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

Payments Policy Team
Attention: Qasim Khan
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

30 April 2021

To: cp21-03@fca.org.uk
CC:

Re: FDATA Response to FCA Consultation Paper 21/03 Changes to the SCA-RTS

Dear FCA Payment Team,

Below is FDATA Europe's response to the consultation on the SCA-RTS. We are grateful for the opportunity to respond, and would like to highlight a few points before presenting our formal response and recommendations:

- Article 10a exemption for TPPs needs to explicitly carve out the requirement to perform SCA every 90 days, and make it clear that ASPSPs do **not** have the option to require it after the initial connection is made and consent is in effect

- Any delays in the implementation of the proposed revisions to SCA-RTS will have materially negative impact on the entire UK market; 2023 is too long to wait, as a number of existing firms will necessarily leave the market due to customer attrition and churn, resulting in a spectacular failure of Open Banking. The timeline for change must be expedited.

As always, we are happy to discuss any points made below, or should any questions arise, we are at your disposal.
Yours sincerely,

Ghela Boskovich
Regional Director, FDATA Europe

Financial Data and Technology Association

Q1: Do you agree with our proposal to create a new SCA exemption for when customers access customer information through a TPP and add a new requirement for TPPs to check customers' consent every 90 days? If not, please explain why.

Yes, FDATA agrees with the proposal to create a new SCA exemption for when customers access customer information through a TPP and supports the requirement that TPPs check customers' consent every 90 days.

We would note that there is no clarity on whether a single confirmation can be used to confirm ongoing access to multiple bank accounts with different providers. We strongly believe that it should be possible for an AISP to obtain confirmation to access multiple accounts at the same time. If re-confirmation requests need to be sent per bank account, this could cause the same kind of friction that is caused by PSUs having to obtain authentication per bank every 90 days.

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. Moreover, it is anticompetitive at its core. Only TPPs, 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.

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.

Over the course of 2020, FDATA hosted a series of roundtables discussing the impact of SCA and 90-day reauthentication, presenting evidence from the UK TPP community as to the detrimental nature of the requirement. The evidence, highlighted from a broad sample of mostly mature TPPs, showed that under the 90 Day Reauth requirement, customer attrition rates span between 13-65% depending on the business model. These rates are simply not economically sustainable at either end of the spectrum, with firms losing customers who fail to reauthenticate for a variety of mostly technical and behavioural reasons, not because of a low service value. Moreover, some banks have an exemption to providing an API, and instead have stood up a modified customer interface (MCI). Due to the nature of MCIs, they require a customer be present for every data transfer from the bank to a TPP. In this case, the SCA and 90 Day rules are an obstacle to a number of use cases, and results in a near 100% customer attrition rate for the TPP.

Current Open Banking roadmap items are also in danger of failure should the 90-day reauthentication requirement remain in place. We see the proposed exemption as a critical success factor to support Sweeping and Variable Recurring payments, which are under consultation by the OBIE for the CMA Order. In order to operate unattended access to payment account information, access needs to be unfettered by the need to reauthenticate every 90 days, or the value proposition is significantly impared. A functionality mandated for competition cannot effectively be delivered without an exemption to 90-day reauthentication.

Moreover, the Department of Business, Energy & Industrial Strategy noted in its Smart Data Research Report that:

> The requirement for re-authentication at 90 days can lead to very significant consumer drop-off and is generally a poor customer experience. The underlying policy for re-authentication lacks some transparency. For the EU, the purpose was to improve security. However, it was later described in the UK as a way to mitigate the risk of continued data sharing by inert consumers who are no longer engaging with a product or getting value from it. Re-authentication appears to cause attrition even among engaged consumers."[1]

SCA was to be about security; it was not meant to manage consent nor to create an obstacle that breaks TPPs' connections with customers. Strong security measures around authentication and no obstacles are two opposing forces sitting within the same legal text. The FCA's solution to create "a

[1]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909363/Dge n_and_BEIS_-_Smart_Data_-_Consent.pdf ,] Page 19

new SCA exemption in Article 10A so that customers do not need to reauthenticate every 90 days when accessing account information through an AISP" (CP21/3, section 2.11) removes that tension between high security standards and obstacles.

TPPs must be explicitly exempt from SCA after the initial connection is made and consent is in effect

FDATA's understanding of this new exemption, based on its discussion with the FCA's payment policy team on 21 April 2021, is that it explicitly carves out TPP from having to push their customers to reauthenticate the connection to the ASPSP every 90 days, and that ASPSPs will *not be permitted* to require SCA every 90 days for those connected accounts, and that SCA will only be required for the initial connection. We urge the FCA to make this new 10A exemption explicit in its language. Although the current language permits for ASPSPs to exempt customers from SCA every 90 days, in practice, it is not in their incentive to apply that exemption, which is the exact behaviour that has prompted this consultation in the first place.

Any delay to implementing the change to the SCA-RTS 90 day reauthentication requirement will irreparably harm the UK market and result in the failure of Open Banking

According to the CP21/3, section 1.14 Measuring Success, key indicators include continued growth in the number of providers and users of open banking in the UK. However, the timeline for rolling out the effective changes will have a negative impact on the number of firms in the market. FDATA member attrition rates indicate that a significant number of firms will most likely exit the market given attrition rate anywhere from 13-35% month on month.

The proposed changes are likely only to be approved by Q3 2021. An 18-month grace period to implement said changes (including the minor technical modifications that must be made by both TPPs and ASPSPs) takes us into Q1-2 of 2023. Delaying the remedy to TPP attrition due to SCA at the 90-day mark will result a significant contraction of the UK Open Banking Market. According to OBIE published KPI Dashboards for March, 2021, there are currently 355 TPPs in production in the market. With customer churn rates hitting double digits monthly, and attrition rates averaging around 24% monthly, and considering value propositions being withheld from market due to reauthorisation requirements, there is no doubt that the UK open banking market will shrink over the next two years if the proposed changes are not delivered more urgently.

A mass exodus of providers from the market means a corresponding contraction of users of open banking in the UK; in no way can a contraction of both the supply and demand side constitute success. It is therefore critical that the timeline for implementation of relief to the

90-day SCA reauthentication requirement be accelerated and hastened to market. We strongly urge the FCA to reconsider its

customary time frame for rolling out these changes. Any delay will have a materially negative impact on open banking, competition, and better customer outcomes for UK consumers and SMEs.

SCA was originally intended to be a security tool, however it has turned into a brute tool to manage consent, resulting in harm to the very competitive firms PSD2 and Open Banking are meant to foster.

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 (personal finance management where the service happens in the background before accessing 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.

Customer churn is a natural part of business, however the SCA and 90-day rules amplify churn rates.

Churn is a reality for all digital solution providers: every app provider across every industry experiences churn. Even during the pandemic Netflix experienced customer churn – in its early days it saw 10% monthly churn, but for the last couple of years it averages at 2% a month.[2] 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: the requirement to reauthenticate every 90 days.

One FDATA member submitted evidence of quarterly churn due to 90-day reauthentication. 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 churn rates have increased exponentially. 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 FDATA member 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

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

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 its 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? Any delay to implementing a change to the rule will continue to produce churn rates so unsustainable that businesses are sure to exit the UK Open Banking market.

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 TPP, all evidence pointed to something other than these typical churn reasons. This TPP has a high product-market fit: 96% of their users would be disappointed if they could no longer use the app.[3] 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 TPP 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 TPP is a repeat British Bank Award winner.

Post FCA Solution Implementation Timeframe: Delays are Detrimental

Any delay to the implementation of the new Article 10A exemption further exacerbates attrition rates, and puts the nascent TPP market at risk of failure and a mass exodus of firms from providing innovative offerings to UK customers. Allowing the customary 18-month period post conclusion of this consultation puts the solution to customer attrition and TPP death out another two years. This is untenable; the open banking competitive landscape cannot survive another two years unscathed. This delay puts the entire open banking experiment at significant risk. We strongly encourage the FCA to reconsider any further delay as:

- No significant tech changes will be required on the ASPSPs side if the Article 10A exemption expressly forbids the ASPSP from applying SCA while customer consent is active, and ● The technical changes for ASPSPs amount to switching a few parameters off, or changing the timeframe parameters for the consent token.

Instead, FDATA proposes a 3 month transition period given the little tech changes required for both ASPSPs and TPPs, rather than the much longer time frame noted from our conversation with the FCA Payments Policy team on 21 Apri, 2021.

[3] 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.

Delegated consent: accountant or solicitor for SME cloud accounting services

FDATA also encourages the FCA to consider alternative approaches to consent management, especially given the particular use case for cloud accounting service providers, for example Delegated Consent.

FDATA members who provide cloud accounting services have noted that the explicit re-consent seems unnecessarily burdensome when the user has authenticated with the TPP application and continues to directly access their account transactions in the TPP application within the previous 90 days (e.g. to include them in their accounting records). Consideration also needs to be given to the impact of this provision on delegated access; in this case, an accountant using accounting software on behalf of their client.

The following use case in particular highlights just how detrimental these SCA and 90-day reauth rules can be: 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.

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.

[4] Not publicly available, however survey and evidence was shared in closed session with UK regulators. 8

This poses a significant risk for 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.

A delegated consent would improve the outcomes for small businesses significantly, and reduce the risk of those SME accounts being disconnected. It would also reduce the security risk of any workaround, and ensure that accountants are accounting rather than chasing their clients for renewed consent. FDATA suggests that as part of the delegated consent journey that each time an advisor, lawyer, accountant, etc. – whomever has delegated consent – re-consents on the PSUs behalf, the PSU receives notification of re-consent as either a push notification or via email.

We urge the FCA to also consider a longer consent access timeframe: 180 days instead of 90. The choice of 90 days may work well at preventing zombie account access in scenarios where the requirement for data is relatively short-lived (i.e., establishing credit worthiness or trying out a new application), however it seems unnecessarily burdensome when the user has regulalary confirmed access over many years. In practice, irrespective of the value proposition or business model, it will be necessary to ask the user to re-consent well before the 90 day limit to avoid the TPP being disconnected and the user having to reauthenticate because the 90 day deadline has

been missed.

We also urge the FCA to consider a “grace period” that maintains authentication but limits the permission to pull data. We advocate a 180 day timeline rather than 90 days to renew consent. We also propose an additional ‘grace period’ when the user has neither granted nor declined consent. During this period, the TPP would not be permitted to pull data from
the ASPSP, but would not need to revoke the authorisation. If consent is renewed within this grace period, there would be no need

for the user to reauthenticate. If consent is not renewed within the grace period, the TPP would be required to revoke access once the grace period expired.

It seems overly punitive to cut off both consumer and TPP at 90 days when the original choice of 90 days is arbitrary, and the only reason for it is to protect the narrow band of consumers who forget they've granted access to data. The proposed grace period still provides for consumer protection in that data cannot be pulled past day 90, but it still allows the consumer additional time to renew consent without having to be inconvenienced by reauthentication or set up the TPPnservice from scratch again.

Q2: Do you agree with our proposal to mandate the use of dedicated interfaces for TPP access to retail and SME customers’ payment accounts and the timeline for making those changes? If not, please explain why.

Yes, FDATA agrees with the proposal to mandate dedicated interfaces for TPP access. However we disagree with the proposed 18 month implementation timeline post FCA published final guidance. Rather, we propose a 9 month implementation timeline. This would also include a transition period for TPPs migrating customers to the API.

FDATA has noted before that due to the nature of MCIs, they require a customer be present for *every data transfer* from the ASPSP to the TPP. Combined, the current 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. MCIs are another technology layer TPPs 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.

Eliminating this exemption pushes the rest of the market to level up to the CMA9. 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.

However, by not explicitly detailing (yet) what level of performance and conformance these APIs will require, the move from MCI to dedicated interface may not result in good customer outcomes. Experience in delivering Open Banking has proven just how crucial consistent performance and conformance is, and the CMA9 have improved both conformance and performance immensely under the OBIE's supervision. But ASPSPs not mandated under the CMA's Order are not held to the same technical standard, nor the performance and conformance requirements. This proves the point that independent oversight and monitoring are crucial to achieve quality delivery across a single market.

Moreover, 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. The contingency access method RTS Article 33 provides is yet another paradoxically ineffective approach to ensure TPPs have access to data. RTS Article 33(4) explains the conditions and expectations on the ASPSP 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 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. 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.

In addition, RTS Article 32(3) specifically says that ASPSPs 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.’

The intersection of poor API performance and mandatory redirection results in bad customer journeys and outcomes. 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 ASPSP, the TPP, 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 ASPSPs cannot force TPPs 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.

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

FDATA urges the FCA to consider the standards to which ASPSPs are held who move from MCI to API, as well as how to best measure conformance and performance. We further encourage the FCA to not allow poor API performance an exception in the form of the Contingency Access Method, and to revoke the applicability of Article 30(1) as well.

Q3: Do you agree with our proposals to only require ASPSPs to make the technical specifications and a testing facility available at market launch of the interface, and to delay the need for a fallback interface for six months from the point of launch? If not, please explain why.

FDATA agrees with the proposal.

Q4: Do you agree with our proposal to treat ASPSPs with exemptions from setting up the fallback interface granted by home state competent authorities, as though they were granted an exemption by the FCA? If not, please explain why.
FDATA agrees with the proposal to treat non-UK ASPSPs operating under the Temporary Permit Regime, who have an exemption from setting up the fallback interface granted by their home state competent authorities, as those the exemption were granted by the FCA – until the time their FCA license is issued.
Q7: Do you agree with the proposed changes to guidance on SCA? If not, please explain why. FDATA agrees with the proposed change to the SCA requirements on dynamic linking (SCA does not need to be reapplied where the final payment amount does not exceed 20% above the original payment amount). We also agree with the Commission's conclusion that baring fraud, the payee's PSP (merchant acquirer) is liable when the transaction is carried out without applying SCA under a triggered exemption. We agree with the EBA's opinion on SCA elements and support the FCA's proposal to update the Approach Document to reflect the same. We agree with the FCA's proposal to update the transaction risk analysis to reflect the EBA's. We agree with the EBA's opinion on the corporate card exemption, and the FCA's proposal to update its guidance to reflect it. We agree with the proposed update to guidance on authentication code usage. We agree that merchant initiated payments for recurring payments is outside the scope of SCA. We also agree with the proposed changes to SCA in relation to contactless card payments.

Q10: Do you agree with the proposed changes to the sections above? If not, please explain why.

Financial Data and Technology Association

FDATA agree with the proposal outlined in section 6.14 and 6.15, Information sharing from ASPSPs to TPPs: the sharing of name of the account holder, account number, and sort code with PISPs.

We also agree with the proposal in section 6.16, eIDAS certificates.