**Video transcript – PSD2 and Payment Services Regulation Deep Dive, Part 2**

**Nicholas Webb, Technical Specialist, FCA:**

***What should firms do to better understand the FCA's position on security measures?***

So, PSD2 for the first time introduced requirements on firms to undertake an operational security risk assessment at least once a year. This is a critical part of making sure firms remain resilient at all times. The framework and assessment needs to reflect individual business models and the harms posed to that business model. Firms should already have undertaken such an assessment when they came through the FCA's re-authorisation or re-registration process for PSD2 but if they've got any questions, then Chapter 18 in our Approach document provides further guidance to firms on our expectations and also the EBA Guidelines on operational security risk frameworks would be a useful starting point.

***What should firms do in case of a major incident?***

So, the definition of a major incident is set out in EBA Guidelines, again, so that's the EBA Guidelines on Major Incident Reporting under PSD2. There are different categories to think about so we have major and minor effectively. If you hit any of the major thresholds, for example, €5 million-worth of transactions being impacted, then they need to follow the process. On the other hand, if they hit three of any of the minor categories, then again an incident should be categorised as major.

What we would expect firms to do is to review the EBA's Guidelines and to make sure they're embedded in their incident processes and incident response frameworks to make sure that they assess any incident against those guidelines. Where an incident has been identified as hitting the thresholds, then firms must notify the FCA within four hours. They do that via a form on Connect. Having notified the FCA, they need to provide intermediary reports up to every three days during the course of the incident. The intermediary reports shouldn't just wait for the three days to tick by, it's important that firms maintain appropriate and regular updates to the FCA so they should be aiming to update us at least every three days, again via Connect.

At the end of an incident, once it's been resolved, all firms need to undertake root cause analysis to identify the cause of the incident and then notify the FCA

within fourteen days via the final report, again through Connect of that root cause.

### *What should firms do if they want to better understand the FCA's position?*

So, we publish our Approach documents. We've combined our Approach to the Payment Service Regulations and the Electronic Money Regulations into a single document which hopefully is crafted in plain English, so that should be the first port of call at all times. If they've got any questions having read that, then do feel free to get in touch with the phone contact centre who again can help provide a useful steer on particular points. Outside of that, firms of course should be taking their own guidance and advice as needed and where appropriate they can also apply for individual guidance from the FCA.

### *Looking ahead to Brexit, what do firms need to be thinking about?*

So, firms should be thinking about Brexit if they aren't already doing so. They need to be thinking about the impact that it will have on their individual business models, we can't really give a stock answer to the question because different business models will be impacted differently. Therefore, firms should be putting in place contingency or at least contingency planning for all possible outcomes. In particular, we expect them to be thinking about the impact on their customers and also communications that need to be made to customers ahead of any likely outcome.