The Information Commissioner's response to the Financial Conduct Authority's Discussion Paper about the potential competition impacts of 'Big Tech' entry and expansion in retail financial services

About the ICO

1. The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR).

2. The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and it takes appropriate action when needed.

Introduction

3. The ICO supports the UK digital economy by empowering responsible innovation and sustainable economic growth. This includes supporting the lawful use and transparent sharing of personal data to drive innovation and economic activity. We work with our regulatory counterparts and other stakeholders to ensure cross-regulatory coherence and maximise certainty for businesses and individuals.

4. Financial services is a crucial sector of the UK economy and it relies on substantial use and exchanges of personal data. This data processing can have a significant impact on people. For example, personal data held about an individual can influence their credit rating, or the premium they pay for insurance. Financial services firms must meet their obligations under data protection law so that people and their personal data are treated fairly and lawfully.

5. Our ICO25 strategy sets out how the regulations we oversee support consumers to trust and confidently use the products and services on offer across the digital economy, including in financial services

markets.[1] The prominent role 'Big Tech'[2] firms play in the digital economy – and the scale and scope of personal data they collect and use – means that their processing activities can have a particularly large impact on the public interest.

6. As set out in our joint statement with the Competition and Markets Authority (CMA), we see strong synergies between the objectives of data protection regulation and competition.[3] Data protection regulation empowers consumers to be in control of their data; requires that firms' information about data processing supports well-informed consumer choices; and incentivises privacy-friendly innovation. By working together with the Financial Conduct Authority (FCA), we can ensure any Big Tech entry and expansion in financial services has a positive impact on peoples' information rights and competition.

7. We therefore welcome the opportunity to engage with the FCA's Discussion Paper on the potential entry and expansion of Big Tech firms into financial services markets.

The role of data protection regulation in financial services

8. Financial services firms face strong incentives to use personal data in ways that give them a competitive advantage, for example, by supporting efficiency, innovation and the creation of new income streams. The Discussion Paper notes that Big Tech firms could be particularly well placed to explore these opportunities when entering and/or expanding in the payments, consumer credit, deposits and insurance services retail markets.[4]

9. The Discussion Paper notes that Big Tech entry and expansion in these markets could benefit consumers via increased innovation and greater competitive pressure on incumbents. Big Tech firms' ability to deliver these benefits, in large part, stem from the personal data they hold about consumers, and the insight this provides. The Discussion Paper also notes that there is potential for risks and harms. Data protection harms that can arise in financial services include:

   - Presentation of information by firms in a way that limits consumer control or nudges them to poor decisions about the use of their personal data.

[1] ICO25 strategic plan | ICO
[2] The FCA Discussion Paper defines 'Big Tech' firms as large technology companies with established platforms and extensive customer networks. We use the term 'Big Tech' in this broad sense throughout our response.
[3] Competition and data protection in digital markets joint statement (publishing.service.gov.uk)
[4] The Discussion Paper does not focus on the technology services Big Tech firms can provide to financial firms, such as cloud services. Therefore, our response does not cover how the Network and Information Systems Regulations (which concerns the security of systems, including cloud services) applies to these firms.

- Poor data security measures that lead to a breach could result in financial loss, for example, if payments or deposit information is disclosed and leads to fraud.
- Personal data provided for financial services purposes could be unlawfully repurposed (eg for marketing or personalisation on online platforms), infringing on individuals' information rights.
- Inaccurate, out-of-date information collected about a consumer could create financial harm if it is used to (incorrectly) inform a consumer's credit rating.[5]

10. Data protection law provides the guardrails that ensure all firms' (including Big Tech firms') data processing activities respect individuals' information rights and limit the risks of harm. Firms must abide by the principles that lie at the heart of the UK GDPR[6]:
    - **Lawfulness, fairness and transparency:** this principle limits the risks of consumers being misled about how firms process their data and mistrusting how their personal data is used in a market.
    - **Purpose limitation:** this principle ensures firms do not reuse or repurpose personal data they have collected from consumers, without having a legitimate, lawful basis for doing so.
    - **Data minimisation:** this principle places a restraint on firms from collecting and processing more personal data than is necessary for delivering their product or service.
    - **Accuracy:** this principle means firms are responsible for ensuring personal data, which can materially influence and impact consumer engagement with financial services, is up to date and correct.
    - **Storage limitation:** this principle means firms can only keep personal data for as long as it is necessary for upholding the original purpose of the processing.
    - **Integrity and confidentiality:** this principle requires that data is kept safe and secure – with appropriate protection in place against unauthorised and unlawful processing, and accidental breaches.
    - **Accountability:** this principle places a clear onus on firms to be responsible for – and be able to demonstrate – compliance with these data protection principles.

11. Personal data processing is also subject to extra protections if it qualifies as 'special category data' under the UK GDPR.[7] An example of

[5] Overview of Data Protection Harms and the ICO Taxonomy
[6] The principles | ICO
[7] Special category data | ICO

special category data processing that could support the provision of financial services is genetic and health data for insurance products. Furthermore, the PECR[8] regime protects consumers and promotes good practice for activities relevant to financial services, such as direct marketing and the use of cookies and similar technology to personalise and target content, including ads.

12. Data protection law takes a flexible, risk-based approach to protecting consumers. The protections we've outlined helps ensure risks of harm for financial services consumers are mitigated and the processing of personal data occurs in a lawful, fair and transparent manner.

Aligning data protection and financial service regulation objectives

13. Data protection and financial services regulation can work together to promote consumers' interests; both now and in a potential future where Big Tech firms play a larger role in financial services markets. Synergies between the ICO and FCA's regimes include:
    - fostering trust in innovative data-driven financial services,
    - promoting consumer choice and control, and
    - supporting a level playing field by ensuring the processing of data by all firms is fair and lawful and individual rights are upheld.

14. There can also be perceived tensions when data protection and competition objectives intersect.[9] To counter this, engagement and cooperation between digital regulators, and between regulators and the industry, is vital. The Digital Regulation Cooperation Forum (DRCF) is important for delivering cross-sectoral cooperation.[10] The ICO is committed to working with our counterpart regulators, including the FCA, and with industry to ensure citizens benefit from competitive, secure and privacy-oriented financial services markets.

Next steps

15. We are keen to engage further with the FCA as its thinking on this topic progresses. We look forward to exploring the synergies between our two regulatory regimes and identifying where we can work together to mutually reinforce our respective regulatory objectives relating to potential Big Tech entry and expansion into financial services markets.

---

[8] What are the Privacy and Electronic Communication Regulations? | ICO
[9] Competition and data protection in digital markets joint statement (publishing.service.gov.uk) pp. 23-26
[10] The Digital Regulation Cooperation Forum - GOV.UK (www.gov.uk)