Financial Data and Technology Association

# Legal Conflicts in the RTS-SCA Text: The root cause of all 90-Day evil

- Published on March 10, 2021


## Ghela Boskovich

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


Anyone who's paid attention to the issue of 90-Day Reauthentication in the last three years since PSD2 went live in the European market is bound to have noticed the unexplainable and seemingly irrational conflicts that sit within the legal text that frames out the **Regulatory Technical Standards (RTS)** on Strong Customer Authentication (SCA). The RTS essentially sets t

wo opposing forces within the same legal text. SCA has introduced obstacles to Third Party Providers (TPPs/fintechs) and risks breaking those connections with their customers; at the same time, it requires that banks introduce SCA but not introduce obstacles to TPPs. These are incompatible requirements in the current market context. Let's examine those incompatibilities in depth, shall we?

But first, a reminder that the FCA is taking steps to reconcile these incompatibilities in their current **consultation**, by shifting from an authentication renewal model to a consent renewal model. It's an elegant approach to unpicking a morass of conflicts contained in a single document. In **previous installments** in this **series**, I've explained exactly why this is a pivotal moment for fintech and for better **customer outcomes**.

As currently written, SCA regulations require consumers to be present for each point of data access if the bank has not applied the Article 10 exemption, regardless of whether the consumer has previously given authorization or not. In this way SCA disconnects consumers from the tools Open Banking has made necessary (**without any added uplift in protection**). But what is this Article 10 exemption? Be prepared for a pedantic breakdown; you've been warned.

Article 10 of the RTS SCA notes that the Payment Service Providers (PSPs, most often the banks) are ***allowed not to apply*** SCA where a consumer (called a Payment Service User in PSD2) is limited to accessing either or both (1) the balance of one or more designated payment accounts; or (2) the payment transactions executed in the last 90 days through one or more designated payment accounts – without disclosing sensitive payment data.

This means banks have a choice of whether or not to apply SCA if someone (via a fintech) is checking the account balance or transaction history. These two scenarios are the vast majority of the types of checks fintechs are actually making. So, SCA doesn't actually have to be in place for either of these two types of data exchange to happen. And yet, and yet the vast majority of banks have opted to apply SCA in those two journeys instead of exempting those journeys as per Article 10.

There are only two conditions under which a PSP is ***not*** exempt from applying SCA:

- when the consumer is accessing their balance on that account *for the first time*, or

when more than 90 days has elapsed since the last time they accessed the payment transactions (and SCA was applied the last time they access the transaction data)

And here arises the first conflict: under PSD2, consumers can give consent to Third Party Providers (TPPs, fintechs, specifically Account Information Service Providers – AISPs) to access to that payment account to provide balance information and 90 days' worth of payment transactions. This is, in fact, the service for which they contract with the fintech. And this contractual permission is addressed under Article 35.5b in the RTS SCA.

Article 35(5)(b) give AISP fintechs permission to access the payment account information for which they have explicit consumer consent up to four times in a 24-hour period without the consumer needing to be present. Basically, if the AISP has consumer consent, no SCA is needed if the AISP is requesting the data instead of the consumer.

Essentially, once an AISP has a contract with a consumer, they have permission to access that payment account data. The first time this connection is made, SCA is required. But from the second data access session, the AISP can keep accessing the account data when the customer is not actively requesting the information (in the background, so to speak), without any additional required SCA. Basically, Article 10 means that SCA is not required for AISPs to access account balance and transaction data. And yet, and yet SCA is still being imposed by banks.

SCA poses a barrier to AISP fintechs to access payment account information already consented to, permissioned by the consumer. SCA prohibits fintechs from refreshing account information up to the legal limit of four times a day without the customer present. SCA impedes this business model from being executed and is a violation of yet another RTS Article: Article 32(3) which prohibits the creation of obstacles to the provision of Payment Initiation and Account Information services.

Now that's just about accessing the account data. It becomes even more conflicting when we factor in authentication (pun totally intended, and no apologies). PSD2 Article 97 requires a payment service provide (PSP, bank) to apply SCA *where the payer accesses their payment account online*. It also notes that SCA applies when the information is requested online through an AISP. So, SCA should happen when a consumer accesses their account online through an AISP. **But**, **when a payer is not actively requesting such information, SCA is not applicable.**

Let's break this down:

- SCA is not applicable when the AISP is accessing the payer's accounts without the payer actively requesting the information
- If the payer accesses their accounts online, and is actively requesting the information either directly or via an AISP, more frequently than 90 days, then SCA does **not** have to apply, it can be exempted.

Logically, this means there is no need to apply SCA every 90 days, nor does SCA need to be applied in order for AISPs to access transactions older than 90 days (because the payer is not actively requesting the information). This is consistent with PSD2 Article 98, which aims to secure and maintain fair competition among all payment service providers.

Article 98 is all about ***not*** being cut off from the customer's account data. Banks have access to a payer's account information and associated transactions ***without*** having to apply SCA. This is not the case when AISPs what to access the same permissioned data. SCA effectively cuts off AISPs from accessing that same data. SCA violates the fair competition principle of PSD2 Article 98. Banks have the opportunity to push relevant alerts or information; with SCA being applied,

AISPs do not have this same opportunity. Banks are left with a distinct competitive advantage due to SCA. SCA essentially violates PSD2 Article 98.

So far, we have these conflicts:

1. RTS Article 10 allows for SCA exemptions, but these exemptions aren't often exercised;
2. RTS Article 35(5)(b) gives fintech permission to access consented to data without SCA being enforced, but banks are still applying it (especially if the bank does not have an API, but relies on a modified customer interface exemption, which is the subject of the next article in this series);
3. RTS Article 32(3) prohibits the creation of obstacles fintech data access, but SCA is just one big obstacle;
4. PSD2 Article 97: SCA is exempt if the payer is NOT resting the data, but a proxy permissioned AISP means there's an SCA exemption;
5. PSD2 Article 98: fair competition equates to fair access to permissioned account data, but with how SCA is applied, banks are *never* cut off from their customer's data, but AISPs are;
6. PSD2 Article 115: requires banks to ***not*** to implement measures that block or obstruct existing PISP and AISP services.

The crux of the RTS incompatibilities is this: word order. Specifically, the order of these two words: allowed and not.

By granting banks the option to choose whether they impose SCA, the RTS is effectively killing the AISP model.

The wording 'allowed not to impose SCA' leaves this at the discretion of the banks, effectively giving the supply side utter control over the access by the demand side. 'Allowed not to impose' means that banks have the choice *to* impose SCA despite the two conditions laid out by the RTS – that the customer is accessing balance information and 90 days' worth of payment transactions.

AISPs are effectively doing just that, as a proxy for the consumer and with the consumer's full consent: checking account balances and checking 90 days' worth of transactions. But the wording of the RTS still allows the bank to impose SCA requirements despite a consented to, contractual agreement between the consumer and the AISP. When a bank does impose SCA requirements, it renders the contractual agreement between the consumer and the AISP impossible to fulfill.

Article 10 says that banks are 'allowed not to apply SCA' to AISP access between the first access and the 90-day reauthentication. It does not say they are 'not allowed to apply SCA'. This means that the RTS has effectively contradicted the intention of PSD2: if the bank applies SCA, they effectively block the TPP from transmitting the personalized security credentials.

Moreover, PSD2 Article 115 requires ASPSPs ***not*** to implement measures that block or obstruct existing PISP and AISP services.

While the RTS clearly seeks to improve security measures, the SCA detail is inconsistent with the intent of PSD2. The unintended consequences of the SCA detail leave the banks protected from competition, the customer with diminished services, and the TPP market blocked from delivering their business model.

As they stand, SCA regulations mean consumers must be present for each point of data access if the ASPSP has not applied the Article 10 exemption, regardless of whether they've 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 combination of SCA as currently applied along with the mandate for customers to reauthenticate every 90 days is not only damaging to the customer journey, it is also an obstacle and burdensome in part due to widely diverging technical standards across the market (specifically in Europe, the UK has the single OB technical standard), and it ultimately damages and limits fintech innovation. The way SCA is applied in the AIS use case violates the principles of competition, innovation, and better customer outcomes as intended by PSD2.

Pedantry over, but clearly necessary. A single instance of conflict within the text would be enough to reverse course and make corrections. Multiple instances of conflict demand an immediate solution. It's time for European regulators to follow the FCA's example, post haste.