Financial Data and Technology Association

Opposing Forces: The PSD2 Secure Customer Authentication & Regulatory Technical Standards Quagmire

- Published on February 11, 2021

Ghela Boskovich

Regional Director/Head of Europe at Financial Data and Technology Association
39 articles Following

If you use any fintech product that relies on data from your primary bank account, you will have navigated Secure Customer Authentication (SCA) processes. You will also have run into the 90 Day Reauthentication requirement that demands you confirm you want the fintech to have access to your bank account data, while at the same time re-navigating SCA and consent

mechanisms. These two components are part of PSD2's regulatory technical standards. They're also the finicky bits that are killing PDS2's ability to deliver competition, innovation, and better customer outcomes to the EU and UK markets.

Earlier this week I published **an article noting how the UK's Financial Conduct Authority (FCA) has proposed changing how SCA and 90 Day Reauth are applied**. They have proposed an elegant solution to a series of conflicting clauses in the second level legal text that have resulted in devastating unintended consequences to the ability of fintechs to provide services and customers to remain connected to these services.

But how did the need for the FCA to propose such a sharp change from the EU law arise? And why does it matter so much to the success of PDS2 and Open Banking? Let us set the stage. Fair warning: we will wander into the weeds at times, and wade through many an alphabet soup acronym, but dear reader, you should come out the other side relatively unscathed, and with a better understanding of why the FCA's proposal makes sense.

PSD2 tried simultaneously to introduce a framework to encourage innovation in Payment Initiation Services (PIS) and Account Information Services (AIS), as well as a raft of new payment security measures on the Account Servicing Payment Service Providers (ASPSP, more commonly known as banks) that affect not only AIS and PIS, but also their Payment Service User's (PSU's, the consumer's) interfaces.

Introducing all of these measures at the same time created a number of unintended consequences, from interrupting critical services to many millions of customers, including small businesses, while severely impeding fintechs' (or Third Party Providers – TPPs – in PSD2 parlance) businesses and creating a range of unnecessary risks for ASPSPs.

The PSD2 Regulatory Technical Standards (RTS) requirements for Strong Customer Authentication (SCA) set two opposing forces in the same legal text*: it requires banks to introduce SCA and to not introduce obstacles to TPPs that break their connections with customers.* Experience has proven that these are incompatible requirements given the current market context.

For the last 15 years, TPPS in the UK and EU have used many types of whole market financial data, including payments data, to build services that help end customers, and were widely used across many customer types and business models. This took place in the unregulated space, until PSD2 arrived. And many of these business models work by accessing financial data using an in-force customer Consent to collect their data for whichever service is being offered, without the customer having to be "present" or initiate the data access. This is the typical AIS data access model. SCA, however, means the customer needs to be present to insert their credentials at the time of the access request, irrespective of the type of data being accessed.

Under PSD2, ASPSPs are required to design systems to enable the TPP to access the customer's **payments** data when they are not present. However, consumers *non-payment* data

is *not* included in the scope of PSD2 and the RTS, but consented access to that data is being prevented because of how SCA is implemented. ASPSP application of SCA to their PSU interfaces restricts TPPs' ability to access non-payments data. Most ASPSPs are implementing SCA at the front gate of their PSU interfaces, therefore applying it to both payment and non-payment financial data.

As they stand, SCA regulations mean customers must be present for each point of data access if the ASPSP has not applied the Article 10 exemption**[1]** (more on that in a moment), regardless of whether the customer has previously given authorisation or not. In this way, SCA is disconnecting consumers from the tools Open Banking had made necessary, without giving any added uplift in protection. Open Banking was meant to provide an efficient, user-friendly service, but this is far from the reality of the SCA being applied as currently scoped; the way SCA is applied to AIS use cases violates the principles of competition, innovation, and better customer outcomes as intended by PSD2.

Now we cannot paint the ASPSPs as the villains here: it is not in the banks' interest, nor their direct customers' interest, to put a lower level of security on the front gate to enable non-payment data access, and *then* apply SCA elsewhere in the digital channel for the payment data access. That would force the customer to log in twice to get to the payments data. And as non-payment data isn't within PSD2's regulatory scope, the bank isn't obligated to go out of their way to make it easy for TPPs to access the data. Data access precedent and aligned incentives are in conflict here, thanks to SCA-RTS requirements.

Because non-payment data (savings, investment, and credit data) are not subject to SCA under the RTS (or PSD2 for that matter), this data should be obtainable and flow freely if the customer has already consented the TPP to access it. However, because of how SCA has been implemented – and in part to reduce avoid customer double-login requirements – non-payment data cannot and does not flow. **In short, all the myriad non-payments data held by ASPSPs is being restricted by technology, whereas it is not restricted by regulation.**

SCA was to be about security, but it was not meant to be applied carte blanche across all services. By legislation, SCA is limited to *payments* data, but it affects all the other data, too.

Viewing an account balance should not require the same level of security as making a transaction. This nuance is important, as SCA currently blocks access to non-payments data *not subject* to SCA under the RTS. This frustrates the AIS business model, a model which predates PSD2 by a dozen years. This frustration also puts the AIS TPPs at risk of going out of business. It is antithetical to the aim of PSD2 to promoe competition and innovation. If left as is, SCA has the potential to disrupt and even dismantle Open Banking as we know it.

The FCA Consultation does address one component of SCA, and that is how often it is applied. The FCA recognises that SCA has inadvertently reduced choice, hindered growth, restricted innovation, and hindered new entrants from the UK market. In order to remedy this, they've proposed creating a new SCA exemption to Article 10A so that consumers do not need to

reauthenticate every 90 days when accessing their account information through a TPP (AISP specifically). This means no more navigating SCA after the initial connection is established. Banks will no longer need to require their customers apply SCA every 90 days when the customer uses a TPP to provide account information services. SCA will still be applied when the connection is first established, but after that, authentication is no longer required. Consent – different from authentication – will need to be reconfirmed every 90 days, but consent does not require SCA beause it will be managed by the TPP going forward, not by the bank.

This proposed approach resolves the problem of non-payments data being restricted by technology. SCA at the first point of TPP-to-account connection and authentication still achieves PSD2's security goals, but it no longer hinders the TPP from performing the service it offers. It also means that under a future Open Finance framework, we have a template of how to ensure all types of financial data can flow within appropriate security constraints.

These two opposing forces – strong security measures around authentication and no obstacles that break TPP's connections with customers – sit within the same legal text. The FCA's solution to this is to provide a new exemption to the RTS Article 10, and to limit the scope of the existing Article 10 exemption. The tension between high security standards and obstacles can be erased with a stroke of the pen: TPPs won't be in danger of being cut off from customers, non-payments data is no longer restricted by technology (repetitive SCA), and the intended security lift SCA provides actually materialises without becoming an obstacle. The FCA's solution works both practically and politically.

---

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC