Financial Data and Technology Association

The Detrimental Impact of 90D Reauth & SCA on Fintech, the Market, & End Customers

- Published on February 16, 2021

Ghela Boskovich

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

Secure Customer Authentication (SCA), combined with the requirement for end-users to reauthenticate every 90 days, is meant to provide a secure and reliable way for consumer to connect their bank accounts to regulated fintech services. Or at least that was the intention when it was enshrined in law as part of PSD2's Regulatory Technical Standards (RTS). But the

road to Hell is paved with good intention, and the path that SCA and the 90 Day Reauth rule have created has been chthonic at best, and hellish at worst: the entire Open Banking market has suffered from lost revenues, lost opportunities, and less innovation with fewer value propositions brought to market because of it.

No more turning a blind eye to the fact that the intension and outcome are mis-aligned. **The FCA in particular has taken notice *and* taken action to fix it.** Their first post-Brexit consultation proposes to move away from reauthentication towards reauthorisation, and with changes to just a few letters and a shift in who manages the process, the FCA removes a boulder of an obstacle to Open Banking's viability. Why other regulators across Europe are not taking similar pains is a mystery, **because without correcting for this misalignment betweeen the legislative text of PSD2 and the SCA-RTS legal text**, end customers are cut off from valuable financial services to their detriment, fintech competition is stymied, and innovation is slowed. All of the things, might I point out, which PSD2 purports to support.

But SCA and 90 Day Reauth are in danger of making PSD2 a political failure, because imposing a 90 Day Reauth rule on regulated and licensed Third Party Providers' (TPPs/fintechs) end customers does more harm than good:

- It has nearly zero positive impact on bank security, in opposition to the objective of the rule [SCA does not make a material difference to bank security due to implementation inconsistencies]**[1]**;
- It poses a hassle to end customers, many of whom have used fintech services fo years without the imposition of either SCA or the need to reauthenticate;
- It has proven to be a customer eduction nightmare, with no convincing argument for end-customers outside of 'it's the law';
- It creates poor customer outcomes, both by marring and creating friction in the customer journey, as well as potentially disconnecting them from critical TPP services that are meant to protect the customer's financial health.

Moreover, it is anticompetitive at its core. Only fintechs, not banks, are disconnected from the customer data if the customer fails to log in to renew/reauthenticate within in the required time frame, or if the reauthentication journey fails due to unavailable/non-working bank APIs. In the UK the banks have been consistently improving their API performance and conformance to standards over the last few years, but in the EU, a lack of uniform technical standards (and no overseeing body to measure how those standards are implemented or perform) means that inconsistent API availability has significant impact on a customer's ability to reauthenticate in a timely manner. If the consumer is cut off, they can rely only on time bound bank supplied services, rather than their chosen and contracted fintech supplier. This asymmetric data access is anticompetitive.

No other market allows incumbent firms to control their competitors' market access, yet this is the *de facto* standard under PSD2. Banks can and do control fintechs' ability to access customer data, despite an end customer granting that permission to the fintech; it is controlled both in

part by how and when SCA is applied in the customer journey, and by the cliff-edge 90-day rule imposed by the SCA-RTS. This asymmetric control of market access is anticompetitive.

And in no other market are incumbent firms in control of their competitors' relationship with their end customers, yet this is exactly what PSD2 enables, as it puts banks in charge of reminding fintechs' customers of the data access connection and service. Consent resides with the TPP/fintech, however reauthentication takes place at the bank. This creates additional friction for the customer, who, in wishing to confirm their consent to the TPP, is required to reauth at the bank. This gives banks the competitive advantage of being obstructionist in the commercial relationship between the end customer and their chosen service provider (the fintech). This asymmetric interference in the customer relationship is anticompetitive.

[Note, this negative impact to competition is exacerbated by those banks who have been slow to recognise that open banking is more opportunity than threat to their traditional business model; for those banks who have embraced open banking, little incentive exists to exploit this asymmetry. For banks who see Open Banking as a compliance mandate rather than an opportunity to future-proof their business model, every incentive exists to obstruct fintech/customer relationships by exploiting the asymmetric data access incumbents have under the legislation.]

The 90 Day Reauth rule also causes material detriment to TPP business viability and commercial metrics in a number of passive use cases: this, too, is in opposition to the objectives of PSD2.

We saw ample evidence of this harm from FDATA members, which they shared with UK regulators over the course of 2020, particularly in terms of customer attrition rates. Across FDATA fintech members, attrition rates typically ranged from 20-40% at the 90-day mark. Multiply that percentage rate across the entire European TPP market, and the only conclusion is that SCA and 90 Day Reauth rule pose a manifest detriment to the entire competitive marketplace. It also means that a significant number of end customer are cut off from these services at the 90-day mark.

This is not due to a lack of perceived value on the customer's part. It's because of technical and behavioural issues. A more nuanced and contextual examination provides insight. For example, one AISP (account information service provider, or TPP) reported a 32.7% drop off of users who do not reauthenticate after day 90, ceasing to use the service at that time. In that group of 32.7%, however, more than 50% of those users log in after Day 90, indicating that they still want the service but that the hassle of reauthentication, or indeed bank API failures during the reauthorization process, means that the service is interrupted and no longer available to them.

Furthermore, for the remaining 67% of customers, only 40% of those users reauthenticate at day 90 – the remaining percentage reconnect to the fintech after the 90-day mark. This results in a large percentage of users who want the service but experience an interruption to that service. In those remaining cases, this requires the user to set up the service from scratch, including all of the categorisation work history they had previously completed. There is also a

significant spike in customer attrition at 180 days, when customers are required to reauthenticate for a second time. This strict requirement to reauthenticate at the bank side to confirm TPP consent to access date results in consumers abandoning services which they are happy with, and which continue to provide value; it's the obstacle to the service, not the value of the service, that means TPPs lose customers because of the conflicts in PSD2 and the SCA-RTS.

This is compounded for customers whose banks provide a Modified Customer Interface (MCI) rather than an API under protection of the SCA-RTS Article 31 exemption. Due to the nature of MCIs, which require a customer be present for every data transfer from the bank to a TPP, SCA and 90 Day Reauth rules are a complete road blocker to a number of use cases. This 'customer must be present' requirement means that all forms of passive use cases (think personal finance management where the service happens in the background before you access your budget and financial dashboards, or cloud accounting services that keep real-time records of business banking transactions) result in a near 100% attrition rate for the fintech.

100% customer attrition. In no way is that sustainable for fintechs nor the market. By continuing to adhere to a rule that paradoxically makes it nigh on impossible to retain and serve customers, regulators who adhere to the 90-day Reauth rule break the market they intended to make by suppressing the very competition they purport to espouse.

There are other value propositions that are being withheld from the market because fintechs know that they would have 100% attrition rate (even with an API connection) at the 90-day mark. Here, the opportunity cost alone is steep: the cost to competition, to innovation, and to the customer's benefit. And all because the legal text has a few conflicting clauses.

In any case, for fintech users, this is a terrible customer journey: the SCA-RTS and 90 Day Reauth rule places obstacles in the way of the fintech delivering the service. It also places obstacles in front of the customer hindering their ability to consume the service. It erodes the value of the fintech proposition, resulting in the objectives of PSD2 missing their mark completely.

Two use cases in particular highlight just how detrimental these two rules can be. For example, small business account automation leveraging both payment account and savings account data. Because savings accounts are not payment accounts, they require SCA to be performed every time that data is access. (in fact, common practice is to pre-load the current and savings accounts to automate the bookkeeping.) Automated accountancy is hindered, as any reconciliation between payments and savings will have to be performed manually to enable savings data to be access using SCA. This is a return to manual loading of savings data renders an 'automated' solution null. This unintended consequence of the SCA/90 Day rule virtually destroys small business accounting system solutions *and* negatively impacts small businesses as well. The rules do double the harm.

Personal finance management (PFM) tools are also crippled by these rules. For consumers relying on budgeting apps, the need for SCA to access bank held savings, investment, and credit data means that automation, especially reminders and push notifications meant to keep customers aware of their finances are rendered moot. Customers have to perform SCA every time they check the PFM tool. And due to a dearth of available financial advice, any technology proxies for that advice cannot step in because data is restricted from flowing to the application that helps customers. This unintended consequence of the RTS leaves PFM tools hindered and customers worse off.

PDS2's political objective is to nurture companies who bring competition to the market, thereby improving competition. Innovation, and security in the EU (and UK) payments market. However, the way SCA and 90 Day Reauth have been crafted and delivered have done much more harm than good: it defeats PSD2's political objectives and fails to materially improve security to protect consumers.

Unless these rules are changed now – with regulators taking all practical steps – many of the political objectives of PSD2 fail, and will fail in a spectacularly public manner. The FCA has read the proverbial tea leaves on this, and reached a similar conclusion. It is time for other regulators to follow suit.

---

[1] Differing regionalised specifications across the EU to deliver SCA and the RTS are a function of differing levels of technological maturity and readiness to implement the open banking model. The significant divergence here means TPPs have to implement several different specifications (sometimes on a country-by-country basis), which adds unnecessary friction in the ecosystem, adding cost and additional compliance burdens for banks and TPPs alike, while providing no consistent security upswing.