Video transcript – PSD2 and Payment Services Regulation Deep Dive, Part 1

Nicholas Webb, Technical Specialist, FCA:

I am responsible for providing advice and guidance to our team of supervisors who are responsible for the 1,158 payment services firms that we supervise.

What should firms do to stay compliant following these regulatory changes?

The key change obviously came in from 13th January 2018 with PSD2 coming into effect, or Payment Services Regulations 2017 for the UK purposes. They introduced a range of changes, things like new rules on complaints handling, so firms now must respond to a consumer's complaint within 15 business days. If they're unable to do that for exceptional circumstances, then they could extend that to 35 business days, so long as they're giving the consumer notice of that and the reason for the delay with a hard deadline at the end of it.

In addition to that, we've got new rules coming in around strong customer authentication, so how firms authenticate their customers, there are a new set of firms being regulated for the first time, account information service providers and payment initiation service providers, and there are new conduct rules for those firms but also for payment service providers that provide payment accounts accessible online, they need to facilitate access in some way and there are new rules and requirements around how they do that coming into force from September 2019.

We also have a whole raft of new reporting to be considered, new complaints reporting, new notifications when things go wrong under the Major Incident Notification process as well as new requirements on operational security risk assessments, basically to make sure that firms are staying on top of what the risks are to their business and then reporting to the FCA at least once a year in that regard as well.

What important regulatory changes should firms think about?

Any firm that's operating in the regulated space needs to consider complaints, they're a vital source of information. It's important that firms are treating their customers appropriately and complaints is a good indicator of that. You can learn from when things have gone wrong. Also, a key interest of the FCA is

resilience, the operation security risk assessments, the new guidelines set around that as well, are useful for firms to understand to respond and ensure that they are resilient. Payments obviously are a crucial part of the UK economy and people's lives so when they can't make a payment as they expected, that can have quite big impacts on people, both for their day to day living but also on larger transactions that they're trying to undertake.

When and how should firms refer to the EBA guidelines?

So, with PSD2, the European Banking Authority was asked for the first time to come up with a whole host of guidelines, Regulatory Technical Standards and implementing technical standards – the key things for firms is that they probably should already have had a look at them, so when they were planning their compliance exercises for the advent of PSD2 and also now the RTS coming into force, you should have looked at those guidelines and reflected upon what they mean for your business and updated any policies or procedures appropriately.

Some of the key ones to look out for are the EBA guidelines on major incident reporting under PSD2, and also the European guidelines on operational security risk frameworks. There are some important Regulatory Technical Standards which are going to come into force from September 2019 so that's the Regulatory Technical Standards on strong customer authentication and common and secure communication which provide quite a lot of information for firms on how to authenticate customers to help reduce fraud but also how to facilitate access for the newly regulated account information service providers and payment initiation service providers.

What is the EBA's RTS?

Yes, so the EBA Regulatory Technical Standards on strong customer authentication and common and secure communication, that's a nice long title, covers two aspects really. So, PSD2 introduced for the first time a requirement for firms to strongly authenticate customers whenever they do one of three things: so that's whenever they access their payment account online, initiate an electronic payment or undertake any activity via a remote channel which may imply a risk of payment fraud.

In order to strongly authenticate when a customer does any of those actions, the firm needs to authenticate the customer using two of three possible factors, the first being knowledge – so that's something the user knows, think PIN or password. The second is possession – so that's identifying them by something they possess, for example a particular device. And finally it's an inherence factor – so that's something that the user is, for example, biometrics.

As well as strong customer authentication, the RTS also provide requirements for firms that provide payment accounts accessible online and need to open up access for the newly regulated account information service providers and payment initiation service providers. So, the RTS sets out the two ways really that firms can go about doing that, the first being adaptation of the payment service user interface, the second being preparing a dedicated interface or more commonly referred to as an application programming interface or API to allow the AISPs and PISPs access.

Now, the key thing here is that firms really do need to go away and look at the RTS in that space to think about whether or not they do offer payment accounts accessible online and start to make changes to their systems to facilitate access for these new firms. In short, there is no easy way of doing it, changes are going to have to happen either way. If you're going to adapt your payment service user interface, then historically firms might have relied upon screen scraping but screen scraping as it's happened in the past is not going to be acceptable going forwards for this purpose. The AISP or the PISP is going to need to be able to identify itself to the payment service provider operating the accounts so it will be some form of screen scraping but with identification, for example.

If they're going to go through the dedicated interface route, then again they'll need to build that interface. They're going to need to provide a fall back option in the event that that dedicated interface fails unless they apply to the FCA for an exemption from that fall back and we would strongly encourage firms to do that and to try and build the most resilient APIs possible in order to support a well-functioning ecosystem and give these new firms the best opportunity to support the future open banking ecosystem.