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

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

Policy
Financial Conduct Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

12 June 2017

Dear Sir / Madam,

CP17/11 Implementation of the revised Payment Services Directive (PSD2): draft Approach Document and draft Handbook changes

This is the Financial Services Consumer Panel's response to CP17/11 Implementation of the revised Payment Services Directive (PSD2): draft Approach Document and draft Handbook changes.

The Panel recognises that PSD2 will be implemented mainly through Regulations, which HM Treasury consulted on in February 2017. We repeat here a number of the points we raised in our response to that consultation as they are still relevant.

Much of the FCA/PSR consultation deals with the technical details of implementation, which are principally for firms to respond to. We are responding only to those questions where we have specific points to raise. There are, however, a number of broader points that the Panel wishes to make:

- **Overall approach -** A key purpose of PSD2 is "*to improve consumer protection, make payments safer and more secure, and drive down the cost of services*". We support these objectives. The FCA's approach must ensure that the risks to consumers arising from authorising Account Information Service Providers (AISPs) and Payment Initiation Services Providers (PISPs) should be managed effectively. It is imperative that the FCA has the necessary powers to do its job and that the Information Commissioner's Office (ICO) has sufficient resources to do its job too. We continue to urge HM Treasury to ensure that consumers do not suffer detriment as a result of the patchwork of legislation in this area and the differences in approach between regulators to supervision and enforcement.

- **Authorisation:** Consumers, as well as all types of data controllers, need to be able to know whether or not an AISP or PISP is authorised, and by whom. The FCA must ensure that information about firms it authorises is available in real time, even if the European Banking Authority (EBA) register is not updated as frequently. This will place greater reliance on the FCA Register. The Panel has argued many times that the Register is not fit for purpose. We would like reassurance that it will be up to the job here. In addition, while it will be for the FCA to authorise new firms, the primary mechanism to protect customer data will be via the General Data Protection Regulation (GDPR) which is policed by the ICO, rather than the FCA. It will be essential for the FCA to work closely with the ICO to ensure that authorisation is robust and takes more account of the provisions of the GDPR.

- **Business models and charges -** AISPs and PISPs need to be transparent about charging. If they are offering "free" services to customers then they must explain what the customer is giving in exchange. There should be transparency about business models so that consumers can easily understand how AISPs and PISPs make their money, and are informed of any commission or payment arrangements made between different organisations. The FCA should consider the impact of business models on end-users when authorising and registering AISPs and PISPs.

  It will also be important for consumers to receive clear information about charges where a third party initiates payment from a customer's credit card. In this instance, the customer may be subject to two different charges: one relating to interest on the credit card; the other relating to the money transfer. Where this occurs, the FCA should make firms disclose both sets of charges in a clear and transparent manner.

- **Data handling and security** – This is a conduct issue, even if the primary regulator is the ICO. If AISPs/PISPs and Payments Service Providers themselves want to process/sell consumers' data, then they should provide simple information about this upfront so it is clear what they are doing. The FCA needs to adopt a joined-up approach with other regulators to ensure that consumers receive a consistent level of protection that is delivered through the appropriate sector regulator.

- **Consumer consent -** It is not clear how consumer consent for AISPs and PISPs to access their account data is intended to work. The Approach Document makes clear that AISPs and PISPs should make available to consumers the information needed for them to make an informed decision and understand what they are consenting to (Paragraph 17.43) yet it is unclear how this will be verified. As we know, simple information disclosure is unlikely to be enough for consumers to make an informed choice and much could be gained from applying the learning from the Smarter Communications work by the FCA in this context. We suggest the FCA consider in more depth how AISPs and PISPs evidence their customers' explicit consent to terms and conditions that they may well not understand. We also question how AISPs will enable consumers to differentiate between explicit consent to share and process payments data generally, versus explicit consent to share and process what may be considered 'sensitive payments data' under the GDPR.

- **Consumer control -** The Panel is also concerned that, once consumers have allowed access to their data by a third party, they will no longer be in control of how it is used. This includes how and where the consent can be reviewed, how it can be limited or withdrawn, and how the consumer can be certain that the AISP has acted on the revoked consent and it is no longer continuing to request data from the bank. The FCA may wish to provide more guidance in its Approach Document on the withdrawal of consent. There should also be greater regulatory co-ordination of the data consent issues that will affect every consumer under the GDPR. There is a risk to consumers from different regulators having responsibility for different aspects of the relationship between providers and consumers. As it stands, the FCA will legitimise AISPs and PISP services through its authorisation process. However, it will not be the primary regulator responsible for supervising or enforcing the GDPR, which will be the primary vehicle for protecting consumers from the main risks that arise from sharing their data. Under what scenarios would/could the FCA revoke authorisation for misconduct under the GDPR?

- **Clarity on liability** – It must be made clear to consumers where liability lies if something goes wrong, and where complaints should be directed. There is a clear liability mechanism for Payment Initiation Services (PIS) under the proposed approach. This says that if a payment is made in error the customer should approach their bank, the bank will refund them and then pursue the third party for the money owed. It is intended that this single point of contact should make it easier for consumers. We understand the rationale for adopting this approach but would suggest that the FCA should be aware that if a consumer interacts directly with a PISP it may seem odd or unduly complex to mandate that they should complain to the bank. In addition, if banks are ultimately liable for customer loss under PSD2 they may have a vested interest in dragging their feet in seeking a resolution. FCA should ensure the system is not able to be 'gamed' in this way.

  Of real concern, however, is that there is no similar liability framework for Account Information Services (AIS) in the event of data breaches. It is not clear what consumers should do if their data has been erroneously transferred, or indeed which organisation they should approach. We encourage the FCA to consider how to plug this gap. The Approach Document (17.24) says that an Account Servicing Payment Service Provider (ASPSP), such as banks, building societies and credit card providers, must not prohibit or discourage customers from using an AIS and PIS. We agree. However, we do question how consumers can be expected to take responsibility in this context when an explanation of the truth may be considered anti-competitive. For instance, is it acceptable for a data controller (in this case the ASPSP) to explain that the onward sharing of your data is done at your own risk and that the supply of service by the third party is not their responsibility?

- **Sensitive payments data –** We believe that the FCA should list potential types of sensitive payments data in 17.48. We understand that the EBA has shied away from doing so in its Guidelines. However, as it currently reads, only credentials may be considered 'sensitive'. Other types of payments data may enable a third party to infer sensitive information about the individual and can therefore be considered 'sensitive payments data'. It is important to signal what might constitute sensitive payments data for consumers and their advocates as much as it is for ASPSPs and Third Party Providers (TPPs), and that it is acceptable for AISPs to store such data with explicit consent.

- **Redaction** – Consumers need to be able to specify that redacted data is shared only where transactions involve sensitive information (e.g. healthcare payments, certain subscriptions or donations) or payments to or from other individuals who have not given their consent to their data being shared (sometimes referred to as "silent parties"). It is for the consumer, not the payments service provider (i.e. usually the bank) to decide whether or not information about a payment should be redacted before being shared with a third party. We believe that the right to redaction is in line with consumer rights contained in the GDPR. We recommend that as part of the authorisations process the FCA, with input from the ICO, should mandate that consumers have the right to redact their own data before it is passed to third parties, and to consider how consumers can ensure that they are not obliged to share sensitive information (e.g. about medical payments, debts, fines, gambling). In addition, the FCA should consider how individuals on the other end of disclosed transactions (as payers or payees) ensure that their information is not disclosed against their will and that they can exercise their 'right to be forgotten' (right to erasure).

- **Resourcing -** Since this is a new and evolving area featuring rapid innovation, the FCA must ensure that it has adequate resources, as well as the technical

skills, to conduct appropriate checks at the authorisations stage and supervise and enforce the new risks associated with PSD2, Open Banking and big data. Failure to do so risks causing reputational damage to an industry in its infancy, and potential widespread consumer detriment.

- **De-risking** – The Panel supports the proposal that credit institutions must provide to the FCA the reasons for the refusal or withdrawal of access to payment account services. We also understand the importance of not 'tipping off' a potential fraudster but ask that ASPSPs and TPPs provide information about CIFAS and the appeals process to consumers in cases of forced account closure.

- **Complaints –** The Panel supports the shorter timescales for resolving complaints. The reduced timescales should be communicated clearly and firms' performance published.

- **Amendments to BCOBS** – The Panel supports the proposal to extend BCOBS to cover deposit takers which are exempt from PSRs 2017. This move will provide a more consistent level of consumer protection.

Yours faithfully,

Sue Lewis
Chair, Financial Services Consumer Panel

Answers to specific questions:

Q2: Do you have any comments on our proposed limited network exclusion guidance in the draft PERG text (Appendix 1)? Do you have any comments on the proposed limited network exclusion notification (draft direction and draft template in Appendix 2)?

The Panel supports the standardisation of the exclusion, which means that the exclusion for payment methods that can be used in only a limited way (e.g. gift or store cards), will apply less widely.

Q4: Do you agree with the proposed guidance related to the definition of AIS and PIS in PERG 15.3? Are there any business models which you believe could be inappropriately viewed as in or out of scope in light of our guidance? If so, please provide us with details of these business models.

We agree that the definitions should be drawn broadly so that they will, as far as possible, be future-proof and apply to new business models or approaches which may emerge, giving the FCA the flexibility required to react to new issues.

While we welcome the guidance on the types of business activity that constitute AIS and PIS, we question whether the definition of AIS is sufficiently broad. In particular, we ask the FCA to consider whether the current guidance captures adequately the activities that may take place in the context of retailers making use of 'Big Data' when undertaking marketing activities.

We also note that Question 9 of PERG states that debt management companies would not be deemed to be providing payment services as a regular occupation or business activity, and would therefore not require authorisation or registration under the regulations. However, a debt management company may have a legitimate interest in accessing a customer's payment accounts, providing what might be considered account information services, for example helping them manage their money on a continuing basis. We believe that this should not be considered an 'ancillary' service but rather a core business service.

Q6: Do you agree with the proposed approach to implementing the new authorisation requirements for authorised PIs, and authorised EMIs, and the registration requirements for RAISPs? If not, please explain why not and suggest an alternative approach?

Yes. However, in addition to requiring RAISPs to include information about their risk management procedures within their application (as at Paragraphs 3.122 – 3.125), the Approach Document should also include reference to the ethical risks relating to the use of data. Where companies use multiple sources of data, including data from banks, they should also consider the need for a means to manage ethical considerations, as well as a risk management function.

As part of the registration process, a RAISP is asked to provide a range of information. We consider that this should be extended to include information about the proposed business model. This would help to provide insight into how the RAISP intends to generate income, and would help to shed light on any potential conflicts of interest which may work against, easily mislead, or exploit vulnerable consumers.

Q10: Do you agree with the guidance we propose in Chapter 8 of the revised Approach Document in relation to changes to information requirements, rights

and obligations and other changes? If not, please explain why not and suggest an alternative approach. Please provide the paragraph number when commenting on specific wording.

Yes.

We also welcome the reduction to £35 as the maximum amount that a customer can be made liable for in the event of an unauthorised transaction arising from the use of a lost or stolen payment instrument. We note that there will also continue to be situations where the customer is not liable for any amount.

Q12: Do you agree with our proposed Handbook changes to implement the PSD2 complaints handling requirements? If not, please explain why not and suggest an alternative approach.

We agree with the proposed application of reduced time limits to both PSD complaints and EMD complaints. We consider that issuing e-money is closely linked to payment services, and customers would benefit from shorter timescales and the application of a more consistent approach.

We also support the retention of DISP 1.5 (complaints resolved by the close of the third business day) for PSD and EMD complaints. In our view, this should help to incentivise even speedier resolution of complaints.

Q13: Do you agree with our proposed changes to the timeline for referrals to the Financial Ombudsman Service? If not, please explain why not and suggest an alternative approach.

Yes.

Q14: Do you agree with our proposed changes to BCOBS? If not, please explain why not and suggest an alternative approach.

We support fully the changes which should help to ensure customers have consistent levels of protection. We agree that the extension of BCOBS coverage is very important and will help to deliver a consistent level of protection for consumers.

Q15: Do you agree with our proposal to extend complaints reporting to payment institutions and e-money businesses and to introduce a new reporting form for all PSPs? If not please explain why not and suggest an alternative approach.

Yes. Collecting this information should enable the FCA to proactively monitor payment institutions and e-money institutions, and to identify potential sources of concern which may merit further investigation.

Q16: Do you agree with our proposals for reporting of statistics on fraud relating to different means of payment? If not, please explain why not and suggest an alternative approach.

Yes.

We think the collection of data will shed light on the need for more proactive steps to protect consumers in the light of the Which? super-complaint. We look forward to the FCA sharing the data it collects and using it as a benchmark to assess whether the joint

steps it is taking with the PSR reduce the incidences of people being scammed or defrauded on push payments.

Q19: Do you agree with our proposed guidance on PSPs' access to payment account services, as set out in chapter 16 of the revised Approach Document? If not, please explain why not and suggest an alternative approach. Is there anything additional that it would be useful for us to provide in our guidance?

Yes, we agree that the FCA should ask for information so it is able to assess whether credit institutions have complied with their obligations to grant access on a proportionate, objective and non-discriminatory basis.

Q21: Do you agree with the guidance we set out in Chapter 17 of the revised Approach Document, including the proposals for guidance set out above? If not, please explain why not and suggest an alternative approach?

We note that banks cannot require AISPs or PISPs to enter into a contract to gain access to consumers' payment accounts. However, as we set out in the cover letter, it needs to be made clear to consumers where liability lies if something goes wrong and that quick redress will be forthcoming.

Paragraph 17.32 of the Approach Document makes clear that such contracts can be agreed if they are mutually beneficial to both parties. Where such arrangements are entered into, it would seem odd if they could not include an approach to liability and consumer protection that is agreed by both parties. The FCA may wish to review a sample of such contracts however to ensure that ASPSPs are not able to manipulate TPPs that may be in a weaker position to negotiate but nonetheless would prefer to operate under a contractual arrangement for their own protection.

Q22: Do you agree with our proposals to direct the form, content and timing of notifications that must be provided where access has been denied to providers of AIS and PIS, including the proposed notification form in Appendix 1? If not, please explain why not and suggest an alternative approach?

Yes.

Q24: Do you agree with our proposed approach to supervising the PSRs 2017? If not, please explain why not and suggest an alternative approach?

We agree with the overall approach, and the move to adopting supervisory measures based on the risk posed by an individual business, their category of business or the sector as a whole. However, it will also be important for the FCA to have sufficient flexibility to react to new, emerging risks. We would request the FCA keep the emerging AISP and PISP market under regular review.

Payment Systems Regulator questions

Q30: Do you agree with the Payment Systems Regulator's proposed approach to monitoring compliance with Regulation 61 of the PSRs 2017? If not, please explain why not and suggest amendments. Is there anything additional that it would be useful for us to provide in our guidance?

We agree that it is right to ensure clear messaging is provided to consumers from independent ATM deployers. Working in collaboration with others (LINK, Visa and Mastercard) seems the right way to deliver this.