FCA Announcement

Open Banking – Adjustment Period

By 14 September third party providers (TPPs) are required by the Payment Services Regulations 2017 (PSRs 2017) and the regulatory technical standards on strong customer authentication (SCA-RTS) to stop screen scraping and, instead, access customer accounts using either a dedicated interface (API) or a modified customer interface (MCI). However, we are concerned that there could be serious disruption to the continuity of TPP services to customers, because:

- some TPPs' migration of customers to Account Servicing Payment Service Providers' (ASPSPs) APIs is not yet complete.
- some ASPSPs have not yet made APIs available for all payment accounts.
- ongoing access to customers' payment account data for Account Information Service Providers (AISPs) via other means, including access via a MCI, will be prevented by strong customer authentication (SCA).
- some TPPs have not yet obtained eIDAS certificates.

However, this is not an industry wide problem. Some ASPSPs have had APIs for all payment accounts available in production and in use since 14 June. We expect TPPs to be ready to use the APIs to access these ASPSPs' payment accounts from 14 September 2019.

6-month adjustment period

To enable TPPs to continue to provide their services while they adjust their software and systems to the other ASPSPs' APIs or MCIs, TPPs will need to be able to continue accessing their customers' accounts via existing (pre-14 September) channels - i.e., screen scraping. To facilitate this, for a period of 6 months, we will not enforce any requirements in the PSRs 2017 and the SCA-RTS that an ASPSP would breach as a result of facilitating TPP access in this way. In practice, during this adjustment period:

- ASPSPs, who did not have APIs available and in use for all payment accounts by 14 June, should maintain existing screen-scraping channels without strong customer authentication, alongside their live APIs, without the risks of FCA enforcement action for 6-months.
- TPPs should continue to be transparent and open about their identities when interacting with ASPSPs, even where existing access channels do not support secure identification.
- For API and MCI access, where a TPP does not have an eIDAS certificate, ASPSPs would enable the use of equivalent certificates, as long as they enable secure identification without the risk of FCA enforcement action.

Registered address c/o Dentons, 1 Fleet Pl, London EC4M 7RA. Company No. 07917853

- We would not take enforcement action in relation to a breach of the contingency mechanism requirement. However, where a firm has not obtained an exemption by the end of the adjustment period we would expect them to have a compliant contingency mechanism in place.

Following this 6-month adjustment period all ASPSPs should ensure they have an interface, either a MCI or API, that is compliant with all the requirements, including SCA, under the PSRs 2017 and the SCA-RTS. By this time all TPPs should have migrated their customers.

We encourage ASPSPs to make use of the Article 10 exemption under the SCA-RTS, including for MCI access where relevant, to allow AISPs ongoing access to customers' payment accounts.

We will monitor ASPSPs implementation of APIs and TPPs efforts to migrate to these APIs and MCIs. If we see sufficient progress by both ASPSPs and TPPs, so that the period of adjustment is no longer appropriate, we will reconsider the length of the adjustment period. This adjustment period will last for 6-months and will not be extended. ASPSPs and TPPs, if they do not already, need to have compliant systems in place by the end of this adjustment period. If firms do not they will be in breach of the PSRs 2017 and SCA-RTS and could be subject to enforcement action by the FCA.

We will communicate to firms seeking an exemption about how the adjustment period will affect their exemption request.

It is important that ASPSPs consider the impact of SCA solutions on different groups of customers, in particular those with protected characteristics, as they continue to implement SCA to their compliant interfaces. It may be necessary for a payment service provider to provide different methods of authentication, to comply with their obligation to apply SCA in line with regulation 100 of the PSRs 2017. For example, not all payment service users will possess a mobile phone or smart phone and payments may be made in areas without mobile phone reception. Firms must provide a viable means to strongly authenticate customers in these situations.