CMA Open Banking Standards Consultation

ObjectTech

ObjectTech is a company which uses new technologies to create new forms of data ownership and control, and allows new business processes with resilient trust frameworks, cutting edge privacy, strong security, and which removes friction from identification processes.

We are fully supportive of the move towards open banking, as a further step towards a true customer-centric banking sector. The Open Banking Standard will serve as the founding document for a direction of travel in banking and commerce which ultimately leads to the emergence of a banking system with the individual consumer at the centre, without reliance on a third party for the management and monetisation of their data.

However, as technology allows these new business practices, security and privacy become more important than ever. In digital commerce and digital banking, particularly with the involvement of third parties and APIs, privacy absolutely must not be an afterthought or something which is compromised by the interests of third party service providers in any way.

In the context of the Open Banking Standard, privacy means control over which companies you allow to become a potential point of failure in the ownership, control and protection of your personal data.

Informed Consent and revoking consent

A customer may choose to give access to their data to a third party aggregator service – perhaps provided for instance by a comparison website – in exchange for new services. In terms of data, the customer is effectively allowing their private data to be accessed, analysed and monetised by a third party. In doing so, they are potentially exposing their data to a third party's:

(a) poor security management;
(b) human error;
(c) potential internal malicious actors;

While the purpose of the standard itself is to prevent these risks, the combination of (i) the exponential increase in the value of personal data; and (ii) the industrial scale prevalence of data hacking, mean these risks remain incredibly high and likely to increase over time.

Informed consent must therefore be explicit and ongoing, and entail a full understanding of the risks associated with exposing their private data to third parties, in terms which can be easily understood. Something in the fashion of T&Cs, or an explanation which is simply a scroll-down-and-click-accept is not a sufficient means of ensuring informed consent.

Moreover, consent is meaningless if the power to revoke it does not exist, and giving sharing data, even on an informed and free basis should not be difficult to withdraw. Therefore, we believe that there should be explicit recommendations on the revocation or consent and the deletion of data held, and that this should be (i) constantly available and (ii) easily revocable.

Strong reading of GDPR

Open Banking and the Second Payments Services Directive – which are aimed at opening up the banks' internal systems and making use of the valuable data within – sit in potential opposition to the forthcoming General Data Protection Regulation. We would encourage the strongest possible reading of GDPR in terms of consent, privacy, security and strong authentication.

Contact: Nick Swanson, Founder & COO