Subject: EMA Response to TPP Side Consumer Protection Consultation (Roadmap Item A12)

Date: 16 November 2020

Background

The UK Open Banking Implementation Entity (OBIE) are seeking feedback on the TPP Guidance which has been prepared in support of the delivery of the OB Roadmap item A12 – TPP-side Customer Protection.

The draft Guidance includes:

- Classification of the Purpose of Consent, and proposes how to address what has previously been referred to as "codification of the purpose of data sharing".
- Security and fraud, replacing the Participant Guides for Information Security Operations and Counter Fraud Operations, and the Security and Fraud sections within the TPP Operational Guidelines.
- Complaints and redress, replacing previous content within the TPP Operational Guidelines.

In-line with the scope of the Roadmap item A12, the OBIE are also looking for views on whether or not it would be **appropriate to develop the TPP Guidance into a Voluntary Code of Conduct with the ICO**.

EMA Response

The following EMA comments will be submitted via the OBIE Confluence feedback page.

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
1	A-12 TPP Consumer Protection Consultation Document	**1.3 a. Gaps in Regulatory Framework**	Aspects of the UK's implementation of PSD2 and GDPR would benefit from review, clarification, and more guidance, in particular with regards to: • 90-day reauthentication - AISPs should be able to operate continuous, unattended access to payment accounts, without the need for the PSU to provide authentication to the bank every 90 days • Regulatory perimeter –PISPs should be able to access relevant AIS data in order to manage their transaction risk assessment (even if they don't intend to offer AIS products.) However, we do not believe there are gaps in the regulatory framework for PSU consent and permissions which is the scope of the A12 Roadmap item.	H
2		**1.3 a. Areas of this Guidance which are of most use.**	TPPs have to navigate numerous pieces of legislation, regulatory guidance, opinions, and industry standards in order to gain authorisation and maintain regulatory compliance. In principle, sharing best practice is of benefit to the whole market, particularly for start-up businesses or those new to the regulated environment. However, sections 3-5 of the proposed Guidance provide high-level, general advice that is not specific to the Open Banking standards or ecosystem, and it is not clear how this adds-value to the existing body of	H

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
			regulatory material. In addition, there is a risk of oversimplifying guidance where TPPs have regulatory obligations. Whilst section 2 – *Classification of the Purpose of Consent*, provides specific guidance in relation to Open Banking. It does require expanding so that the 'purpose of consent' classifications can be consistently implemented in customer journeys (see our suggestions under #6). We would prefer that the TPP guidance focuses on OB ecosystem or standards guidelines, but have provided comments on the security, fraud operations, and complaints handling sections below for completeness.	
3		**1.3 b. Additional guidance that would be helpful**	We believe there is scope for developing further guidance for handling disputes within the OBIE ecosystem. Please see suggestions under #11.	L
4		**1.3 c. Support voluntary (eg Code) or prefer regulatory action to fill gaps identified**	The Executive Summary suggests that the voluntary Code would encompass all the topics covered in the draft guidance. We would welcome clarification from OBIE on whether this is the intent. It is not clear why a 'Code' is necessary in the areas which are already covered by regulatory obligation (security, fraud, complaints handling), nor whether the ICO would be the appropriate overseer if these topics were contained in a voluntary Code.	H

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
			We would welcome further clarification on why a voluntary 'Code' on the purpose of consent classifications is required, if the recommendations are going to be implemented via OBIE's CEG.	
5		**1.3 d. Views on the optimal options for governance and enforcement of a Code**	As discussed above, we do not believe that the rationale for a separate Code has been sufficiently explored and established yet to comment on the governance and enforcement options.	L
6		**1.3 e. Views on the purpose consent classifications**	In general, we support the 'purpose of consent classifications' that have been defined by the CEF. However, our key concern is how the classifications remain current in a rapidly evolving and expanding Open Banking ecosystem to be of practical benefit to end consumers. In addition, further detail on the classifications' practical implementation is required to fully understand the impact on TPPs. For instance: • how and when these classifications should be applied; • how the governing body of any voluntary Code oversee that the classifications are applied consistently across the ecosystem • if included in the OB CEG which elements will be mandatory/optional for TPPs (forming part of conformance testing?) • if a voluntary Code is developed, how will this integrate with the OB CEG, including change management and oversight of implementation	H

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
			• how will the classifications evolve overtime to accommodate new use cases • how will updates/changes to the classifications be propagated through the ecosystem • how will a common understanding of the classifications be communicated to consumers and SME if the application is not applied uniformly by all TPPs. Practically, the wireframes and standard text proposed in the Guidance has not been optimised for mobile customer journeys. Further exploration of the impact on TPP's user experience should be conducted before any guidance is finalised with particular attention paid to whether any required text or messages introduces obstacles to the TPP providing their services.	
7		**3. Security Good Practice Guidance**	This section provides largely generic, sound best practice guidance with some added references to financial services' industry InfoSec frameworks which may be useful in helping start-up firms establish robust security policies and controls that are required of regulated entities. However, TPP's already have to comply with a plethora of EBA GLs covering topics like ICT and Security Risk Management, Operational/Security Incident Reporting, Outsourcing Arrangements, etc. Additionally, TPPs are required to provide detailed evidence of their InfoSec. management framework as part of their application for authorisation. The value of adding additional guidance would therefore seem limited.	M

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
8		**3.2 Security Frameworks**	To reduce complexity and maintain proportionality for smaller firms operating in the OB ecosystem the Guidance should not refer to InfoSec arrangements which may not be necessary. For instance, references in section 3.2.3 to a Security Operations Centre (SOC) and the use of a Security Incident & Event Management (SIEM) platform is disproportionate to the size of most TPPs operations. These are certainly useful Information security arrangements that are used by the larger and more established PSPs; however, a number of TPPs deliver their services securely without ever using such arrangements.	M
9		**4. Counter Fraud Good Practice**	This section contains useful guidance to assist firms with developing a counter fraud strategy and operations. However, the principle of developing appropriate and proportionate risk-based anti-fraud (AF) policies, systems, and controls in-line with the scale and nature of each individual business needs to be made much clearer throughout. As it stands, we have concerns that these TPP Guidelines don't reinforce the concept of developing AF strategies and operations which are commensurate with the fraud risks posed by a given business, in particular for small TPPs. The operational guidance (in section 4.3) in particular, seems to be based on the assumption of significant resources available for AF systems and controls which would not be justified in a small TPP. For example, it is unlikely that small, and start-up TPPs will have, nor require, a "*Counter Fraud Operational department*" as referenced in section 4.3.1.	M
10		**4.6 ONBOARDING KYC AND CDD**	We would suggest that this section is removed from OBIE TPP Guidance in its current form.	H

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
			At the moment the Guidance is extremely generic without fully considering TPP-specific obligations or operations. As the Guidance notes (in section 4.6.8), there exists numerous reference points for firms to ensure compliance with the MLRs. Unless the OBIE guidance can offer additional practical guidance for TPPs implementing CDD policies and controls that goes beyond existing industry and regulatory guidance and best practice, then we consider that this section could be removed.	
11		**5 Complaints and Redress**	As all UK PSPs, are subject to the complaints handling requirements of the FCA, and again we question the added value of a very high-level summary of the rules for complaint handling as set out in Dispute Resolution (DISP) sourcebook of the FCA Handbook. Particularly, when PSPs have further guidance on complaints handling in the FCA Approach Document for Payment Services and E-money. We believe that there is scope for developing additional guidance on how OB participants should handle queries and disputes which arise within the ecosystem. Such as: • Where a PSU disputes that AIS data is correct, and liability for when that data has been used to provide another service. • Where a PSU reports fraud in relation to a transaction initiated by a PISP A consistent approach across the ecosystem for handling disputes will help to drive consumer and SME trust in the services being provided.	M

#	Artefact	Document TOC reference	Feedback	Priority (H/M/L)
12		**5.2 Disputed Transactions (General)**	This section gives the impression that disputed transactions are the only type of complaint that may arise and does not consider AIS-related or data related disputes and complaints.	H
13		**5.2 Disputed Transactions** (First paragraph)	PISPs initiate payment transactions but do not receive or process the funds relating to the subsequent transaction which is executed by the PSU's ASPSP. They cannot therefore "*refund a customer*" as indicated at the end of the paragraph. The ASPSP would refund the PSU in the case of an unauthorised or defective transaction, and thereafter any remaining disagreement with regards the processing of the payment initiation would be a matter between the PISP and ASPSP. All of section 5 should be clear where the guidance refers to intra-PSP disputes, or to PSU-related complaints handling best practice.	M