Financial Data and Technology Association

How SCA and 90-day Reauth Harm Competition & Security

- Published on February 18, 2021

Ghela Boskovich

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

If you've read the previous tomes in this series, you'll know that the **FCA's proposed change to the 90-day reauthentication requirement** will have significant positive impact on the industry – and why this course correction is good for the competitive landscape and fintech innovation. You'll also already know the context for how the rules combining **secure customer authentication (SCA) and the 90-day rule are mired in a conflicting quagmire** that does nothing to materially improve customer security and access to open banking value

propositions. Not to mention, you'll already be familiar with **how SCA and 90-day do nothing to further the PSD2 objectives** to improve innovation, promote competition, and secure consumers better financial outcomes; in fact, it does the just the opposite as it dooms PSD2 to a political failure rather than an innovation triumph.

But what you may not yet be familiar with is to what extent this regulatory combo actually harms fintech businesses, creates security risks, and ultimately leaves consumers and small businesses worse off by limiting their choices to make better financial decisions. It's this damage we'll dive into today.

Let's talk about customer churn. It is a reality for all digital solution providers: every app provider across every industry experiences churn. Even during the pandemic, our favourite distraction app Netflix experiences customer churn – in its early days it saw 10% monthly churn, but for the last couple of years it averages at 2% a month. **[1]** Being able to control customer churn is essential for business survival. Like any other business, fintechs accept this fact. Unlike other digital businesses outside of a highly regulated industry like financial services, however, fintechs are handicapped by an inability to control for churn related to anything but the service value. While they can battle churn based on the value of the service they deliver, their hands are tied when it comes to artificial influences on customer attrition. I refer to the 90-day reauthentication rule here.

Let us take one fintech/Third Party Provider (TPP) who submitted evidence to UK regulators last year to showcase just how detrimental the 90-day rule is to competitive providers. The firm has been in the market pre-PSD2 and have so far survived Open Banking being rolled out; but the post-Open Banking implementation scars are brutal. Before Open Banking, their quarterly churn rate hovered just under 7%. Post Open Banking, their 90-day churn metrics have risen to 44%. That's almost a 600% increase in customer churn for a service that had not changed its business model or its value proposition. In fact, customers had reported positive feedback on additional features and functionality, so the quality of the service had only increased between pre- and post-Open Banking.

Another TPP provided data showing the decline of reauthentication over a 3 month/90 day period, comparing the total number of connections week over week, with week one measuring the number of customers onboarded to the service. 90 days later, there is an abrupt drop in connections. An estimated 97% of customers were not re-authenticating at the worst of the dip (at the 90 day mark). This level of attrition is not typical churn – it sits so far outside of any anticipated statistical standard deviation that it's outlier status is a huge red flag.

A 3% customer retention rate at day 90 is clearly not sustainable for any business. How could a rule that punishes competitive market entrants on a routine cadence be argued to promote competition?

Normally customer churn is attributable to three primary things: poor product, poor customer service, and better alternative products. But in the case of the aforementioned fintech, all

evidence pointed to something other than these typical churn reasons. This fintech has a high product-market fit: 96% of their users would be disappointed if they could no longer use the app.[2] This fintech perpetually rates a 95%+ Customer Satisfaction on Zendesk score, so customer service is not a churn issue. Moreover, survey after survey for this fintech indicates that 80% of their users prefer this app over comparative bank apps providing a similar service, so this fintech isn't facing a slew of better alternative competition. In fact, this fintech is a repeat British Bank Award winner.

So why is this fintech losing nearly half its users after only 90 days? And why is this company not alone in suffering staggering churn rates? All signs point to the 90-day Reauthentication Rule, and the obstacle it proves to keeping customers connected to their chosen services.

Proponents of the SCA + 90-day combo argue that it improves customer security. Is there an uplift? It's unlikely for two reasons: increased security credential exposure, and non-technical workarounds and hacks. Let's look at a concerning example of the latter reason first.

Basic non-technical work arounds are being used to breach security protocols and expose those login and password credentials to others whose name is not on the bank account. Case in point: accountants' hack on circumventing the problem of getting their clients to reauthenticate every 90 days.

In the UK a significant number of small and medium business rely on cloud accounting services to run their businesses; these accounting services are directly connected to bank accounts via Open Banking. But not all of these SMEs directly manage their accounts, a vast majority of them rely on certified accountants to maintain the bookkeeping on their behalf. (By the by, SMEs account for 60% of employment, and around 50% of turnover in the UK private sector[3]. In other words, they are the lifeblood of the UK economy.)

A 2020 survey of nearly 500 licensed bookkeepers and accountants by a cloud accounting firm, 100% of whose clients connect their accounts via Open Banking, showcased just how damaging SCA + 90-day is to small businesses.[4] Of those accounting professionals asked, 97.9% confirmed that the requirement for clients to reauthenticate their bank feeds every 90 days caused significant problems.

Nearly a hundred percent of respondents (97.3%) spent time chasing their clients to reauthenticate. 83% said their clients were not even familiar with the reauthentication process. And 76.6% said that they frequently had to deal with out-of-date accounting records because required reauthentication had not happened. And 69% said that they spend *at least an extra hour* of additional time *per client per month* helping clients reconnect their bank feeds. A quarter of respondents spent more than *three hours* per month per client chasing reauthentication. They don't spend this time accounting, they spend it chasing reauthentication.

So that's a pain for the accountants, but here's where it gets dicey for those small businesses: 77% of respondents said that there is at least some risk of their clients getting into cash flow problems because of disconnected bank feeds, with at least double the number of firms at very high risk in comparison to those in the low-to-no risk range.

In that context, a vast majority of SMEs rely these automated, bank-feed connected services, and expect that those connections remain intact, despite the rule to reauthenticate every 90 days. And this is where the aforementioned non-technical workaround comes into play. Accountants are reporting back to these providers that their clients suggest that the accountants be set up as users on the clients' bank accounts so that they can do the 90-day reauth on behalf of the SMEs.

This poses material security issues for both the small business *and* the accountants. But SMEs are seemingly more willing to go this route than to log in every 90 days themselves. If SMEs aren't able to reconnect/reauthenticate, or they forget to do it, it leaves the accountants in a position of working with and advising on out-of-date data, or large data gaps. Sharing passwords and login credentials with accountants poses increased security problems and risk; inaccurate data poses a different set of increased risk. For SMEs, there is no proverbial King Solomon solution while the 90-day rule is in place. Rather, the only solution for SMEs and accountants is to remove the rule. For SMEs and their accountants, the FCA's proposal offers much needed relief.

SCA + 90-day also happens to introduce an unnecessary technical security risk, one that has nothing to do with sharing security credentials, but one that does exist because of how often security credentials are exposed.

Fact: Every additional exposure of a customer's security information required to login or validate themselves, increases the risk of exploitation by hackers. Attach sophistication continues to improve, and each time a customer is asked to authenticate at the bank, the risk of customer exploitation materially increases. Given this exposure, if the customer is required to reauthenticate every 90 days with each of their banks directly, the customer is subject to increased risk. Frequency is directly related to risk (and compounded by the number of accounts and services that are connected. With account aggregation services, this risk increases linearly in line with the number of banks with whom the customer is required to authenticate. For example, a customer who has accounts with four different banks presents an opportunity to be exploited by attackers at least 4 times every 90 days *for each fintech service connected to each of those accounts.*

Despite improvements in the authentication process over the years, the weakest link has always been the initiation and input of authentication data. Between 2018-2029, mobile-based malware detections increased by 72%. This is of primary concern because most fintech apps are mobile based, yet the mobile is the most common attack vector today. And 2020 marked the year where everything went online, and mobile-first really came out first in preferred channels.

Take, for example, the ExoBot (or Marcher) trojan. ExoBot is an Android based malware that focuses predominantly on financial organisations in relation to the multi-factor authentication process, where it acts as a 'man-in-the-middle' to steal that multi-factor authentication information to gain access to the customer's bank services. An estimated 7% of UK Android devices are infected with this trojan.**[5]**

The UK National Cyber Security Centre (NCSC), a wing of GCHQ, recommends that where possible, authentication processes on trusted devices (i.e., mobile phones) be minimised**[6]**; instead, the NCSC suggests opting for session-based authentication, thereby reducing the need for the customer input in order to validate the authenticity. NCSC suggests that organisations should minimise the requirements for non-user led authentication.

Authentication data is the most sensitive data a customer holds. Requiring a customer offer that sensitive data up on a frequent and unnecessary basis violates the principles of sound and secure data/platform management. It also does not adhere to the NCSC guidelines (nor the National Institution of Standards and Technology, a non-regulatory agency of the US Department of Commerce).

SCA + 90-day amounts to repeated security credential exposure, resulting in increased security risk. This is exacerbated by financial institutions who offer a modified customer interface rather (MCI) than an API, because that MCI means a customer has to be present to go through SCA in order for the TPP to be able to access the data in order to perform the contacted service. MCIs mean even more numerous security exposures. Allowing for an MCI exemption nullifies the intended purpose of weaving increased security measures into PSD2; it completely fails the consumer from a risk *and* access to competitive services perspective. The good news for the UK market is that the FCA has proposed to remove the MCI exemption, which means all UK financial service providers will be required to deliver a financial grade API (FAPI standard) to market. Security and service will be improved because of it.

There is no doubt that SCA + 90-day rules have hurt fintech businesses, which does nothing to improve the competitive landscape PSD2 strives to create. The rules do little to improve security – partly because of human behaviour combining efficiency, apathy, and laziness, partly because of technical exposure – which also falls far short of the original political intention enshrined in PSD2. The rules leave consumers and SMEs in danger of being cut off from important services and up-to-date financial information crucial to making the best financial decisions for their households and businesses. It also leaves them with less choice, and fewer innovative value propositions that can't and won't be delivered to market because those services rely on assured uninterrupted data access. The rules hinder innovation, increase security risks, stifle competition by giving banks an unfair data access advantage, and provide zero upside; not to mention, they're the reason PSD2 will fail if nothing is done to reverse course. The FCA's proposal acknowledges this and is the first step to fixing yet one more of PSD2's paradoxical problems.

[1] https://gibsonbiddle.medium.com/4-proxy-metrics-a82dd30ca810 - Netflix CEO Gibson Biddle's reported estimates mid-2019

[2] Metrics are based on an industry standard survey popularised by Sean Ellis, where any app with over 40% of respondents who would be 'very disappointed' to lose access to the app has attained product-market fit.

[3] FSB UK Small Business Statistics: https://www.fsb.org.uk/uk-small-business-statistics.html

[4] Not publicly available, however survey and evidence was shared in closed session with UK regulators.

[5] https://www.threatfabric.com/blogs/exobot_android_malware_spreading_via_google_play_store.html

[6] https://www.ncsc.gov.uk/collection/end-user-device-security