of organisational efficiency and £66bn of new business and innovation opportunities for the UK economy.[1]

Financial services are increasingly digital markets, as firms increasingly deliver many core activities, such as payments, lending, trading, and customer onboarding, through digital platforms.

The City of London Corporation published *Securing growth: the digital verification opportunity* in March 2025, in collaboration with EY, which articulated the need for scalable Digital Verification Services (DVS) in the UK. The report followed over a year and a half of close engagement and research with the financial services industry and government departments, and we are now advancing the recommendations. This includes the scaling of an "orchestrator", which is the centrepiece of our proposed Digital Verification model.

Data is a fundamental asset to firms. It underpins their ability to innovate, supports better and more efficient decision-making, enhances risk management, and enables more personalised solutions for customers. Therefore, the industry is well-positioned to drive innovation through Smart Data initiatives. The UK financial services industry is already a global leader in Smart Data initiatives, and DSIT should consider our industry's experience with Open Banking as a blueprint for wider reform.

[1] RAND, 'The Digital Catapult and productivity A framework for productivity growth from sharing closed data' (September 2015), available at: 'The Digital Catapult and productivity: A framework for productivity growth from sharing closed data | RAND

Addressing customer needs (questions 1-2)

Issues customers face

Financial services customers generate large amounts of financial data, while their personal and behavioural data is often fundamental to accessing, tailoring, and pricing these services. However, despite the deep data pools sitting across the industry, customers can face significant barriers in accessing and securely sharing the data held about them by financial services providers.

The safe, secure and private storage and transfer of customer data is paramount to our industry. Historically, this has resulted in firms holding fragmented customer data across multiple institutions, with no single interface for the customer. Even when data is available, different financial firms often store and transmit it using proprietary systems and non-standardised formats, which creates significant challenges for integration, comparability, and portability between providers. Customers may also be reluctant to share their own data due to low levels of trust in how institutions will handle, secure, and use it.

In 2017, the UK pioneered Open Banking to address these issues for the banking sector, empowering banks to share customer information securely via application programming interfaces (APIs). This has been a success story for the UK, with one in five UK consumers and small businesses now actively using Open Banking.[2] However, these challenges remain across the rest of the financial services ecosystem.

Use cases

Building on the UK's success in Open Banking, the government should support similar data-sharing principles across other financial sectors, paving the way for Open Finance. While the cross-industry use cases for Open Finance are vast, the Centre for Finance, Innovation and Technology (CFIT) identified several priority use cases.[3] These included improved consumer financial management. APs could combine customer data from across different products, such as savings, loans, mortgages, pensions, and insurance, to create tailored budgeting, investment, or savings tools. This could also facilitate easy switching to more cost-effective or more suitable options. Customers could view accurate, real-time pension balances and contributions in a single dashboard, supporting improved financial literacy and greater retirement readiness. In this way, Smart Data could complement and enhance the government's existing Pensions Dashboards Programme (PDP).[4] This is integral to the government's growth agenda, fostering higher long-term savings, driving increased investment, and building a more resilient economy prepared for the challenges of an ageing population.

Smart Data could support financial inclusion and protect vulnerable customers. CFIT found that Open Finance could enable up to 150,000 more vulnerable individuals per year to receive tailored financial guidance by giving agencies such as Citizens Advice an instant, accurate and consolidated overview of

[2] Open Banking, 'Open Banking Impact Report' (May 2025), available at: The open banking Impact Report 2025 May
[3] CFIT, 'Embracing the UK's Open Finance Opportunity' (February 2024), available at: CFIT-Open-Finance-Blueprint.pdf
[4] Refer to, Department for Work & Pensions 'Pensions dashboards: guidance on connection: the staged timetable' (August 2025), available at: Pensions dashboards: guidance on connection: the staged timetable - GOV.UK

their financial information. Alongside regulatory reforms such as targeted support[5], this will be a helpful tool to encourage more individuals to engage with their finances. Smart Data can also enhance customer trust by enabling secure, cross-sector data sharing that strengthens fraud prevention and identity verification, allowing firms to detect and address suspicious activity more quickly. Reducing financial crime is key to long-term economic growth across the UK[6] and plays a vital role in building customer trust in financial markets, which will then encourage further Smart Data adoption.

The increased integration of Smart Data across digital markets will give rise to new, innovative financial products and business models. This will drive greater competition, reduce costs, give customers more control and convenience and, in turn, stimulate further innovation.

The scope of a scheme (question 3)

Supporting wider Smart Data reforms across financial services will require broader datasets than those in Open Banking today, some of which may be more sensitive. Given the importance of data privacy and protection across financial services, data sharing within Smart Data schemes should be use case-dependent, ensuring that firms only share necessary datasets for the specific, consented services they are providing. However, the following types of data would need to be in scope as a minimum:

- Financial and behavioural data, such as credit history, spending patterns, savings and investments and insurance claim frequency.
- Identity and verification data, including Know Your Customer (KYC) information.

Access to data on customer preferences and permissions would also support personalisation and tailoring of services. This would help align products and services to individual needs and deliver better consumer outcomes.

To enable customers to securely share and manage a complete picture of their financial data, DSIT should consider the full spectrum of financial institutions.

The scheme should also support cross-sector data sharing, ensuring that Smart Data initiatives in one sector, such as retail, are interoperable with those in other sectors. A practical example is linking card transaction data with corresponding retailer records. Achieving this interoperability could be challenging if the government does not consider this during the scheme's design from the outset.

Assessing a digital markets Smart Data scheme (questions 4-6)

Feasibility of delivery

The UK's leadership in Open Banking has demonstrated the feasibility and impact of implementing Smart Data schemes. In the context of financial services, the UK has already tested the technical,

[5] HMT, 'Targeted Support Policy Note' (July 2025) available at: Targeted Support - GOV.UK
[6] UK financial institutions spent over £38 billion on financial crime compliance in 2023, reflecting a 12% increase from the previous year. LexisNexis, 'True Cost of Compliance' (July 2024), available at: Report: True Cost of Financial Crime Compliance.

regulatory, and governance approach to Smart Data at scale. The success of Open Banking has also provided a solid foundation of consumer trust and engagement with Smart Data initiatives.

However, there will be significant costs in developing the infrastructure, governance frameworks, and new services that firms will require to underpin wider Smart Data schemes. For firms to invest in innovation, there must be a significant opportunity for commercial viability, which customer demand will largely drive. Customers must clearly understand the terms and benefits of sharing their data, including time savings, cost reductions, and personalised services. Smart Data schemes should convey these benefits in a quantifiable and clear manner and should emphasise the secure nature of the scheme to build the public trust that is essential for adoption.

Providing early regulatory clarity on the use of Smart Data is also paramount to the scheme's feasibility, as this will enable safe and confident industry-wide adoption at scale. The future scheme's success will depend on a robust regulatory framework that protects customers while enabling innovation.

To successfully implement Smart Data across wider digital markets, the UK should leverage the lessons learnt from Open Banking. DSIT should work closely with HM Treasury (HMT), the financial services industry, in particular the banking sector and the 'CMA9' banks that the Competition and Markets Authority (CMA) chose to deliver the initial framework[7], as well as the relevant regulators to understand these. For example, mandating Financial Conduct Authority (FCA) accreditation for TPPs and requiring common API standards were both critical to the success of Open Banking. The CMA has identified its own key learnings, such as a lack of periodic review mechanisms, insufficiently defined roles and responsibilities and compliance monitoring challenges.[8] While the 20% uptake rate for Open Banking across UK consumers and small businesses marks positive progress, the industry may have valuable insights on why the remaining 80% are not actively using.

The success of Smart Data reforms depends not only on financial services but also on other sectors progressing at pace. To help 'level the playing field,' sectors outside of financial services must catch up with the progress made in Open Banking, rather than relying solely on financial institutions to continue opening up more datasets in isolation. Cross-sector alignment is key to unlocking the full benefits of Smart Data.

Impacts

As discussed above, enhanced data mobility can drive competition, improve customer experience, and lead to the development of new financial products tailored to individual needs. Small and Medium-sized Enterprises (SMEs) could also benefit greatly from Smart Data schemes. CFIT found that Open Finance could significantly address the £22bn SME funding gap, concluding that lenders could have given more than 25% of declined SME loan applicants access to finance if they had broader data sharing models in place.[9] Overall, the economic opportunity of delivering Smart Data is huge. CFIT

[7] The nine largest banks and building societies in Great Britain and Northern Ireland, based on the volume of personal and business current accounts/ For the full list of CMA9 banks, refer to: CMA9 - Open Banking
[8] CMA, 'Open Banking Lessons Learned Review' (May 2022), available at: Open banking lessons learned review
[9] CFIT, 'Embracing the UK's Open Finance Opportunity' (February 2024), available at: CFIT-Open-Finance-Blueprint.pdf

estimated that Open Finance alone could generate over £30bn of growth in the UK economy by boosting lending to SMEs, supporting access to financial advice, and improving productivity.

However, as noted above, implementing Smart Data will present a significant cost for firms, especially in the initial stages. This may be particularly challenging for SMEs, which often have less budget and resources to manage the costs and meet new compliance burdens. While the long-term benefits and efficiencies that initiatives such as Open Finance present may justify the upfront costs, the government and regulators must take costs into account when designing rules and timelines for Smart Data adoption. We would urge the UK authorities to focus on use cases that target areas where deploying smart data is likely to yield the greatest benefits and where the costs to firms are most manageable.

DSIT should also seek to ensure that the requirement to comply with new smart data schemes falls only on those firms necessary to make the scheme viable, rather than a broad scope that imposes costs on the whole industry unnecessarily and undermines the support for such schemes. For example, where use cases emerge in consumer-facing applications such as budgeting, savings and mortgage tools, there should be no need for such schemes to involve wholesale firms that do not engage directly with retail consumers.

The role of data brokers and aggregators requires careful consideration. As Smart Data schemes enable individuals to access and share their data, the scheme should avoid established financial institutions bearing the costs of making customer data available, while new entrants or data intermediaries benefit commercially from using that data without contributing proportionately to the infrastructure or compliance costs. Policymakers should work with industry to balance allowing individuals to access their data with firms having to subsidise challengers in this area.

Risks (question 7)

Without robust safeguards, implementing Smart Data schemes across digital markets could increase the risks of data misuse and privacy breaches. The financial services industry is heavily regulated and adheres to strong data protection requirements. However, Smart Data initiatives depend on TPPs accessing these datasets. Open Finance requires a broader ecosystem of TPPs than those which Open Banking established. This will increase the number of entities that could experience a cyber-attack or data breach. Meanwhile, any TTP data misuse or unauthorised access could expose customers to identity theft and fraud, risking financial loss and reputational harm. To mitigate this, the government should work with the FCA, Information Commissioner's Office (ICO) and Prudential Regulation Authority (PRA) to ensure the robust accreditation, liability, and oversight regime for Open Banking extends to wider Smart Data schemes across financial services. Where feasible, the future scheme should leverage state-of-the-art cybersecurity and privacy-enhancing technologies. This can also serve as a blueprint for mitigating similar risks in other sectors.

In designing the future scheme, the government should consider resiliency risks across different sectors. For example, Smart Data-based services need to be reliable, scalable and always available. If there is significant demand for the scheme amongst customers, insufficient system capacity could result in network congestion or unexpected periods of downtime. If these services crash, slow down, or are unable to manage large volumes of users, this would directly affect customers and risk

negatively impacting confidence and trust in Smart Data. This could deter future adoption and customer appetite for such schemes, leading to lost revenue for firms. From a security perspective, inadequate scaling or a highly centralised scheme concentrates the vector for cybercriminals to attack. Scalability helps to mitigate this risk and, therefore, should be a priority consideration in the design stage of the scheme and its associated regulations.

The future regulatory regime must be proportionate to the risks. Overly prescriptive regulatory requirements would stifle innovation and could hinder SMEs' ability to compete effectively with larger firms. The risks associated with data sharing cut across different regulatory remits. Coordination between different regulators will, therefore, be key to ensuring a proportionate, coherent and consistent approach to governing Smart Data schemes. The government should consult the industry on any regulatory proposals before designing the future regime.

Implementation (question 8)

For Smart Data schemes to deliver on their promise, there must be clear commercial incentives for industry investment. Early regulatory clarity, industry engagement, and quantifiable benefits (e.g., cost savings, improved customer outcomes) are critical to drive adoption and innovation. The government should work closely with industry to ensure the framework is commercially viable and future-proofed.

Protecting customers (question 9)

Protecting customers must be the foundation of any Smart Data scheme. In addition to the above points, this should include mandatory, clear consent management processes with simple revocation controls, ensuring that customers always retain control of their data. The government must establish clear liability allocation between data holders and accredited TTPs, and support this with independent dispute resolution mechanisms. Transparency around data use is critical to building and maintaining consumer trust.

Wider design principles (question 10)

To realise the full potential benefits of Smart Data schemes, several elements should influence strategic decision-making during the scheme's development. This includes data transparency, proportionality, resiliency and interoperability of systems, and strong customer protection. A clear policy aim should unpin this, alongside clarity on dispute resolution, a sufficiently empowered coordinating body, support from industry, and commercial viability. The coordinating bodies will need sufficient funding and resources to implement the framework, and have a clear governance structure.

The UK context (questions 11-13)

Harmonisation between the future UK financial services regulatory regime and different sectors and jurisdictions is vital to reduce costs, foster innovation, and provide certainty for firms operating in digital markets. To maximise impact and minimise regulatory fragmentation, we urge alignment with existing financial data access regimes, including UK Open Banking and the EU's regulation on financial data access (FiDA), and with international standards and frameworks, especially the EU Digital Markets Act (DMA). The US Consumer Financial Protection Bureau's (CFPB) shift on Section 1033 illustrates

how regulatory direction can diverge across jurisdictions, meaning international banks must navigate different obligations, timelines, and cost structures.[10]

The UK is making progress towards the next stage of Open Banking in the UK[11] and setting the pathway to Open Finance. To ensure coherence and avoid duplication, DSIT should work with HMT and the financial services regulators to align the development of a Smart Data scheme with developments in our industry. This includes next steps on the long-term regulatory framework for Open Banking and the FCA's planned Open Finance roadmap, due by Spring 2026[12]. The government has now appointed the FCA as the lead UK regulator for Open Banking, which we support. We encourage the FCA to engage extensively with industry to co-design the appropriate regulatory framework for Open Banking and other Smart Data sharing schemes. Regulators for other sectors' Smart Data schemes should equally engage with industry and adopt a flexible approach to accommodate the challenges specific to that sector and new, emerging business models within it. For the lessons learnt on Open Banking, please refer to our answer to question 4.

The DUA Act also established a legislative framework for DVS. DVS are key to unlocking secure and effective Smart Data schemes, by enabling customers and businesses to verify their identities online in a safe and standardised way. DSIT and HMT should align Smart Data reforms with developments on DVS to underpin secure, efficient and frictionless data sharing authorisation.

The government and regulators should coordinate Smart Data reforms with key technological developments, particularly in artificial intelligence (AI). Through Smart Data, AI can leverage high-quality, permissioned datasets to deliver more personalised services, stronger fraud detection, and automation-driven efficiencies.

The government should also embed Smart Data principles across wider financial market reform to support innovation and competitiveness. We welcome HMT identifying 'utilising Smart Data' as a key action under its Wholesale Financial Markets Digital Strategy (WFMDS)[13]. Within this, one area of opportunity is the dematerialisation of UK shareholdings[14]. A modern, digital UK shareholdings framework would create the right foundations to foster and leverage innovative initiatives such as Smart Data. For example, these principles could enable secure, API-based access (or any other modern technology solution) to share ownership records. This would allow registrars, brokers, custodians, and investors to exchange verified shareholding data instantly, improving settlement efficiency, transparency, and investor services. However, while the government has confirmed its ambition to transition to such a system (in an intermediated, single digital register), it has not set a clear timeline for this. Initial steps focus on digitising the existing framework, but the longer-term design must deliver an authoritative, standardised, and interoperable source of truth that supports Smart Data principles. The government must work with industry to develop a system that supports data

[10] For more information, refer to JD Supra, 'A Hard Reset on 1033?: A Look at What's Next for Open Banking | Morrison & Foerster LLP - JDSupra' (June 2025)
[11] Refer to: FCA, 'FS25/4: Design of the Future Entity for UK open banking' (August 2025), available at: FS25/4: Design of the Future Entity for UK open banking | FCA
[12] The FCA's 5-year Strategy in March 2025 committed to releasing a roadmap within a year: FCA, 'Strategy 2025-2030' (March 2025), available at: Our strategy 2025 to 2030
[13] HMT, 'Wholesale Financial Markets Digital Strategy' (July 2025), available at: Wholesale Financial Markets Digital Strategy - GOV.UK
[14] Refer to HMT, 'Digitisation Taskforce Final Report' (July 2025) available at: Digitisation Taskforce - July 2025 - GOV.UK

portability, clarity of ownership, and consistent standards, be that through the interim solution in the first instance, or the final goal of a single central register. The single intermediated register would consolidate all holdings into one authoritative source, ensuring the necessary data completeness to meet regulatory requirements and enable market-wide solutions. This would set strong foundations to harness the full potential of Smart Data. DSIT and HMT should work together to implement Smart Data within the digitised shareholdings framework and ensure a timely and successful transition to a single, intermediated system that enhances Smart Data adoption and innovation[15].

International examples (question 14)

The EU's DMA identifies a focus on 'gatekeepers', large commercial providers of core platform services, which the Act defines by role, size, and durability in the market. The DMA did not define 'provider of core platform services', leaving market participants' responsibilities unclear. In contrast, the Australian Consumer Data Right (CDR) legislation employs a deliberative sectoral designation process. Ministers must extensively consult with industry and analyse the impact of "opening data" before any sector becomes subject to data sharing obligations. Sector designation does not confer substantive obligations. Instead, regulators then develop CDR rules setting out sector-specific frameworks for industry to follow.[16] The Australian example exhibits greater predictability through a gradual implementation approach. By undertaking a sector-specific process, the CRD is more likely to clarify market participants' responsibilities.

To avoid similar ambiguity to that found within the DMA, UK policymakers should clearly define the targets of legislation and the thresholds at which it regulates entities. The policy should also clarify the regulated entity's responsibilities, for example, in relation to data protection, access and portability, both in the present and with a view to issues that could arise in the future, to help ensure that the framework is sufficiently future-proofed. Clarification could also include the production of industry guidance, which could be delivered alongside specific implementing bodies like the Open Banking Implementation Entity. The absence of such an entity in Europe has resulted in variance in the quality of APIs due to the market being fragmented along member state lines. The European Banking Federation (EBF) highlighted this challenge, recommending standardisation for aspects like data transfer mechanisms, data formats, and their security requirements.[17]

Additional comments (question 15)

We urge the government and regulators to maintain ongoing, meaningful engagement with industry participants throughout the rulemaking process. This will ensure that Smart Data schemes are responsive to market realities, adaptable to emerging business models, and that the firms implementing them are supportive.

[15] The government should sequence transition timelines alongside other major reforms, including the ISA system modernisation and the introduction of Targeted Support, to ensure coherence and minimise disruption.
[16] Refer to: Australian Government, The Treasury: 'Consumer data right: Telecommunications sectoral assessment' (November 2021), available at: Consumer data right: Telecommunications sectoral assessment
[17] EBF, 'The European Commission's proposal of a Digital Markets Act – EBF Key messages' (June 2021), available at: EBF_045188-Digital-Markets-Act_EBF-key-messages.pdf