Financial Data and Technology Association

Leveling up the UK Market: Why the FCA has determined the MCI has got to go [but also why API performance matters]

- Published on March 24, 2021

Ghela Boskovich

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

It may seem like a minor change in regulatory policy; it, however, is not. I've said that repeatedly about various points in the **FCA's recent consultation** on changes to the Regulatory Technical Standards (RTS). It bears repeating, but this time my poetical waxing focuses on a

major change to how all banks across the UK market provide access to consumer data: the removal of the modified customer interface (MCI) exemption.

When combined with Secure Customer Authentication (SCA), those banks who took the exemption to providing an API, instead offering up an MCI, ended up with something that basically stopped data access in its tracks. It also rendered passive screen scraping impossible. [Screen scraping is verboten under PSD2, except when an MCI is the only means of accessing the data; it's also a materially less secure means than API data access as it's all about repeated security credential sharing.] And for those customers of banks who only offer an MCI, screen scraping is the only way they're able to access value added services fintechs provide; yet they can't extract the full value of those services because of how SCA is applied. Why? Because screen-scraping is technically impossible without the customer present to authenticate every data request.

MCIs are the proverbial catch-22, with bad consumer outcomes no matter how you slice it.

Fintechs (third party providers, TPPs under PSD2) have proven business model utility time and again over the last 15 years, pre-PSD2; yet SCA policy is the proverbial looming sword over the TPP business model neck. It is not the lack of proven business model value that threatens the aims of PSD2 to deliver competition and innovation to the market; it is bad policy that threatens to kill fintech.

In short, due to the nature of MCIs, they require a customer be present for *every data transfer* from the bank to the fintech. Combined, the SCA and 90-day Reauth rules in the MCI scenario result in a near 100% customer attrition rate for the fintech; and a 100% value loss for the end customer.

Before APIs became de rigueur, screen scraping was the norm. Screen scraping access models for TPPs typically involve the Account Information Service provider (AISP) or their Technical Service Provider (as their agent) storing static login credentials, then passing those credentials through the end consumer's interface when the customer is not present. PSD2 did try to protect the TPP's right to pass through these security credentials in the **Level 1 final text** (PSD2 itself), however clarifications in the **Regulatory Technical Standards** (RTS) step back from this.

The pedantry from my **previous article** continues. Bear with me here, because this matters – and it proves why the FCA's proposal to revoke the MCI exemption is such a big deal for end consumer value.

PSD2 Article 67(b) states that the AISPs must *'ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels'.*

However, RTS Chapter II introduces authentication codes, dynamic linking (to enable authorisation in the payment flow) and a requirement to keep the Knowledge, Possession, and Inherence elements of the SCA flow strictly separate to avoid the compromise of one element afflicting another.

Remember Article 10 in the RTS? It says that Payment Service Providers are 'allowed not to apply SCA' to AISP access between the initial set up access and the 90-day reauthentication. If a bank applies SCA here, they block the TPP from transmitting personalized security credentials. It's this point at which the RTS effectively contradicts the intention of PSD2 – particularly in the case of banks offering an MCI.

Instead of using the end-customer's security credentials (typical screen scraping stuff), the fintech is now obligated to identify itself to the bank in order to access the data via the MCI. This becomes a double challenge when the bank has designed SCA for the MCI in such a way that there is a dynamic element to which only the customer has access. This is especially troublesome as the bank has no obligation *not* to use SCA for all connections. It is another technology layer fintechs must contend with in order to pass through the authentication gateway, another engineering challenge, and another obstacle to circumvent in what should be obstacle free consented data access.

Compounding insult to injury, the engineering workaround introduces even more security vulnerabilities. If banks fail to address these and implement SCA, fintech (AISP) customer-not-present access is completely inhibited. Moreover, banks are not providing test environments for SCA through their MICs, which causes significant business interruption for both fintechs and the end consumers.

Long story short: while the RTS seeks to improve security measures, SCA as applied to an MCI is inconsistent with the intent of PSD2, and materially impacts continuity of customer service *and* introduces security vulnerabilities.

The FCA consultation addresses dynamic linking of authentication in section 4.7 of their consultation; it is the justification for eliminating the MCI exemption. By eliminating this exemption, the FCA is pushing to level up the rest of the market to the big nine UK banks mandated under PSD2 to deliver a dedicated API. This is good for the market, and especially good for end consumers. It means less risk of being cut off from data access and services.

And yet. (You were waiting for that, weren't you?). And yet this is where API performance and conformance are clutch hitters in whether that unblocked data access is a reality.

It's fair to say that some fintech services require continuous access, otherwise they don't function. However, not all banks are delivering consistent high-quality performing APIs unilaterally across the UK market. Early on in the UK open banking journey, consistent performance and conformance was a pipe dream; however, both have improved immensely for the big nine in particular under the supervision of the Open Banking Implementation Entity. But

banks not mandated under the Competition and Market Authority's order are not held to the same technical standard, nor the performance and conformance requirements. This fact alone is proof that independent oversight and monitoring are crucial to achieve quality delivery across a single market.

However, relying on banks to provide self-assessment of API performance and conformance is tantamount to leaving the student to mark their own exams: it's meaningless and subjective. Rather, tech should be used to measure tech, and all parties in the ecosystem should be supervised to the same standard. Going forward, all banks across the UK market should be held to the same API standards that apply under Open Banking, and the FCA would be wise to hold that line for all UK banks once the MCI exemption is removed.

There is another reason why the quality of an API matters: contingency access methods. This contingency method is provided for in the RTS in yet another paradoxically ineffective approach to ensure TPPs have access to data.

Because of inconsistent API implementations (aside from the UK big nine, this inconsistent delivery is true for both the long tail of UK banks as well as financial institutions across the EU as a whole), banks have had to fall back on providing contingent methods of access. RTS Article 33(4) explains the conditions and expectations on the bank in providing contingency methods to access when their dedicated access (the API) fails:

"As part of the contingency mechanism payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32."

TPPs are hopeful that the risks are somewhat mitigated by real rigueur in the exemption process, however the TPP community is very skeptical as to whether the Contingency Access Method is realistic, because it is costly to maintain two types of access methods. Normally, once customers have been migrated to the API access model, they stay there. The wholesale transition of TPPs' customers to a new Consent, Authentication, and Authorisation flow cannot be reversed easily. Moreover, TPPs **cannot** maintain direct access (screen scraping) agents for ASPSPs which they are not allowed to use, that can reasonably be expected to function in a crisis. Customers cannot be induced at the 'touch of a button' to re-enter credentials for the AISP use case. There Is no scenario under which a PSU will re-authenticate daily, let alone several times a day, to maintain access.

It is more than likely a fintech would remain non-functional while waiting for the ASPSP to fix their API channel. In addition to the technical and customer security issues, there would be material customer communication, confidence, and engagement challenges. Moreover, the bank would be violating RTS Article 32(3) by creating an obstacle to PIS and AIS services. Any

faith that contingency access while an API is down is mooted even before we're out of the gate. Article 33(4) is pointless in the face of reality.

Just one more point about obstacles, and more to the point, what RTS Article 32(3) specifically says that banks are obligated to ensure that their "interface does not create obstacles to the provision of payment initiation and account information services" It ALSO explicitly states that obstacles to the provision of those services may include, among other things, 'imposing redirection to the [bank's] authentication or other functions, requiring additional authorisations and registrations.'

Here is where poor API performance and bad customer journeys intersect: in mandatory redirection. Licensed fintechs have a right to access consenting customer account data in order to retrieve information strictly necessary to provide their services under Article 66(2). Banks have a choice to continue to allow for direct access via the customer-facing online banking interface (including mandatory identification of the TPP) or to provide a dedicated API.

Mandatory redirect is a clear violation of Aritlce 32(3), as well as PSD2's principles of technology and business model neutrality. Mandatory redirect is also excluded under Aritlce 30(2b), in that the interface needs to ensure that the communication session between the bank, the fintech, and the consumer concerned be established and maintained throughout the authentication step. Article 30(2b) explicitly forbids disrupting a TPP session to divert the consumer back to the bank; such a disruption is the very definition of redirection.

The principles of technical and business neutrality enshrined in Article 98 PSD2 would dictate that the banks cannot force PISPs and AISPs to use redirection. Rather, the RTS provides that banks must leave the possibility open to offer the customer an option to use and stay connected to the fintech's own website for authentication.

Moreover, mandatory redirection only exacerbates the SCA problem. If SCA is imposed in an obstructive manner, and SCA includes mandatory redirection, fintechs will suffer additional negative impacts and restrictive competitive opportunities Mandajtory redirection relegates the noble aims to promote competition and improve customer outcomes to the rubbish bin: it allows banks who offer the poorest customer journey to suffer the least competition.

I mention mandatory redirect to underscore a point: where and how SCA is being placed in the customer journey has been so poorly executed that it necessitates being declared an obstacle. Mandatory redirect is just insult to injury in a line of obstacles to accessing data and hurdles to be cleared in the customer journey. It is time for those obstacles to be removed. The FCA clearly recognizes this, and their proposed elimination of the MCI exemption is proof of it. The UK market – banks, fintechs, and end customers – will profit from this. It's time the rest of the EU markets saw the same light and upgraded the whole market to API first (based on harmonised, interoperable tech standards across the board).