Financial Data and Technology Association
c/o The University of Edinburgh
13-15 South College Street
Edinburgh
EH8 9AA

17 April 2020

Vice President Valdis Dombrovskis
European Commission
Rue de Spa 2 (SPA 2 2/20)
B-1000 Brussels/Bruxelles
Belgium/Belgique

Chairperson José Manuel Campa
European Banking Authority
20 Avenue André Prothin
92400 Courbevoie
France

Sent via email to:

Dear Vice President Dombrovskis and Chairperson Campa,

RE: The Detrimental Impacts of SCA Reauthentication to Open Banking

The Financial Data and Technology Association (FDATA), on behalf of its members, is asking the European Commission and the European Banking Authority to urgently revisit the requirements on Secure Customer Authentication and 90-day Reauthentication, due to its extremely detrimental impact to Third Party Providers (TPPs).

Companies who have operated as TPPs pre-PSD2, as well as newer firms, have shared with us that they are contemplating returning money to shareholders because they cannot sustain their business under these circumstances.

PSD2's political objective was to nurture those companies, improving competition, innovation and security in the EU payments market. However, currently the way 90-day Reauthentication and SCA work defeats the political objectives of PSD2, and fails to materially improve security to protect consumers.

These PSD2 policy objectives have been undermined by the specific drafting contradictions in the RTS. FDATA Europe recognises the enormous challenges and competing interests of arriving at the final RTS that had to allow for transition to an API technology never contemplated during the drafting of PSD2.

Until this point, the arguments on various legal interpretations have gone back and forth, highlighting where RTS conflicts with PSD2, and where some clauses in RTS conflict with others. Every vested interest can find some point to support their position. However, it is now time to move past theoretical arguments on the impact of various interpretations; it is time to point to irrefutable evidence of the attrition rates afflicting TPPs due to RTS contradictions, which do not afflict ASPSPs.

In the document attached to this letter, we make a series of technical arguments which we hope will usefully articulate the conflicts in the drafting detail. However, nothing should distract from the key message: **irrespective of these arguments, many of the political objectives of PSD2 still fail, and will fail in a spectacularly public manner, unless these issues are resolved now, taking all practical steps.**

The evidence, highlighted from a broad sample of mostly maturing TPPs companies, shows that:

1. Some Modified Customer Interfaces (MCIs) provided by ASPSPs are requiring the customer to be present for every data transfer to an AISP. This is an obstacle to use cases and has near 100% customer attrition for the TPP.
2. 90 day reauthentication shows customer attrition rates between 13% and 65%, rates which are simply not economically sustainable at either end of the spectrum, with firms losing customers who fail to re-authenticate for a variety of mostly technical and behavioural reasons.

In summary, FDATA Europe recommends the following sequential steps to mitigate the devastating impacts of 90 Day Reauthentication and customer present SCA have on the success of Open Banking:

Step 1 - EBA to issue an Opinion explaining the contradiction in the RTS, and that Article 10 should be interpreted as “not allowed” to require SCA for TPPs within the 90 day period. Any other interpretation renders AIS activity moot.

Step 2 - EBA to require that SCA implementations preventing customer-not-present access must immediately remove SCA to enable credential sharing access to resume (supported by the TPP identity).

Step 3 - EBA to issue a new Opinion enabling AISPs to conduct 90 day re-authentication of their customer, and SCA to be removed from TPP channels until this is possible.

Step 4 - European Commission to develop an 'Open Finance' policy that enshrines the customer data right, empowering every data subject to direct, share, and determine the length of time for which they grant consent to their financial data.

Step 5 - European Commission to work with the EBA and NCAs to develop an interim approach to mitigate market risks in the transition period, including requiring ASPSPs to not apply SCA if they are (a) blocking non-payment accounts from access which have been in wide usage, and (b) if APIs do not include all Evaluation Group functionalities; and allowing TPPs to continue accessing all customer-facing online interfaces by identifying themselves based on HTTP Header.

Step 6 - European Commission redraft RTS to remove the 90 day time limit and seek parliamentary approval. TPPs to be required to communicate with their customer on a frequent basis (at least once every 90 days) using the agreed channels to confirm continued access, but not requiring the customer to perform an action.

Step 7 - European Commission and Markets to work with their NCAs to develop incentives and plans to widen mandatory scope, whilst also providing a period of customer transition, which could reasonably be measured for each ASPSP individually on the basis of being compelled to implement new SCA 12 months after they have provided a fully functioning API.

Step 8 - European Commission seek to bring in legislation to deliver a full Open Finance policy, built on a customer data right, explicit consent, a clear liability model, robust APIs with full functionality, and an orchestrated delivery.

Yours sincerely

Ghela Boskovich
Chapter Leader, FDATA Europe

Background

PSD2 tries 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) that affect not only AIS and PIS, but also their Payment Service User's (PSU) interfaces.

Introducing all of these measures at the same time creates a number of unintended consequences, from interrupting critical services to many millions of customers, including small businesses, while severely impeding TPP's businesses and creating a range of unnecessary risks for ASPSPs.

RTS requirements for Strong Customer Authentication (SCA) set two opposing forces in the same legal text. New SCA will undoubtedly introduce obstacles to TPPs and break connections with customers. The RTS requires ASPSPs to introduce SCA and to not introduce obstacles. These are, in most situations, incompatible requirements in the current market context.

Below we explain why SCA needs to be balanced with the rights of access under PSD2 while protecting the customer from the harm of being severed from their TPP services delivered using non-payments data that is outside the scope of PSD2.

As they stand, SCA regulations mean PSUs 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 an obstacle and burdensome in part due to widely diverging technical standards across the market, 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.

Discussion of impacts of 90 Day Reauthentication and Secure Customer Authentication to AISPs and PISPs businesses

90 Day Reauthentication

Imposing 90 Day Reauthentication on TPP end customer has no merit for a number of reasons: ● It has nearly zero positive impact on ASPSP security, in opposition to the objective of the rule

● It poses a hassle to end customers, many of whom have used TPP services for years without this imposition

● It is proving to be a customer education nightmare, and has no logical explanation to share ● It is anti-competitive at its core

- o Only TPPs and not ASPSPs are disconnected from the customer data if the customer fails to login. Customer can rely only on time bound services supplied by their ASPSP, rather than their chosen and contractual TPP
- o No other market allows incumbent firms to control their competitors' market access o TPP Business viability and commercial metrics suffer material detriment in a number of passive use cases, which is in opposition to the objective of PSD2 ● It puts ASPSPs in charge of reminding TPPs' customers of the connection and service, permitting them to be obstructionist in the commercial relationship between customer and their chosen TPP

● 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

Increased Attrition Rates

A number of FDATA members have provided feedback on the damaging impact SCA and 90-day Reauthentication has on their ability to provide service to their customers. The following table shows the percentage of customer attrition during the first 90-day reauth cycle experienced by a sampling of FDATA members:

Business Type Rate of Attrition when SCA is Applied
PFM 100%
PFM 29%
AISP/Aggregator 19%
AISP 13%
AISP 40%
Financial Services 65%

Cloud Based Accounting Software 52%

Attrition ranging from 20-40% is typical from our survey of members; multiply that out to the entire TPP market across Europe and the only conclusion is that SCA poses a manifest detriment to third party providers. It also results in a significant number of end customers being cut off from these services at the 90 day mark.

To give context to some of these numbers, an AISP FDATA member 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, almost half of those users log in after Day 90, indicating that they still want the service but that the hassle of reauthentication, or indeed ASPSP 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. 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. This is a significant hindrance to the customer journey – in fact it places obstacles to the TPP delivering service, but also to the customer from consuming the service. It also erodes the value of that service, which results in the objectives of PSD2 missing their mark completely.
FDATA members are also reporting that several new services are being withheld from the market, due to the 90-day SCA reauth requirements, which would result in 100% attrition at the 90-day mark. The opportunity cost alone is steep: the cost to competition, to innovation, and to the customer's benefit.

Non Payment Data Impact

In the EU, and for circa 15 years, TPPs have been using many types of whole market financial data, including payments data, to build services that help end customers. This activity has taken place in the unregulated space and is in very wide use across many customer types and business models.

AIS models work when the customer is not present, by accessing the financial data using an in force customer Consent to collect their data for whichever service is being offered. Dynamic or multi-factor SCA pushes the customer to be present to insert their credentials.

Under PSD2, ASPSPs are required to design systems to enable the TPP to access the customer's **payments** data when they are not present. The RTS seeks to enhance the security of protected resources in payments. But PSUs non-payment data is not included in the scope of PSD2 and the RTS, but consented access is being prevented nonetheless.

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.

It is not in the interests of ASPSPs, or their direct customers, to put a lower level of security on the front gate to enable non-payment data to be gathered, then apply SCA elsewhere in their digital channel for the payments data. This would force the customer to log in twice to get to the payments data. As the non-payments data is not yet within the regulatory scope, the ASPSP is not obliged to go out of their way to be helpful.

Because savings, investment, and credit data were not subject to SCA under the RTS, this data should be obtainable and flow freely if the customer has already consented the TPP to access it. However, ASPSPs are putting the SCA as a front gate prohibiting non-payments data to 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.

Moreover, viewing a balance should not require the same level of security as making a transaction. This nuance is important; as banks are wont to roll out SCA unilaterally across all
accounts, this blocks access to non-payments data not subject to SCA under the RTS. This frustrates the existing AISP business model, a model that has been in the market for a number of years preceding PSD2. This frustration puts the AISP at risk of going out of business. This is antithetical to the aim of PSD2 to promote competition and innovation. SCA implementation has the potential to disrupt and even dismantle Open Banking as we know it.

Immediate Detrimental Consequences of SCA

Whilst the SCA element of RTS has been widely criticised by the TPP market from the start, some of the issues are coming into sharp relief now that we better understand the full range of repercussions. **The product access enabled is too narrow in scope, the technical standards not narrow enough. Unilateral SCA implementation by ASPSPs across current regulatory timelines is ruining businesses and causing serious customer detriment. SCA does not make an immediate material difference to the security of ASPSPs due to the implementation inconsistencies.**

The lack of common technical solution and API standards for information exchange across Europe is of particular concern. There are several different API standards and specifications being used by banks across Europe, including those of the Berlin Group and Open Banking Implementation Entity in the UK. These standards and specifications are different, and they disagree on the same underlying security models for performing authentication with a bank for typical payment flows. Most ASPSPs are using some version of redirection to deal with the initial and subsequent SCA, even where an API is present.

Differing regionalised specifications in attempts to deliver the RTS are themselves a function of differing levels of technology maturity and readiness to implement the open banking model. This significant divergence means cross-country third party providers must address implementing several different specifications, sometimes even having to do this on a country-by-country basis. This unnecessary friction in the ecosystem adds cost and additional compliance burden for banks and TPPs alike.

Examples of detriments due to everyday authorization

1. **Small business account automation:** Because savings accounts are not payment accounts, they require SCA to be performed every time they look at the books (common practice is to pre-load the current and savings accounts to automate the bookkeeping). Automated accountancy will be hindered, as any reconciliation between payments and savings will have to be performed manually to enable savings data to be accessed using SCA. This is a return to manual loading of savings data, ultimately rendering an automated accounting system null. This unintended consequence of the RTS virtually destroys small business accounting system solutions, and negatively impacts small businesses as well, doing double the harm.

2. **Personal Financial Management** tools are crippled. For consumers relying on budgeting apps, the need for SCA to access ASPSP 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 will 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 trying to manage their finances worse off.

3. **Non-ASPSP providers of financial products** rely on knowing the customer's financial position in order to deliver their service. For any non-ASPSP provided product,

customers are forced to perform SCA each time they need to execute that product. This disruption in the distribution of digital financial products was not intended by the RTS, yet is the case because of how SCA is being implemented.

4. **Commercial and contract issues**: The RTS did not intend to induce breaches of contract for the supply of services, but the consequence of applying SCA causes TPPs to fail to fulfill commercial and contractual agreements with customers and suppliers because of restricted access to data, despite consent being granted by the customer in order to receive those contractual services.

SCA Applicability

SCA for accessing payment accounts only applies when the PSU is accessing their payment accounts online.

Article 10 of the SCA & CSC RTS notes that Payment Service Providers (PSPs) shall be ***allowed not to apply*** SCA where a PSU is limited to accessing online either or both (1) the balance of one or more designated payment accounts; (2) the payment transactions executed in the last 90 days through one or more designated payment accounts – without disclosing sensitive payment data.

There are only two conditions under which a PSP is *not* exempt from applying SCA, according to Article 10:

1) the PSU is accessing online the balance of one or more designated payment accounts *for the first time*, or
2) more than 90 days have elapsed since the last time the PSU accessed online the payment transactions executed in the last 90 days through one or more designated payment accounts and SCA was applied.

However, consent for AISPs can be given for account information service provision as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the PSU.

Article 35.5.b addresses this: where the PSU does not actively request such information (i.e., is not online), AISPs are allowed to access the payment account information to which the PSU has given explicit consent, no more than four times in a 24-hour period.

Once an AISP has received a mandate from a PSU (as per the contract when signing up for the TPP service) to access their payment accounts, and SCA has been applied to access their payment accounts for the first time, the AISP can keep accessing the accounts when the PSU is

not actively requesting such information without requiring any additional SCA. Moreover, it follows that in those instances, SCA is not applicable because the PSU is not accessing their balances and accounts online and this access is not initiated by the PSU. Therefore under Article 10, PSPs are *allowed not to apply SCA* to the AISP access. SCA is therefore not required in order for AISPs to access account balance and transaction data. Yet it is still being imposed by ASPSPs.

SCA poses a barrier to AISPs to access payment account information already consented to by the PSU. It prohibits AISPs from refreshing account information up to the legal limit of four times a day without the customer present. SCA impedes execution of the AISP business model, which is in violation of RTS Article 32(3) to not create obstacles to the provision of PIS and AIS services.

Article 97, as it relates to authentication, requires a PSP 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. SCA should be applied when a PSU accesses their payment accounts online through an AISP. ***However, when a PSU is not actively requesting such information, SCA is not applicable.***

SCA is not applicable when the AISP is accessing PSU accounts without the PSU actively requesting the information. And if the PSU accesses their accounts online, and is actively requesting the information, either the PSU interface or via a TPP, more frequently than 90 days, then SCA can be exempted.

Therefore, there is no need to apply SCA every 90 days or to access transactions older than 90 days when the PSU is not actively requesting the information. This is consistent with Article 98 of the Directive that aims to secure and maintain fair competition among all PSPs. ASPSPs have access to the PSU's payment account information and associated transactions without having to apply SCA, but AISPs have been effectively cut off from accessing that same data. ASPSPs have the opportunity to push relevant alerts or information that AISPs do not. ASPSPs are left with a distinct competitive advantage due to SCA, in violation of the Directive's Article 98.

The primary problem with the RTS comes down to the order of two words: allowed and not. By granting PSPs 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 PSP, effectively giving the supply side utter control over the access by the demand side. 'Allowed not to impose' means that PSPs 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 PSU and with the PSU's full consent: checking account balances and checking 90 days worth of transactions. But the wording of the RTS still allows the PSP to impose SCA requirements despite a consented to, contractual agreement between the PSU and the AISP. When a PSP does impose SCA requirements, it renders the contractual agreement between the PSP and the AISP impossible to fulfill.

Article 10 says that PSPs will be '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 ASPSP 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 ASPSP protected from competition, the customer with diminished services, and the TPP market blocked from delivering their business model.

Immediate Consequences of SCA on Modified Customer Interface

TPPs have proven business model utility time and time again over the last 15 years, yet SCA policy is a looming proverbial sword over the TPP business model neck. It is not the lack of proven business model utility that threatens the aims of PSD2 to deliver competition and innovation to the market; it is bad policy that threatens to kill fintech.

SCA flows from the RTS and applies to forms of payments and access to payments data. ASPSPs must impose SCA from the end of the transition period, meaning that screen-scraping becomes technically impossible without the customer present to authenticate every data request.

Any SCA requirement for ASPSPs who do not offer a dedicated API and who do not have an exemption means any TPP will be cut off from accessing account data, as screen scraping is no longer allowed. Nor can the TPPs migrate customers to an API in this instance.

Screen scraping access models for TPPs typically involve the AIS provider, or their Technical Service Provider (as their agent) storing static login credentials and then passing these through a PSU interface when the customer is not present. Whilst PSD2 sought to protect the right of the TPP to pass through credentials in the Level 1 final text, the clarifications in the RTS seems to step back from this.

PSD2 Article 67(b) states that the AIS 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 an SCA flow strictly separate to avoid the compromise of one element afflicting another.

Again, we refer to Article 10 which says that PSPs are 'allowed not to apply SCA' to AIS access between the first access and the 90 day reauthentication. If an ASPSP applies SCA here, they block the TPP from transmitting personalised security credentials. Here, the RTS effectively contradicts the intention of PSD2.

Instead, the TPP is now obligated to identify itself to the ASPSP in order to access the MCI. This becomes a challenge when the ASPSP 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 ASPSP has no obligation *not* to use SCA for all connections. It also presents another technology layer TPPs must contend with in order to pass through the authentication gateway, and additional engineering challenges.

This workaround engineering introduces security vulnerabilities. If ASPSPs fail to address these security vulnerabilities and implement SCA, AISP customer-not-present access is completely inhibited. Moreover, ASPSPs are not providing testing environments for SCA through their PSU MCIs.

TPPs will need to adapt their access method for hundreds or thousands of connectors simultaneously without any documentation and / or testing environment causing a significant business interruption.

At minimum, TPPs should be given a 3-month testing window to ensure SCA access via an MCI. This 3-month minimum however, has been shown by the UK implementation experience to be already 9 months too short anyway.

In the EU, there are many millions of customers using TPP services; some TPPs and TSPs have over a million connected accounts. There are also hundreds, potentially even thousands, of ASPSPs TPPs will need to integrate with to maintain existing customer services. These ASPSPs might all provide a completely different integration challenge. The

RTS does not provide adequate timelines to transition customers, irrespective of the ASPSP providing an MCI or an API.

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.

Immediate Consequences of SCA on dedicated API

Some services require continuous access otherwise they don't function. However, no ASPSP is delivering a consistent high-quality performing API unilaterally across the market. Nor are there consistent standards being applied across the EU market that would provide for a high-quality API being offered by the supply side. Lack of standards is one limitation in this. The other is that there is a lack of uniform performance and conformance measurements being reported to overseeing NCAs. Relying on ASPSPs to provide self-assessment of performance and conformance metrics is no way to guarantee minimum levels of performance, and therefore no way to guarantee a high-quality API. This is a technology problem that can be fixed using technology. Applying a technology tool to test both performance and conformance is the solution to ensuring ASPSPs are meeting their obligations under PSD2.

Because of these inconsistent API implementations, many ASPSPs have had to fall back on providing contingency methods of access. RTS Article 33(4) explains the conditions and expectations on the ASPSP in providing contingency methods to access when their dedicated access (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. The wholesale transition of TPPs' customers to a new Consent, Authentication, and Authorisation flow cannot be reversed easily. 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 AIS 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 TPP 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 ASPSP would be violating RTS Article 32(3) by creating an obstacle to PIS and AIS services.

Mandatory Redirect

Licensed TPP's have a right to access consenting PSU account data in order to retrieve information strictly necessary to provide their services, under PSD2 Article 66 (2). ASPSPs 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. If the ASPSP opts for the use of an API, according to Article 32(3) RTS, the bank is obliged to ensure that 'this interface does not create obstacle to the provision of payment initiation and account information services'.

RTS Article 32(3) explicitly states that obstacles to the provision of PIS and AIS may include, among others, 'imposing redirection to the [ASPSP's] authentication or other functions, requiring additional authorizations and registrations'.

Mandatory redirect is in clear violation of Article 32(3) RTS, as well as PSD2's principles of technology and business model neutrality. Instead, ASPSPs should ensure that the API enable any credentials transmitted by the PSU to the ASPSP (e.g., token generator one-time codes), to be transmitted by the TPP, and that the PSU does not need to interact with an ASPSP-provided landing page in order to use Mobile Bank-ID.

Mandatory redirection is also excluded under Article 30(2b) RTS, in that the interface needs to ensure that the communication sessions between the ASPSP, the AISP, the PISP, and any PSU concerned be established and maintained throughout the authentication step. Article 30(2b) explicitly forbids disrupting a TPP session to divert the PSU 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 PSU to use and stay connected to the TPP's own website for authentication.

An API that offers only a redirect-based user journey will be considered an obstacle (as per RTS Article 32(3)) by all existing TPPs who have used direct access up to now. Direct access gave the PSUs the most frictionless payment flows possible. TPPs must not be blocked from the possibility to adapt their customer interfaces to new contexts and devices. TPPs must not

be required to use redirection.

Mandatory redirection only exacerbates the problems of SCA. If SCA is being imposed in an obstructive manner, and such SCA includes mandatory redirection, TPPs will suffer even more negative effects and restrictive competitive opportunities.

Mandatory redirection also allows ASPSPs who offer the poorest customer journey via TPPs to suffer the least competition.

Mandatory Redirection Impact on Customer Journey

In countries with existing bank-owned or bank-integrated payment execution services, e.g. Netherlands, Germany, Austria, Poland, and many more, which offer a payment guarantee and are all based on redirection, it would be a complete show-stopper for a PIS being forced to use redirection as well. Not being able to offer payment guarantees until Instant Payments become the norm, they must be enabled to differentiate at least on the user experience level.

An API that only offers a redirect-based user journey will be considered a strong obstacle by all existing PIS providers having used direct access up to now and whose PSUs accustomed to the most frictionless payment flow possible. In the interest of innovation and user experience as well as PSD2 and RTS compliance, TPPs must not be blocked from the possibility to adapt their customer interfaces to new contexts and devices, i.e. must not be required to use redirection.

AISPs should manage 90 Day SCA Reauthentication

AISPs should be able to manage every 90 Days SCA for payments and non-payment accounts instead of the ASPSP. RTS Article 10 confirms that SCA can be performed by any PSP, including AISPs and PISPs as regulated entities.

Under GDPR Article 6(1a), a bank has to share account data with a TPP based on the PSU's consent, which can be granted to the TPP. Banks do not have to verify the customer's consent to share data with the TPP. Requiring an ASPSP to verify PSU consent puts an additional burden and cost on the TPP to prove consent. It also breaches PSD2 Article 115, which requires ASPSPs not to implement measures which block or obstruct existing PISP / AISP services.

Forcing the TPP to rely on bank SCA means the TPP would have to conduct several SCAs every 90 days with a single customer, to ensure authorization for any separate accounts and for separate banks. This significant multiplication of SCA is a material detriment to the service whose primary purpose is to

facilitate bank account access and information consolidation across several accounts, including those at separate banks.

Instead, ASPSPs should allow TPPs to issue their own SCA for the 90-day reauthentication, so that PSUs would only have to refresh SCA once, irrespective of the number of banks and accounts being serviced by the TPP. This also allows TPPs to avoid a potential cliff-edge, after which they would not longer have access to the account data, and to consolidate the necessary refreshers into a single session.

Requiring TPPs to remind customers, via push notification or an alternative, every 90 days that they are still connected, rather than forcing the customer to login with their ASPSP to enable TPP service to continue, is the easiest short term solution. TPPs can notify the ASPSP that they have reminded the customer of their in-force Consent. This is in line with the recommendations of the European API Evaluation Group, and is a practical and simple solution to the matter.

PSD2 Article 68(5) clearly sets out that banks may only deny AISP access to payment account data 'for objectively justified and duly evidence reasons relating to unauthorized or fraudulent access to the payment account by that AISP.' For that reason, AISPs should be allowed to issue their own SCA for 90 day reauthentication. Any ASPSP denying this effectively obstructs access to accounts in violation of Article 68, stifles TPP competition, and abuses its position as gatekeeper.

Any other approach would also fail to meet the principles of business model neutrality, which require that ASPSPs should provide TPPs with access to PSU account data in the least obstructive way.

Recommended Course of Action

We recommend the following sequential steps to mitigate the devastating impacts of SCA and 90-day Reauthentication have on Open Banking:

Step 1 - EBA to issue an Opinion explaining the contradiction in the RTS, and that Article 10 should be interpreted as "not allowed" to require SCA for TPPs within the 90 day period. Any other interpretation renders AIS activity moot. ASPSPs can certainly choose to SCA their own customers within this period, but not TPP customers who are clearly not trying to access their ASPSP online account.

Step 2 - EBA to require that SCA implementations preventing customer-not-present access must immediately remove SCA to enable credential sharing access to resume (supported by the TPP identity).

Step 3 - EBA to issue a new Opinion enabling AISPs to conduct 90 day re-authentication of their customer, and SCA to be removed from TPP channels until this is possible. All API initiatives should mandate that this be supported.

Step 4 - European Commission to develop an 'Open Finance' policy that enshrines the customer data right, empowering every data subject to direct, share, and determine the length of time for which they grant consent to their financial data.

Step 5 - European Commission to work with the EBA and NCAs to develop an interim approach to mitigate market risks in the transition period, including requiring ASPSPs to not apply SCA if they are (a) blocking non-payment accounts from access which have been in wide usage, and (b) if APIs do not include all Evaluation Group functionalities; and allowing TPPs to continue accessing all customer-facing online interfaces by identifying themselves based on HTTP Header.

Step 6 - European Commission redraft RTS to remove the 90 day time limit and seek parliamentary approval. TPPs to be required to communicate with their customer on a frequent basis (at least once every 90 days) using the agreed channels to confirm continued access, but not requiring the customer to perform an action.

Step 7 - European Commission and Markets to work with their NCAs to develop incentives and plans to widen mandatory scope, whilst also providing a period of customer transition, which could reasonably be measured for each ASPSP individually
on the basis of being compelled to implement new SCA 12 months after they have provided a fully functioning API.

Step 8 - European Commission seek to bring in legislation to deliver a full Open Finance policy, built on a customer data right, explicit consent, a clear liability model, robust APIs with full functionality, and an orchestrated delivery.