FCA clarifies safeguarding and SCA requirements for payment and e-money firms

HOT TOPIC

December 2021

Highlights

The FCA's Policy Statement clarifies its guidance for payment services and electronic money firms.

Most firms will be required to undertake significant enhancements in their safeguarding, SCA, risk management, governance and financial modelling capabilities.

Summary

The FCA issued PS21/19: Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual as well as an amended Approach Document (AD): Payment Services and Electronic Money – Our Approach on 29 November 2021.

New amendments in the documents include enhancements and clarifications over the safeguarding and prudential risk management regimes, as well as a definitive position on liability for fraudulent or unauthorised transactions between payment service providers (PSPs).

The FCA will also create a new strong customer authentication (SCA) exemption, removing the customer need to reauthenticate with their Account Servicing Payment Service Provider (ASPSP) every 90 days, when accessing their account information through a third-party provider (TPP).

Contacts

Nick Barratt
Director, Authentication & Transaction Monitoring

T: +44 (0) 7483 416290
E: nicholas.barratt@pwc.com

Gregory Campbell
Director, Safeguarding

T: +44 (0) 7971 479439
E: gregory.campbell@pwc.com

Stephanie Henderson-Begg
Director, Prudential Risk Management

T: +44 (0) 7711 562280
E: stephanie.k.henderson-begg@pwc.com

Laura Talvitie
Manager, Regulatory Insights

T: +44 (0) 7850 908244
E: laura.talvitie@pwc.com

Background

In its 2020/21 business plan, the FCA identified the payments sector as one of its three-year priority areas to ensure consumers transact safely with payment firms, that payment firms meet their regulatory obligations while competing on quality and value, and consumers and SMEs have access to a variety of payment services.

In line with this, the FCA published a consultation in January 2021, proposing changes to the SCA-RTS, the European Banking Authority's (EBA) regulatory technical standards (RTS) on SCA and secure communication.

The purpose of the consultation was to remove identified barriers to continued growth, innovation and competition in the sector, including open banking. The proposals were also intended to support resilience in the sector and protect consumers if firms fail.

The FCA will implement its proposals largely as consulted on. This includes a number of clarifications and amendments around:

- SCA
- safeguarding
- prudential risk management
- other updates, including onshoring changes relating to Brexit as well as amended regulatory reporting requirements.

Changes to the AD and perimeter guidance came into force on 30 November 2021. The changes to the technical standards on SCA and common secure methods of communication are implemented between 30 November 2021 and 26 May 2023.

Amendments to the SCA-RTS

The Policy Statement makes a number of changes to the SCA-RTS. The key amendments are summarised below.

90-day reauthentication

Currently, customers accessing account information through a TPP must authenticate via SCA when accessing their data for the first time. TPPs include organisations which offer account information services (AISPs).

Customers are also required to re-authenticate every 90 days for the TPP to continue accessing the customer data held by an ASPSP.

According to the FCA, the requirement to re-apply SCA every 90 days has proven burdensome for customers. As a result, it can create friction in the user experience and hinder uptake of open banking services.

The statement confirms that the FCA will implement its proposal to create a new SCA exemption (Article 10A) for when customers access account information through a TPP. As a result, customers will not need to reauthenticate with their ASPSP every 90 days. SCA will still be required when customers first decide to connect their account to a TPP service.

The FCA will add a requirement for TPPs to reconfirm their customer's consent for continued access to that customer's account data at least every 90 days.

What do firms need to do?

- AISPs will need to reconfirm at least every 90 days that the customer explicitly consents to the AISP accessing the account data.
- A single reconfirmation of consent may apply to more than one account, as long as it is clear that consent is given for multiple, specifically identified accounts.
- TPPs are responsible for re-confirming customer consent and will not be required to communicate customer consent to ASPSPs.
- TPPs must stop accessing the account information, where the customer fails to reconfirm consent after 90 days until consent is reconfirmed.
- The FCA strongly encourages ASPSPs to apply the new SCA exemption under Article 10A of the SCA-RTS as soon as practicable after it has come into effect, unless they have proportionate and objective reasons for not doing so (for instance, involving unauthorised or fraudulent access).
- AISPs must reconfirm customer consent under Article 36(6) of the SCA-RTS no later than four months following the new rules being made.
- AISPs must not access information without the customer actively requesting it, unless the customer has reconfirmed their consent within the previous 90 days.
- An ASPSP can rely on the SCA exemption in Article 10 (which requires ASPSPs to apply SCA at least every 90 days) where it is providing information to its customer as part of its own account information service. For example, where the ASPSP is providing information to its customer on accounts that it operates for its customer and accounts that another ASPSP operates for the customer.

Access interfaces

The SCA-RTS currently requires ASPSPs to establish an interface through which TPPs can access customer account information and payment functionality securely. This can be through a dedicated interface or a modified customer interface (MCI), where access is provided to TPPs via an existing customer interface, such as an online banking platform.

The FCA will implement its proposal to mandate the use of dedicated interfaces for TPP access to certain consumer and SME customers' payment accounts. This excludes interfaces which use screen scraping.

The requirement applies to personal payment accounts within the scope of the Payment Account Regulations 2015 (PARs), equivalent payment accounts held by SMEs, and credit card accounts held by consumers and SMEs.

The requirement will apply to credit institutions, authorised payment institutions, authorised electronic money institutions, and credit unions which offer these types of payment accounts online. However, the requirement will exclude accounts provided by small payment institutions, small e-money institutions, firms relying on the temporary permissions regime (TPR) or supervised runoff regime and non-SME businesses' accounts. This means the use of MCIs will remain a compliant alternative for such accounts.

What do firms need to do?

- Relevant firms will need to make necessary changes within 18 months (aligned to the 18 months the SCA-RTS originally provided for open banking changes).
- ASPSPs will continue to be required to have fallback interfaces unless an exemption has been obtained under Article 13 of the SCA-RTS.

Technical specifications and testing facilities

At present, the SCA-RTS require ASPSPs to make a testing facility for TPPs available and provide interface technical specifications six months before new products and services are launched. The SCA-RTS also require those ASPSPs, which have developed a dedicated interface, to adapt their customer interface for use by TPPs if the dedicated interface becomes unavailable (the fallback interface).

The FCA will implement its proposals to require ASPSPs to make the technical specifications and the testing facility available only by the time of the market launch of a new product or service, rather than six months in advance. The FCA will also delay the need for a fallback interface for six months from the point of product launch.

What do firms need to do?

- The FCA expects testing facilities, available by the time of the market launch, to resemble the means by which the TPP accesses accounts on the live interface.
- It encourages ASPSPs launching new dedicated interfaces, to publish technical specifications and planned launch dates of their dedicated interfaces as soon as practicable, including for example in the Transparency Calendar of the Open Banking Implementation Entity.
- ASPSPs will be required to have a fallback interface no later than six months after launch.

Fallback interface

Where ASPSPs in the TPR have been granted fallback interface exemptions by their home state competent authorities, the FCA will treat them as though their exemptions had been granted by the FCA for the purposes of Article 33(6) of the SCA-RTS.

What do firms need to do?

- ASPSPs with a temporary authorisation will not need to apply for an FCA exemption while they are within the relevant temporary scheme.
- When European Economic Area ASPSPs apply to the FCA or the PRA for authorisation under the Electronic Money Regulations 2011 (EMR), Payment Services Regulations 2017 (PSR) or Financial Services and Markets Act, they will need to apply to the FCA for an exemption from the requirement to have a fallback interface, or put the fallback interface in place.

Changes to the AD - SCA

Under the PSR, payment service providers must apply SCA when a customer accesses a payment account online, initiates an electronic payment transaction or carries out any action through a remote channel that may create a risk of payment fraud.

The FCA's amendments to the AD reflect the consultation proposals as well as various Q&A responses and opinions on SCA, as published by the EBA and the EC.

Dynamic linking

Dynamic linking requires a customer's authentication of a payment instruction to be linked to a specific payee and a specific amount. Currently, difficulties may arise where the final amount is not known in advance (for instance, where substituted products change the final price).

The FCA will implement its proposal to amend its guidance to explain that SCA does not need to be re-applied where: i) that final amount is higher than the original amount authorised, ii) the final amount is within the 'customer's reasonable expectations', and iii) the customer was made aware that the amount could increase.

The FCA confirms that the 'customer's reasonable expectation' means that the payment should not exceed 20% above the amount originally authorised, without further SCA being performed. This includes any taxes and shipping costs.

What do firms need to do?

- The merchant must specify that the price could vary upwards. The customer must agree to that possibility.
- If neither is completed, the ASPSP must re-apply SCA.
- ASPSPs need to ensure systems and processes are in place to verify that the new transaction amount does not exceed 20% above the original amount authorised.

Liability for fraudulent or unauthorised transactions

The FCA will adopt the allocation of liability as consulted on. This aligns with the European Commission's (EC) opinion, published by the EBA in July 2019.

As a result, the payee's PSP will be liable where it triggers an exemption and the transaction is carried out without applying SCA. Where the payer has not acted fraudulently, the payer's PSP must refund the customer and will be entitled for a reimbursement by the payee's PSP.

What do firms need to do?

- Where the payee's PSP invokes SCA, that SCA must be delivered in line with the RTS-SCA. Where exemptions are used this must also be delivered in line with the RTS-SCA.
- If the payee's PSP outsources any SCA elements, they must ensure that all parties comply with the general requirements on outsourcing, including the requirements in the EBA Guidelines on Outsourcing.
- Firms need to ensure that, in specific relation to the use of the exemption laid out under Article 18 of the RTS, they have had an independent and qualified external auditor conduct an audit of the methodology, the model and the reported fraud rates.

SCA elements

The FCA will adopt the EBA's view, from June 2019, on possession and static card data.

A device can only be used as evidence of possession where there is a reliable means to confirm it (i.e. the device is used by the owner). The FCA also confirms that static card data (including the card security code) cannot constitute a knowledge factor or a possession factor for SCA.

The FCA expands the EBA's definition on inherence, as a possession factor under SCA. Inherence is a characteristic attributable to a person. This can be a physical property of the body (e.g. a fingerprint) or a behavioural characteristic (e.g. detailed shopping patterns).

What do firms need to do?

- Firms must ensure that any individual SCA inherence solution used complies with regulatory requirements. This includes Article 8 of the FCA's Technical Standards for SCA.
- Firms should consider how to use the behavioural characteristics of an individual for SCA purposes and how it could enable SCA solutions better suited to protect vulnerable customers.

Other updates include:

- The FCA will implement the EBA's previous view that the authentication elements a customer uses when they access their payment account online, may be reused if the customer then initiates a payment within the same online session.
- The FCA will incorporate the EBA's previous clarification on transaction risk analysis. As a result, fraud rate calculations for transactional risk analysis should only include unauthorised or fraudulent remote electronic transactions for which the PSP was liable.
- The FCA will adopt the EBA's previous note that the corporate exemption under Article 17 of the EU-RTS applies to card payments, provided that those cards are used in a secure corporate payment process.
- The FCA will implement the EC's previous clarification on the position relating to merchant-initiated transactions. Transactions initiated by the payee only, without any involvement from the payer, are not in scope of SCA (e.g. subscriptions).

Changes to the AD - safeguarding and prudential risk management

The FCA published temporary guidance on safeguarding and prudential risk in July 2020. The purpose of the guidance was to strengthen payment and e-money firms' arrangements in the exceptional circumstances of the pandemic. The FCA considers the guidance to remain helpful long-term and implements it largely as proposed in CP21/3.

Safeguarding - external audit

The FCA confirms its expectation for firms to instruct external auditors to provide an annual reasonable assurance opinion over:

- whether the firm has maintained adequate organisational arrangements to enable it to meet the FCA's expectations of its compliance with the safeguarding provisions in the EMRs or PSRs, throughout the audit period
- whether it met those expectations at the audit period end date.

The FCA clarifies that it expects this audit opinion to also address effectiveness of controls throughout the period.

The FCA will not mandate the use of a specific audit standard (such as ISAE 3000). The regulator acknowledges that there may be scope to develop a bespoke audit standard for the sector at a later date, similar to CASS.

The FCA increases the cost estimates for the safeguarding audit from £12,000 for all firms to £100,000 for medium firms, and £200,000 for large firms. No change is made to the cost estimates for small firms.

The FCA notes a four-month deadline for audit report issuance after period-end 'as a rule of thumb', The FCA expects that some firms may wish to align the audit period with their account year end.

Other safeguarding updates

- The FCA removes the ability to use a credit institution within the same corporate group.
- The FCA amends the AD to build out the expectations around its insurance approach.
- It also adds specific requirements for firms to review third party providers at least annually. The FCA clarifies the the nature of breaches/issues which would require an ad hoc FCA notification.
- Finally, given a recent High Court judgment, the FCA removes the interpretation that the EMRs create a trust over the money received by an EMI. The FCA has appealed the decision.

What do firms need to do?

- Review the adequacy of the audit(s) that have been performed to date.
- Review the changes to Chapter 10 of the AD to determine whether changes or enhancements need to be made to existing policies, processes and controls.
- Consider adequacy of breach reporting mechanism.
- Consider triggers that would meet the definition of 'significant change'.

Prudential risk management

The FCA implements its proposals as consulted on. While the content of the proposals for prudential risk management were previously provided under temporary guidance during COVID-19, PS21/19 will make these changes permanent.

Application programming interfaces, authorised e-money institutions and small electronic money institutions are required to operate effective procedures to identify, manage, monitor and report any risks to which they might be exposed. This is outlined under the conditions for authorisation or registration in regulation 6 of the PSRs and regulations 6 and 13 of the EMRs.

The FCA's guidance clarifies the most effective way of complying with regulation, reducing the risk of a firm failing to meet its capital requirements or failing to meet its liabilities as they fall due. This includes any material risks that arise as a result of the firm's relationship with other members of its group. Where firms do not follow this best practice approach, they will need to demonstrate that they are still adequately managing liquidity and group risk, complying with their conditions of authorisation or registration.

The FCA also provides additional clarification on wind-down plan development and the expectation for the plans to include scenarios in which a firm's business would need to be wound down.

What do firms need to do?

- Overall, most firms will be required to undertake significant enhancements in their risk management, governance and financial modelling capabilities.
- Firms need to carry out liquidity and capital stress testing, to analyse how exposed they are to severe business disruptions and assess the potential impact, using internal and / or external data and scenario analysis.
- Firms need to use the test results to ensure they can continue to meet their conditions of authorisation and own funds requirements.
- Results should help firms to assess whether they have adequate liquidity and capital resources as well as identify changes and improvements to required systems and controls.
- Firms must accurately calculate their capital requirements and resources on an ongoing basis and report these correctly to the FCA in regulatory returns and upon request.
- Firms need to consider their own liquid resources and available funding options to meet their liabilities when they are due, and whether they need access to committed credit lines to manage their exposures. Firms should do this as part of their liquidity risk-management procedures.
- Firms need to develop and maintain wind down plans to help manage their liquidity and resolution risks.
- Wind down plans should consider different scenarios under which a wind down may occur, including both solvent and insolvent scenarios.

Other updates

The FCA's publications contain many other updates, including Brexit implications on on-shoring and other general updates. Firms should refer to the FCA's publications for further information.

Next steps

The FCA's amended AD (version 5, November 2021) came into force on 30 November 2021.

Perimeter guidance (payment services) Instrument 2021 came into force on 30 November 2021.

Regarding the technical standards on SCA and common and secure methods of communication (amendment) (No 2) instrument 2021:

- Articles 10A and 36(6) in the Annex, and the amendments to Article 10 in the Annex come into force on 26 March 2022.
- The amendments to Article 31 in the Annex come into force on 26 May 2023.
- The remainder of the Annex came into force on 30 November 2021.

ASPSPs offering personal payment accounts in the scope of the PARs, equivalent payment accounts held by SMEs and credit card accounts operated for consumers or SMEs will need to have a dedicated interface in place no later than 18 months after the rules come into force.

The FCA strongly encourages ASPSPs to apply the new exemption from the obligation to carry out SCA as soon as practicable after it has come into effect. TPPs will need to reconfirm customer consent under Article 36(6) of the SCA-RTS no later than four months after the rules come into force.

Contacts

Nick Barratt
Director, Authentication & Transaction Monitoring

T: +44 (0) 7483 416290
E: nicholas.barratt@pwc.com

Gregory Campbell
Director, Safeguarding

T: +44 (0) 7971 479439
E: gregory.campbell@pwc.com

Stephanie Henderson-Begg
Director, Prudential Risk Management

T: +44 (0) 7711 562280
E: stephanie.k.henderson-begg@pwc.com

Laura Talvitie
Manager, Regulatory Insights

T: +44 (0) 7850 908244
E: laura.talvitie@pwc.com