Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

Smart Data Review
Consumer and Competition Policy Directorate
Department for Business, Energy and Industrial Strategy
1st Floor
1 Victoria Street
London
SW1H 0ET

6 August 2019

Dear Sir / Madam,

Smart Data: Putting Consumers in control of their data and enabling innovation

The Financial Services Consumer Panel is an independent statutory body. We represent the interests of individual and small business [1] consumers in the development of policy and regulation of financial services in the UK. We welcome the opportunity to respond to the Department for Business, Energy and Industrial Strategy consultation on Smart Data.

While we recognise and support many of the technological solutions this consultation paper addresses, we still believe that more work is needed to inform consumers about both the risks and benefits smart data could bring.

The consultation recognises that much work is already underway in financial services. There is some hope that Open Banking, the pensions dashboard, and other data-driven and fintech-based competition remedies may produce some consumer benefits, but it still seems unlikely that they will deliver a tech-driven nirvana to address the harm to consumers of staying in poor value products when better ones are offered by their existing providers.

Open Finance has the potential to give firms access to far more data, which could lead to poor consumer outcomes if firms do not use the data only to act in consumers' best interests. To address this risk, use of data should be limited to specific, clearly stated purposes. The chain of providers who can access the data from one consumer consent should also be limited. Government should be very clear about the problems and harms it is hoping Smart Data will address, and not simply open up access to data to see where it leads.

Within financial services, data ethics should form part of regulation, including ensuring individual accountability through the Senior Managers & Certification Regime (SM&CR).

Consultation Questions

<u>Enabling data driven innovation in consumer markets</u>

Q1. Do you agree with the proposed objectives and expected benefits of Open Communications? Are there any other benefits or risks that we should consider?

We limit our response to the financial services sector. However, in cases where data shared over Open Communications includes mobile payments, consideration should be given to how this may be considered consumer financial data and therefore accrue more protection.

People are often subject to scams which are enabled over SMS. It would be pertinent to consider how Open Communications may give rise to increased risk of fraud, and what mitigations could be put in place to reduce this.

[1] By 'small businesses' we mean microbusinesses and smaller SMEs

Social engineering scams often involve fraudsters pretending to be from companies, including telecoms providers. Fraudsters access credentials on this basis and then take over accounts or make payments from them. Telecoms providers should be part of a campaign to provide consumers with clear warnings that they will never ask for consumers' credentials and play their part in providing compensation to consumers who are inadvertently scammed.

Moreover, the introduction of Secure Customer Authentication in September 2019 as a result of the Second Payments Services Directive (PSD2) means that banks are increasingly going to be using mobile phone text messages to send authentication codes to consumers. This means that the value to scammers of fraudulently taking over a mobile phone account will increase substantially. This type of fraud exists already, but it is likely to become more common.

Q2. What is the most effective approach to implementation to ensure the success of Open Communications in enabling innovation and delivering the best consumer outcomes?

Digital exclusion is a key issue in the UK and has an impact on people's ability to access financial services in areas where there is limited access to branches. Mobile phones are increasingly important in facilitating people's financial lives and thus ensuring digital inclusion is imperative. This includes either ensuring all consumers access to a working mobile phone signal, or ensuring alternatives are available.

Smart data initiatives will only be as successful as the accuracy and availability of the data that is required to support them.

Q3. Are there any further actions we should take to enable consumers to benefit from Smart Data in regulated markets?

See our responses below.

Q4. In which other markets, outside of the regulated and digital markets, would there be the greatest benefits from Smart Data initiatives? Please explain your reasoning

It may be helpful to enable consumers to access more detailed purchase data from retailers, like supermarkets. Currently, Third Party Providers (TPPs) cannot accurately categorise spending where retailers offer multiple types of products under one roof, for instance, groceries and clothing. This problem extends to the provision of debt advice, where intervention is still required to categorise payments.

Q5. What other roles might industry find it useful for Government to perform in addition to it acting as a facilitator for Smart Data?

Purpose

Government should be very clear about the purpose of data sharing and how it will address the needs of vulnerable people in particular, who are unlikely to benefit if they are not online and cannot meaningfully manage the risks. Government should be very clear about the problems and harms it is hoping Smart Data will address, and not simply open up access to data to see where it leads.

Creating markets and serving vulnerable people

Simply making data available does not create a market in and of itself. Thought should be given to the supply and demand of intermediary services, that are (currently) under no obligation to use the data that is made available. For instance, the Service Level Indicators required by the CMA Order are not being utilised by comparison websites. The envisaged personalised comparison services for current accounts have also not materialised.

Government could give regulators powers to consider what else may be needed to make Smart Data Initiatives work properly, including measures that consider adoption, distribution and creating a level playing field for new entrants. Access to data for training algorithms is important in reducing risk to consumers and enabling firms to assess the potential impact of their algorithms.

Where there is a limited business case, firms may struggle to get products adopted en masse. People who are traditionally excluded and vulnerable will remain so unless commercial incentives align with their needs. For instance, in the credit sector, there is demand among firms to access more accurate data so they can mitigate their risks of consumers not meeting their repayments. Consumers are also more willing to share their data where they have a strong desire for credit which over-rides their caution. However, there has been very limited innovation in the credit products provided, suggesting that firms are getting what they need but consumer needs for cheaper alternative overdrafts, help getting a better product at the end of balance transfer offers etc, remain unserved.

Technology harmonisation and implementing the APIs properly

The Consultation document is encouragingly bold in suggesting that all data should only be made accessible over APIs. The design principles for these APIs should ensure utmost security and privacy. This would set expectations and provide certainty to the industry about what it could expect when.

However, screen-scraping will persist where APIs are not available, meaning that firms wanting to offer holistic services will have to maintain both.

We believe the Government should phase out screen-scraping in order to create a strong motivation for the industry to sign up to the API standards (especially in financial services where such a standard exists for PSD2 regulated accounts and could be easily extended to other similar products such as savings accounts with limited cost impact). However, this relies on:

- APIs being available to support the data flow; and
- APIs being implemented properly by firms (who may not have an interest in sharing the data, due to the competitive threat)

In the event where firms cannot use screen-scraping and the data is not readily available, they may use reverse-engineering. The Government could work with regulators to ban such practices which undermine security and consumer control over their data. Regulators should intervene early before undesired practices become established.

We believe the Government should have a strategy for implementing secure and privacy enhancing APIs across sectors, banning alternative forms of data-sharing, including within the financial services sector.

Informed consent

While we recognise and support many of the technological solutions this consultation paper addresses, we still believe that more work is needed to inform consumers about both the risks and benefits smart data could bring.

In 2018, we commissioned research to understand better what financial data sharing really means for consumers.[2] The findings from this research were not surprising:

- People don't really understand the value of their data;
- Even when people read terms and conditions, they are usually none the wiser;
- They rely on reviews, or a vague feeling that government and regulators are looking after their interests; and
- People value privacy, but not as much as speed, when they want goods or services.

Consumers' clear preference for speed and convenience must coincide with better consumer protection measures, such as an overhaul of online terms and conditions and so-called privacy notices, in order for the potential benefits of data sharing to be realised.

The ability to merge account data with geographical data, social media data, health data or behavioural data collected from other sources complicates the issue of informed consent. Consumers should be made aware that the data they consent to share could be supplemented

[2] https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf

by data that they did not consent to share, or consent to share for this purpose, or did not realise was publicly available.

Consent management and consent switching

The Smart Data Consultation provides an opportunity to consider the regulatory regime for data sharing. The proposals are helpful but do not go far enough to ensure consumers can manage their data, or multiple data sharing arrangements easily.

Government should consider, in the event of a successful data sharing eco-system, how consumers will be able to manage multiple consents with multiple providers across multiple sectors. The landscape could become confusing quickly. Steps to bring harmonisation to consent, authentication, real-time revocation of consent, re-authenticating etc could help. Further consideration should be given to whether consumers should be able to manage all their consents in one place (including allowing them to revoke access etc). This process will be complicated by the fact that consumers may be willing to share some information quite widely where it is relevant to the provision of a range of services, but will be unwilling to share that information with other services providers or government bodies who do not need to know. For example, somebody on home dialysis might want their electricity and water suppliers as well as their hospital to be aware that they need continuity of service, but their bank, mortgage provider, phone company and local authority do not need to know this.

Furthermore, the Government should provide for technology to enable the seamless switching of consents between providers. The current PSD2 regime means that consumers will face additional hurdles in switching their current account because they will need to manually re-establish all the consents with TPPs, including re-authenticating these with the new provider. This has the perverse effect of potentially making current accounts even stickier, which appears to contradict the aims of improving competition.

Data training and algorithmic governance

The rise of data-driven services sits alongside the growth in artificial intelligence. The risks associated with big data and AI have still yet to be fully understood. Government should introduce a regulatory regime for AI to ensure that firms adhere to robust standards for the use and analysis of people's data.

RegTech

Government should require more investment in RegTech to keep pace with firms' investment in their own commercial objectives. RegTech would seem to present an opportunity to ensure that new services can be appropriately monitored and supervised.

Q6. Do you agree that we should establish a cross-sector Smart Data Function with the proposed responsibilities set out above?

Government needs to establish a new regulatory regime for data sharing, especially where consumers' financial data is being used by non-financial services companies. This regime should consider whether there are circumstances when it would not be appropriate for certain types of provider to access consumers' financial data.

It will be possible for consumers' financial data to be shared with non-financial services providers and vice versa. It needs to be clear to consumers how they can make a complaint or claim redress if their financial services data is breached by a firm not covered by the Financial Ombudsman Service (FOS). The process for redress through the Information Commissioner's Office (ICO) needs to be more accessible and should not require consumers to have to take their claim through the courts.

Q7. What would be the best form for the Smart Data Function to take? Should it be, for example, a new body, part of an existing body or some other form?

In the light of our comments under "Purpose" in our response to Question 5, we believe a new body should be established. The Open Banking Implementation Entity (OBIE) should be part of this new body.

Q8. How can we ensure that the costs of Smart Data initiatives are shared fairly between the participating businesses?

As we have set out above, the funding of Open Banking, by the CMA9, has had limitations. A whole of market solution should be funded in a way that will ensure technology can be developed to benefit consumer outcomes. The regulator should have the ability to raise levies to fund open finance, should that be deemed the best or most appropriate mechanism.

Using data and technology to help vulnerable consumers

Q9. What other actions could the Government or regulators take to support the use of data and innovative services to improve outcomes for vulnerable consumers?

We believe that the government and regulators should carry out more research, including with focus groups and citizens panels, to understand what is acceptable use of individuals' data and what level of data sharing may be deemed socially acceptable or preferable. Research should also determine whether peoples' appetite and comfort level with data sharing is context-specific, which may mean differences between markets which should be taken into account. We also encourage the FCA to use its Financial Lives survey, or other research methods, to understand more about how consumers' financial and data lives intersect.

All firms, including third parties, that take data should be required to have no conflicts of interest and to act in the best interest of the consumer whose data it has taken. Firms should be clear whose interests they should be acting in, and should owe a duty of care to their customers.

If a consumer has been identified as vulnerable, they should still be able to choose whether or not they wish to be classified as such. Their right to privacy should be protected and they should be able to choose for firms not to record specific information about them if they wish.

In 2017, the Panel carried out research [3] looking at consumers and competition, and in particular how far it is reasonable for competition authorities to expect consumers to drive competition. In reaching its conclusions, the research took into account the automated switching market and found that automated decision-making, based on consumers' own profiles and preferences could have the potential to provide better consumer outcomes. However, we also made clear that regulators should ensure the market develops in the interest of all consumers and prevent consumer exploitation.

For example, firms could use transactional information to market other products beyond financial services. They could use it to assess how much the consumer is willing to pay for a service, their propensity to use credit or take out insurance add-ons. Checks and balances (such as algorithmic governance) are required so that firms do not exploit data in ways that are detrimental to consumers. Consideration should also be given to whether consumers should have a right of appeal against decisions made by an algorithm.

Q10. Should we strengthen the powers of sector regulators to enable them to use consumer data to improve their understanding of the challenges faced by vulnerable consumers and to intervene to improve outcomes?

Yes. There are benefits to be realised from regulators developing big data sets, which may allow them to begin to recognise patterns, model impacts, and understand algorithms better. The Global Open Finance Centre of Excellence is trying to get the CMA9 to share real, anonymised data on consumers transactions, in order to begin to understand the interactions between that data. Data sets released in this way could aid socially responsible developments and improve outcomes for all consumers.

Q11. How can we ensure that the Smart Data Function improves outcomes for vulnerable consumers? Do we need to consider any further actions?

[3] https://www.fs-cp.org.uk/sites/default/files/fscp_consumers_and_competition_position_paper.pdf

The Smart Data Function has the ability to help bridge the digital divide. Generally, people who are not online, for whatever reason, tend to be vulnerable. More needs to be done to ensure there is full coverage across the UK and people can access services affordably. It should be borne in mind that technology imposes significant costs on consumers. In particular, apps will often only work with the latest hardware, so consumers may have to upgrade their phone or tablet every 2-3 years. This will be unaffordable for many.

To date, there has been no suitable consumer awareness campaign about rights to share data, so many consumers, as our research referred to in our response to Question 5 above identified, will be unaware that they are sharing their data as well as the potential consequences of doing so.

Government and regulators should be very clear about the problems and harms they are hoping Smart Data and Open Finance will address, and not simply open up access to data and see where it leads.

New data services have the potential to allow firms to provide services for consumers that will make a difference to their lives. These changes need to be inclusive and bring all consumers on the journey. The 4th Industrial Revolution cannot leave behind great swathes of the population.

Protecting consumers and their data

Q12. Do you agree these protections for when TPPs use Smart Data are needed? Are there others we should consider?

Consumers will need to know how to find out which firms are legitimate and which ones aren't. Directing people to the FCA register will not be sufficient. Social engineering scams often involve fraudsters pretending to be from legitimate companies, and there must be a way for consumers to know they will not easily fall victim to phishing or other scams. Moreover, as we have seen recently, firms can be on the FCA register for a single minor activity, but also be undertaking a range of unregulated business as well.

As we say above, Government should phase out screen-scraping in order to create a strong motivation for the industry to sign up to the appropriately-designed API standards. Consumers should have more information on their rights in relation to their data, as well as an understanding of what consent means and how to revoke it. Revoking consent should be as easy as consenting was in the first place. Consumers should not be required to 'register' with a firm to revoke their consent if they were not 'registered' in the first place to provide the consent (this could be the case where an Account Information Service Provider (AISP) has provided a service to another firm, a lender for instance).

The process for onward sharing data of data beyond the Third Party to the Fourth Party to the Fifth Party and so on, needs consideration. The more parties involved in a supply chain, the higher the chance of a data breach, and the more difficulty there will be to address liability. If a firm wants a consumers' data, they should be regulated and access it directly from the consumer, rather than through another party.

Q13. How should our proposed approach to accreditation operate in practice if it is to effectively ensure that consumers' data are protected and minimise burdens for TPPs?

We agree with the principle that providers accessing consumers' data should be accredited and required to meet high standards of security for the transfer and storage of consumers' data. Financial data is a high-quality data set and thus 'high risk'. Its use should be limited to accredited providers only.

Q14. What are the advantages and risks of introducing a cross-sectoral general authorisation regime for TPPs?

A general cross-sectoral authorisation regime for TPPS should cover only the access to the data. We would expect sector regulators to take responsibility for the conduct of firms use of the data. Sector regulators should be held accountable for firm conduct but it may be useful to

review the boundaries between each regulator and the ICO to ensure no consumers can fall between the gaps. It may also be necessary to review the powers of regulators to ensure that, where a firm uses data from across sectors, regulators have sufficient powers to act together where there is misconduct.

Where TPPs do not have a sector regulator to ensure good conduct, consideration should be given as to whether it is appropriate for them to access the data. BEIS may need to consider a new regulatory body for intermediaries who are not currently within the purview of conduct regulation.

BEIS must ensure that is an appropriate liability and redress regime in place to ensure consumers are protected from the variety of unhappy pathways that could materialise with the increased risks associated with data sharing.

Q15. What other options should we consider to ensure that consumers are protected when using TPPs?

Conflicts of interest between firms is the one thing most likely to undermine the smart data initiative. Those with access to consumers' data should be working on behalf of, and to improve the outcomes of, those consumers at all times. We believe that an actionable duty of care to be owed by firms to such consumers would provide necessary protection. A guarantee that consumers will be better off for having shared their data would engender trust and also set a clear bar for firms to improve consumers' situations.

Yours faithfully

Wanda Goldwag
Chair, Financial Services Consumer Panel