Date: October 2020

UK Finance Industry Guidance on Strong Customer Authentication under PSD2

Introduction to UK Finance and purpose of the guidance

UK Finance is providing this guidance to assist the industry in implementing the requirements under the revised Payment Services Directive (PSD2) and the accompanying Regulatory Technical Standards on strong customer authentication and common and secure communication which have been in place since 14 September 2019.

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation. We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

This guidance was originally published in October 2018 and has been updated to incorporate key output and guidance of UK Finance members under the 'managed roll-out' pursuant to which the FCA announced and agreed to provide the payments and e-commerce industry extra time to implement SCA. Further information on the work of UK Finance in relation to the managed rollout and its implementation plan for SCA readiness can be found on the SCA homepage of UK Finance's website.

This version of this guidance is dated 1 October 2020. UK Finance expects to update this guidance to include additional sections, for example, dealing in detail with GDPR considerations of behavioural biometrics and implementation of the Article 18, transaction risk analysis (TRA) exemption, as discussion on these topics concludes.

This guidance is written and provided for general information purposes only. It is not intended, and should not be used or relied upon, as a substitute for taking appropriate legal advice, and such advice should be taken before acting on any of the topics covered.

Neither UK Finance nor Osborne Clarke LLP accept any liability to any third party in relation to the contents of this document, and any opinions expressed in this document are the opinions of UK Finance.

Table of Contents

1. Introduction to strong customer authentication

1.1 One of the major aims of PSD2 is to reduce fraud in electronic payments. One of the core measures to achieve this aim is the requirement in Article 97 PSD2 (regulation 100, Payment Services Regulations 2017 (PSRs 2017)), which mandates the application of strong customer authentication (SCA) in specified scenarios. Article 97 PSD2 has been implemented in the UK through the PSRs 2017 and regulation 100 in particular. There are some very slight differences of wording, for example, the PSRs 2017 refer to "payment service user" rather than "payer", but these do not affect the substantive aspects of the requirements, rather they make them clearer and more accurate.

- 'Strong customer authentication' is defined in PSD2 as "*an authentication*[1] *based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data".*
- Article 97(1) requires that a PSP applies SCA "*where the payer: (a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses*".
- Article 97(2) requires that *"for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee."*

1.2 In accordance with Article 98(1) PSD2 the EBA has developed regulatory technical standards (RTS) that provide further detail on the requirements of SCA, certain exemptions from the application of SCA and requirements with which security measures must comply in order to protect the confidentiality and integrity of users' personalised security credentials (PSC). The RTS provisions relating to SCA have applied from 14 September 2019. However, in the UK, the FCA has given firms extra time to implement SCA in relation to e-commerce card transactions by a revised date of 14 September 2021. The timeline was originally extended by 18 months after the EBA accepted that the FCA and other national competent authorities may give firms extra time to implement SCA in these circumstances in response to concerns about industry readiness to apply SCA to e-commerce card transactions, with the FCA granting a further six-month extension given the impact of the Covid-19 crisis. Separately, the EBA has specified a deadline of 31 December 2020 (by which the period of supervisory flexibility should end) and has not extended the timeline beyond this.

1.3 The EBA has also published two opinions (EBA Opinions):

a) dated 13 June 2018 which aims to provide clarity on the implementation of certain aspects of the RTS (June 2018 EBA Opinion); and

b) dated 21 June 2019 which aims to provide clarity on compliant approaches to the three elements of SCA (June 2019 EBA Opinion).

This guidance also makes reference to the EBA's Single Rulebook Q&A tool, through which the EBA seeks to provide further clarity on the interpretation of the RTS.

1.4 The new regulatory requirements on SCA make authentication a key requirement for the provision of electronic payment services and should therefore be a strong focus for all PSPs.

1.5 This guidance first considers the requirements of SCA as set out in Article 97 PSD2 (regulation 100, PSRs 2017), the accompanying RTS provisions and where relevant the EBA Opinions. It then goes on to deal with the exemptions from the application of SCA and certain key topics or key sectors in relation to which UK Finance has identified that additional guidance is required.

[1] 'Authentication' is also defined in PSD2 as: "*a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials*"

2. Scope of strong customer authentication

This section gives further detail on the scope of SCA, what is out of scope and what SCA applies to.

What is strong customer authentication?

2.1 In its simplest form, SCA means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data. However, there are multiple other requirements that sit alongside this.

2.2 The RTS require that the two or more authentication elements used result in the generation of a secure authentication code. The recitals to the RTS explain that the authentication code "*should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled*".

2.3 In addition, for electronic remote payment transactions (e.g. payments on the internet), the authentication code generated must be specific to the amount of the payment transaction and the payee. This is known as 'dynamic linking' and is discussed in more detail below.

2.4 The RTS also require (see Articles 24 and 25) that PSPs ensure that only the user is associated in a secure manner with the personalised security credentials (e.g. online banking log-in credentials or card PIN numbers), authentication devices and software and sets minimum requirements for such association and for the delivery of the personalised security credentials, authentication devices and software to the legitimate user. These include ensuring that where delivery occurs outside of the PSP's premises or through a remote channel no unauthorised party can obtain more than one feature and that the delivered credentials, devices and software require activation in a secure environment before usage. For example, a card issuer should ensure delivery of a payment card and the associated PIN separately and arrange for activation of the card by applying the PIN before first contactless usage. A similar approach should be adopted for a user's registration for online banking or a mobile banking app. Similarly, where association of the user's identity with the personalised security credentials and with authentication devices and software takes place through a remote channel, the RTS requires that such association is to be performed using SCA (Article 24(2)(b)).

What does strong customer authentication apply to?

2.5 Unless a transaction is out of scope or an exemption applies, PSPs must apply SCA in specified scenarios, i.e. where a user:

a) accesses their payment account online;

b) initiates an electronic payment transaction; or

c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2.6 All electronic payments initiated by the payer are covered by the scope of the SCA requirement, unless one of the limited number of exemptions applies. This scope is broad as it covers both remote and face-to-face electronic payments initiated by the payer and extends to all channels or devices through which initiation occurs, so including payments made through a browser, mobile, in-app, devices using the Internet of Things (IoT), as well as payments made via a terminal where the data extracted in relation to the payment is all electronic.

2.7 This means SCA applies in a number of noteworthy environments, for example, card payments and online transactions. All PSPs are required to apply SCA when the payer initiates an electronic payment transaction, or when executing (acquiring in the context of card payments) such electronic payment

transactions. The requirement for SCA applies to all electronic payment transactions initiated by the payer, regardless of whether the payer is a person or a legal entity.

2.8 SCA should also be applied each time a payer accesses its payment account online or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse.

2.9 Examples of actions through a remote channel 'which may imply a risk of payment fraud or other abuse' include:

- customers setting up a 'trusted beneficiary', changing a trusted beneficiary's account details, creating a standing order or giving an e-mandate for Direct Debits;
- updating an address, changing a PIN number or other personal security credential activity in addition to other activity which PSPs may identify.

What payment types are out of scope?

2.10 In addition to the specific exemptions from SCA provided for in the RTS, certain payment transactions are out of scope of the requirement to apply SCA, including those set out in the table below.

Transaction type	**Reason for being out of scope of SCA requirement**
Direct Debits of fixed or variable amount that are initiated by the payee **only** without any direct intervention from the payer	These Direct Debit payments are initiated by the payee based on a pre-existing authority, not by the payer: the payer is not involved in the initiation of these transactions. However, when the payer sets up the Direct Debit mandate, this action may be caught by the SCA requirement if given electronically (e.g. an e-mandate) under the third 'other action' requirement of SCA (SCA does not apply to paper Direct Debit mandates). This is more generally applicable to SEPA Direct Debits which use e-mandates rather than to Bacs Direct Debits for example. Direct Debits need to be distinguished from standing orders, which are set up by the payer with their bank, rather than with the merchant. Standing orders are initiated by (or on behalf of) the payer, and therefore are caught by the SCA requirement unless an exemption applies.
Card payments of fixed or variable amount that are initiated by the payee **only** without any direct intervention from the payer (these are known as 'Merchant Initiated Transactions' or MITs)	The payment is initiated by the payee based on a pre-existing authority, not by the payer: the payer is not involved in the initiation of these transactions. However, as with Direct Debits, if the authority for the payments is given electronically (such as with online subscription services), then the action of granting the authority will be caught by the SCA requirement under the third 'other action' requirement of SCA. In certain use cases, the payment authority will have been given on paper and so will be out of scope for that reason.

MOTO (mail order and telephone order) transactions	The payment is initiated by paper or telephone (not electronically), notwithstanding that they result in the generation of an electronic transaction[2]. The EBA has clarified that Interactive Voice Response (IVR) mechanisms may, depending on the precise solution, be treated as MOTO transactions, however, where such technology is used to initiate electronic payment transactions through the internet or otherwise at-distance channels, they will generally be treated as electronic transactions and therefore are in scope of strong customer authentication.[3] While MOTO is realised through manual "PAN Key" entries, it should be noted that such entries may only be used with genuine MOTO transactions and not, for example, for face to face transactions.
Telephone banking (e.g. paying a credit card bill via telephone conversation)	Out of scope as it is a telephone transaction.
Paper-based transactions (e.g. fax)	Out of scope as it is a paper-based transaction.
Payments made through anonymous payment instruments	Due to their very nature, these transactions need to be out of scope[4].
Payments initiated as a result of product switching (for example use of the Current Account Switch Service (CASS))	Out of scope, along with the Bacs Cash ISA Transfer Service, on the basis that such payments rely upon the original take-on instruction given by the consumer to the transferee entity.

Why are Direct Debits and MITs out of scope?

2.11 Payee or card-based merchant initiated transactions (MITs) are out of scope of the requirement for SCA and do not need to rely on an exemption. They include Direct Debits or card transactions, where the transaction is initiated by the payee only.

2.12 Direct Debits are out of scope only where the Direct Debit payment is initiated by the payee without any direct intervention from the payer. The Direct Debit mandate itself may be caught by the SCA requirement if given electronically (e.g. an e-mandate for a SEPA Direct Debit) under the third 'other action' requirements of the RTS, but it is not in scope if given on paper. The EBA has expressly confirmed this position.[5]

2.13 MITs are very similar and describe a payment or series of payments initiated by a payee without any direct intervention from the payer under the terms of a pre-existing authority given by the payer to the payee.

2.14 While the customer or payer will be involved in setting up the authority and (for a series of transactions) may initiate the first transaction, they will play no part in initiating subsequent transactions. Typical examples of MITs include:

- a contract mobile phone bill where a different amount is taken by the payee each month according to the customer's usage;

[2] EBA Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of PSD2 (23 February 2017), Q46 in EBA Feedback Table; FCA Approach Document, paragraph 20.11
[3] EBA Single Rulebook Q&A: 2018_4058
[4] Recital 8, RTS
[5] EBA Single Rulebook Q&A: 2018_4031

- an annual magazine subscription where the same or a slightly differing amount is debited monthly on the same day of the month for twelve months (or longer);
- additional charges on a hotel bill where the customer has chosen to use an express checkout service.

2.15 The EBA has clarified[6] that MITs are considered out of scope of the SCA requirement so long as they are governed by a valid authority given by the payer to the payee, are initiated by the payee only, and where required (e.g. if established electronically) SCA was applied when that authority was first given or when it is amended. It does not matter if the first transaction is initiated based on an instruction given at the same time the authority is given or later, or if by mail or telephone order. It also does not matter if the MITs occur with varying frequency or for varying amounts, so long as they are consistent with the authority given (i.e. within the customer's reasonable expectation). There is also no regulatory requirement for the MITs to include any indicator connecting them to the payer's original authority; the responsibility for keeping a record of this lies with the merchant and is necessary to enable a 'look-back' when a transaction is disputed, though it is good practice for controls around MITs to be applied by the card schemes (which may provide for rules around transaction IDs which link a subsequent transaction back to the original transaction) and acquiring PSPs. UK Finance is also of the view that mandates currently in place can be grandfathered once the SCA requirements in relation to e-commerce transactions are enforceable (i.e. from 14 September 2021).

Geographical scope generally

2.16 The SCA requirement in PSD2 is not expressly limited in its territorial scope, so for example it applies where a payer accesses their account online irrespective of from where they are accessing it on a particular occasion. The same applies when a payer initiates an electronic payment transaction or carries out any other action through a remote channel.

Application to OLO card transactions

2.17 In a cards context, however, additional considerations apply because card transactions for UK or EEA issued cards may be initiated outside of the EEA, by merchants and their acquirers located elsewhere, for example in the USA. These considerations are further complicated by Brexit.

Best-effort basis for OLO card transactions

2.18 Such scenarios are recognised by the EBA in its June 2018 EBA Opinion (see paragraph 32), which states that "*the EBA's view, after discussing it with the European Commission, is that SCA applies to all payment transactions initiated by a payer, including to card payment transactions that are initiated through the payee within the EEA and apply only on a best-effort basis for cross-border transactions with one leg out of the EEA. In such a case the liability regime stated by Article 74(2) PSD2 applies*" (emphasis added). UK Finance understands that this view was formed on the basis that the payee's PSP (acquirer) in such cases will typically be located outside of the EEA and so not subject to the SCA requirement and the payer's PSP (card issuer) has no way of controlling or imposing SCA when the non-EEA payee (merchant) initiates the card transaction.

No expectation to apply SCA where issuer cannot technically impose use of SCA

2.19 The EBA elaborated on its view as part of its EBA Single Rulebook Q&A: 2018_4233 published on 6 September 2019:

"*In the case of card-based payments where the payee's PSP (the acquirer) is located outside the Union (the so-called "one-leg out transactions"), the acquirer is not subject to PSD2. Where the payer wishes to make a card-based payment at the point of sale (POS) or in an online environment of a merchant whose acquirer is located outside the Union and the issuer cannot technically impose the use of SCA, the issuer shall make its own assessment whether to block the payment or be subject to the liability requirements under Article 73 PSD2 vis-à-vis the payer in the event that the payment has been unauthorised.*

[6] EBA Single Rulebook Q&A: 2018_4031

In the case of card-based payments where the payer's PSP (the issuer) is located outside the Union (the so-called "one-leg in transactions"), the issuer is not subject to PSD2. Where the payer wishes to make a card-based payment at a POS or in an online environment of a merchant whose acquirer is located in the Union, the acquirer is subject to PSD2 as it offers its services in the Union. As such, it is required to be in a position to accept SCA and thus has to put in place mechanisms that allow for SCA."

Application post-Brexit

2.20 Put another way, the expectation to apply the SCA requirements on a 'best-effort' basis to OLO transactions is limited to where the issuer cannot technically impose the use of SCA. This is an important distinction post-Brexit, because while then the UK technically ceases to be part of the EEA and so strictly speaking cross-border UK/EEA transactions become one leg out (OLO) transactions, issuers need to assess if they technically can impose the use of SCA. This in turn leads to the view that where a UK issued card is used outside of the UK, there is a difference between it being used in the EEA (SCA should be applied because it can technically be imposed, because PSD2 requires that it be applied in the EEA) and elsewhere such as in the USA (SCA should be applied on a 'best-effort' basis). This in turn means that where a UK issuer receives a 'direct to auth' card transaction for authentication from an EEA merchant and acquirer, it should 'soft decline' the transaction, forcing the transaction through 3DS.

2.21 This view is supported by the text of PSD2: Article 2(4), PSD2 requires that SCA is applied to those parts of the payment transaction that are carried out in the EEA.

2.22 So in the case of EEA card issuers, since the authentication part of a card transaction is carried out by the card issuer in the EEA and the UK has an SCA regime and SCA infrastructure, there is a legal obligation on EEA issuers to apply SCA to UK/EEA cross-border transactions: Article 2(4), PSD2 applies in full (and not on a 'best-effort' basis) in relation to cross-border transactions with the UK, as no technical limitations will exist to apply SCA to those transactions.

2.23 Similarly, for UK card issuers: regulation 63(2) of the PSRs 2017 makes the same provisions as Article 2(4), PSD2 for the UK. Once these are amended by the EU Exit Regulations 2018, regulation 63(2) confirms that regulation 63(1)(b)(i) and (iii) only apply "*in respect of those parts of a transaction which are carried out in the United Kingdom"*. Since the authentication part of the transaction is carried out in the UK and the EEA has an SCA regime and SCA infrastructure, there will be a legal obligation on UK card issuers to apply SCA to UK/EEA cross-border transactions.

Working assumptions

2.24 This legal analysis is based on the assumptions that authentication is to be regarded as carried out in the jurisdiction of the payer's PSP (i.e. the location of the card issuer) and that post-Brexit EEA based payers and merchants will be supported by EEA card issuers and acquirers (for both scheme and regulatory reasons: passporting rights of UK firms to provide payment services to EEA users will cease as of 31 December 2020).

Aligned with FCA preliminary view

2.25 UK Finance understands that its views are aligned with the likely view of the FCA. UK Finance understands that the FCA will be updating its Approach Document, including as regards the treatment of OLO transactions, before the end of 2020. Meanwhile, UK Finance understands that the FCA's preliminary view is that if a UK card issuer is able to apply SCA (i.e. because the merchant can and there is a connection with the card issuer, e.g. through 3DS), then the FCA would expect the card issuer to do so. The FCA would likely tolerate them not doing so where the merchant is unable to apply SCA where the merchant and acquirer are outside of the UK (post-Brexit) or the EEA (for now) but it is unlikely that, post-Brexit, EEA countries will not be able to apply SCA, as PSD2 will apply in the EEA, so in all likelihood the FCA would be unlikely to tolerate card issuers not applying SCA for transactions where the acquirer is in the EEA. Conversely, where the card issuer is in the EEA but the payee's PSP in the UK, those card issuers will be subject to SCA under PSD2 and therefore the FCA would, in all likelihood expect SCA to be applied too. The FCA's view takes into account EBA Single Rulebook Q&A: 2018_4233, which it describes as helpful in this thinking.

Acting for non-UK/EEA merchants

2.26 Where a UK or EEA acquirer acts as payee's PSP for a merchant located outside of the UK and EEA, the acquirer will need to ensure that SCA can be applied to those transactions. In practice, this means that such a merchant would need to support 3DS or a similar alternative solution.

Summary of application of SCA to cross-border UK/EEA e-commerce card transactions

2.27 The table below summarises the application of SCA to cross-border UK/EEA e-commerce card transactions (RoW = Rest of World).

	UK merchant/UK acquirer	**EEA merchant/EEA acquirer**	**RoW (e.g. USA) merchant/RoW acquirer**
UK issuer/UK cardholder	SCA must be applied, unless MIT or exempt	SCA must be applied, unless MIT or exempt (as technically possible)	Expectation to use 'best efforts' to apply SCA (e.g. if transaction is submitted via 3DS)
EEA issuer/EEA cardholder	SCA must be applied, unless MIT or exempt (as technically possible)	SCA must be applied, unless MIT or exempt	Expectation to use 'best efforts' to apply SCA (e.g. if transaction is submitted via 3DS)

2.28 The table above focuses on cross-border UK/EEA e-commerce card transactions. Where a RoW cardholder supported by a RoW card issuer is using their card in the UK, unless the UK acquirer supporting the UK merchant knows the RoW card issuer can support SCA for that card transaction, then UK Finance's view is that the UK acquirer may send the transaction 'direct to auth' and treat it as out of scope of SCA.

Exemptions

2.29 Since there is a de facto recognition of each jurisdiction's SCA regimes, it should follow that exemptions from SCA, as allowed by both regimes, should also be mutually recognised and can be availed of.

Inclusion in TRA calculation

2.30 The EBA in its Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (EBA/RTS/2017/02) confirmed that OLO transactions should not be included in a PSP's fraud rate calculation. The EBA stated "*..the EBA is of the view that, in the light of the limitations of cross-border transactions, they shall not be included in the transactions for the purpose of the calculation of fraud rates..*" (page 142 of EBA/RTS/2017/02). Since there would be no technical limitation in this particular case of UK/EEA cross-border transactions, these transactions should be included in the calculation of a PSP's fraud rate for the purposes of the Article 18 (TRA) exemption.

Transitional Period

2.31 As noted above, there are different implementation deadlines for the application of SCA in e-commerce card transactions for the EEA and the UK, 31 December 2020 and 14 September 2021, respectively, and there are ramp-up periods before each of these deadlines. As a result, it is necessary to consider the position during this transitional period for UK/EEA OLO card transactions. Working on the assumption that authentication is to be regarded as carried out in the jurisdiction of the card issuer (as the payer's PSP), UK Finance's view is that:

UK issuers

- UK issuers should not change their behaviour towards EEA-acquired transactions until after 31 December 2020.
- Thereafter, assuming no post-Brexit treaty is entered into, UK issuers should change their behaviour towards EEA-acquired transactions in line with their own approach towards UK-acquired transactions, i.e. applying soft declines and requiring SCA as part of their own ramp-up plans.
- By and from 14 September 2021 UK issuers should be requiring SCA for EEA-acquired transactions (unless the transactions are otherwise out of scope of SCA e.g. because they are MITs).

Conversely, UK Finance's expectations is that:

EEA issuers

- During the period from 1 January 2021 to 14 September 2021, EEA issuers are free to insist upon SCA on UK-acquired transactions at any time.
- However, during this period, not all UK acquirers and merchants will be ready to submit transactions via 3DS and not all EEA issuers will be technically able to exclude UK-acquired transactions from mandatory SCA.
- Therefore, in order to align soft decline behavior between EEA issuers and adopt an approach which all issuers can sustain, during the UK's ramp-up, UK-acquired transactions will be excluded from SCA.
- From 14 September 2021, EEA issuers will insist upon SCA on UK-acquired transactions.

Non-UK/EEA transactions

2.32 For clarity, UK Finance does not expect issuers to change their approach to Rest of World (RoW) transactions which should be treated on a 'business-as-usual' basis.

Summary of application of SCA to cross-border UK/EEA e-commerce card transactions during transitional period

2.33 The table below shows the timing of the application of SCA during the transitional period. UK Finance is aware that national competent authorities in the EEA may take a different approach depending on their own ramp-up plans as applicable.

	UK merchant/UK acquirer	**EEA merchant/EEA acquirer**	**RoW (e.g. USA) merchant/RoW acquirer**
UK issuer/UK cardholder	SCA must be applied, unless MIT or exempt *Timing: from 1 January 2021 – market readiness; from 1 June 2021 – ramp-up and soft declines; from 14 September 2021 – fully in force*	SCA must be applied, unless MIT or exempt (as technically possible) *Timing: As for UK merchant/UK acquirer (as UK implementation follows EEA implementation)*	Expectation to use 'best-effort' to apply SCA (e.g. if transaction is submitted via 3DS) *Timing: Effective now, subject to issuer readiness for 3DS transactions*
EEA issuer/EEA cardholder	SCA must be applied, unless MIT or exempt (as technically possible) *Timing: Now – follow local ramp-up plans if*	SCA must be applied, unless MIT or exempt *Timing: Now – follow local ramp-up plans if applicable; from 1 January 2021 – fully in force*	Expectation to use 'best-effort' to apply SCA (e.g. if transaction is submitted via 3DS)

	applicable; from 1 January 2021 – exclude UK; from 14 September 2021 – include UK for SCA		*Timing: Effective now, subject to issuer readiness for 3DS transactions*

When can exemptions be applied?

2.34 The RTS include a number of exemptions where, subject to certain conditions being met, it is not necessary to apply SCA to a payment transaction. There is also one exemption where account information is being accessed, not a payment being made. The exemptions are listed in the table below and are discussed in more detail in the dedicated sections of this guidance.

2.35 A PSP can choose whether or not to rely upon an exemption, and so can choose to apply SCA even where an exemption is available. Where more than one exemption is available, a PSP must choose which exemption it is relying upon for a particular payment transaction.

2.36 The PSP applying SCA will be the ASPSP that issued the PSU's personalised security credentials. It is consequently also the same PSP (acting as ASPSP) that decides whether or not to rely upon an exemption or to apply SCA in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them.[7]

2.37 In a cards context, the EBA has clarified in its June 2018 EBA Opinion that the payee's PSP (i.e. the merchant acquirer) can rely upon certain types of SCA exemption or to request that an SCA exemption is relied upon. However, the EBA also clarified that the payer's PSP (i.e. the card issuer) always makes the ultimate decision on whether or not to accept or rely upon an SCA exemption. This is discussed further below.

2.38 The table below lists the exemptions.

RTS article	**Exemption**
Article 10	Access to payment account information
Article 11	Contactless payments at point of sale
Article 12	Unattended terminals for transport fares and parking fees
Article 13	Trusted beneficiaries
Article 14	Recurring transactions
Article 15	Credit transfers between accounts held by the same natural or legal person
Article 16	Low-value transactions
Article 17	Secure corporate payment processes and protocols
Article 18	Transaction risk analysis

3. Requirements of the elements for SCA

3.1 SCA means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence

[7] Paragraph 38, June 2018 EBA Opinion

(something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.

3.1 UK Finance's view is that as far as possible, whether in a cards, online banking, or open banking context, PSPs should do their utmost to deliver the best customer journey and deliver the spirit behind PSD2. This includes focusing on innovating to ensure the best customer experience. We have therefore deliberately remained less specific in the cases listed below.

3.2 UK Finance further recognises that the industry is constantly innovating and that in time the introduction of new data analytics and associated technologies such as physical and behavioural biometrics will bring improvements to security and the user experience. However, biometric capable devices are not available to all consumers yet and will take some time to be adopted by all.

4. Requirements of the elements categorised as knowledge

4.1 The authentication process can include an authentication element that is something only the user 'knows'.

4.2 PSPs have to mitigate the risk of this element being accessed by unauthorised parties, with measures in place to prevent disclosure of any knowledge elements to unauthorised parties.

4.3 In the June 2019 EBA Opinion, the EBA stated that: "*knowledge, by contrast with possession, is an element that should exist prior to the initiation of the payment or online access*". This means that for approaches currently observed within the market, a one-time password (OTP) which is generated or received on a device cannot constitute a knowledge element. More practically, in the context of e-commerce card transactions, it also means that a user cannot choose (or reset) their knowledge factor during the 3DS authentication challenge flow.

Guidance:

4.4 The table below, which is taken from the June 2019 EBA Opinion, sets out a non-exhaustive list of possible knowledge elements.

Element	**Compliant with SCA?*** *Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements
Password	Yes
PIN	Yes[8]
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated by, or received by, a device (hardware or software token generator, SMP or OTP)	No (for approaches currently observed in the market)
Printed matrix card or OTP list	No

5. Requirements of the elements categorised as possession

5.1 The authentication process can include an authentication element that is something only the user 'has'. PSPs must mitigate the risk of this element being replicated by unauthorised parties.

5.2 The June 2019 EBA Opinion confirms that the element of possession does not solely refer to physical possession but may refer to something that is not physical (such as an app). Recital 6 of the RTS refers to the requirement to have adequate security features in place and provides examples of possession as "*algorithm specifications, key length and information entropy*". Article 7 of the RTS requires that PSPs adopt measures "*to mitigate the risk that the elements of [SCA] categorised as possession are used by*

[8] UK Finance understands that the recognised industry position is that the 4-digit PIN that is ordinarily used for Chjp and PIN card-present transactions is not recommended for use as a knowledge factor in card-not-present transactions.

unauthorised parties" and that such measures are "designed to prevent replication of the [possession] elements".

5.3 The June 2018 EBA Opinion confirms that a device could be used to evidence possession, provided that there is a "*reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device*". The June 2019 EBA Opinion notes that evidence could, in this context, be provided through the generation of a one-time password, whether generated by a piece of software or by hardware, such as a token, SMS or push notification.

One-time passwords (OTPs)

5.4 OTPs will be a key component of many SCA-compliant journeys, applying equally in the context of credit transfers and card payments. The use of an OTP to evidence possession is most commonly carried out by way of OTP sent via SMS with possession by the cardholder of the SIM-card associated with the pre-registered mobile number.

5.5 However, there is nothing in the RTS nor the EBA Opinions to preclude the use of other means of sending OTPs not by SMS, namely landline or email, as a compliant SCA possession factor, provided that they can be associated, bound or linked adequately to the particular cardholder and provided the requirements of Article 7 of the RTS are met.

5.6 An issuer might consider using technology to help satisfy the requirements of Article 7 RTS, e.g. call-forwarding (for landline OTPs) and malware detection (for bound devices such as laptops and mobile apps), just as it might use SIM-swap technology (for SMS OTPs).

5.7 However, this is much more difficult where there is no such bound device (e.g. in the context of an email account) and issuers will likely look to satisfy the Article 7 RTS requirements using a risk-based approach, ensuring they have in place sufficient risk mitigation measures to reduce the risk of fraudulent transactions.

5.8 This may be easier to achieve where OTPs to email accounts are used in a corporate context where access to email accounts is often through multi-layered access-controlled secure corporate systems. Any risk here can also be more readily managed where the user is a corporate and the parties have agreed under the so-called 'corporate opt out' to disapply certain of the provisions of the PSRs 2017, including those which set a default position for the allocation of liability as between a PSP and its corporate payment service user. This approach would assist issuers with managing risk resulting from multiple persons having proxy access to an individual's email account (to whom an email OTP is sent), as liability for any unauthorised transactions can be placed with the corporate irrespective of the person accessing the email account.

5.9 In the context of payment service users who are not corporates, email OTP solutions may be particularly useful for issuers as a fall-back for customers for whom receipt of an SMS OTP is not possible, for example, because such customers do not have access to a mobile phone or sufficiently reliable mobile network coverage or because they are considered actual or potential 'vulnerable customers' in accordance with FCA guidance (e.g. due to a low knowledge of financial matters or low confidence in managing money). Absent email OTPs, alternative SCA-compliant journeys for these customers are also extremely limited, notably where data relating to behavioural biometrics is limited or weak, or where the use of landline OTPs is not possible.

5.10 Although compliance with the requirements of Article 7 of the RTS presents challenges, issuers may, using a risk-based approach, opt to use email OTPs as an SCA possession factor for customers in respect of whom there is no other alternative option or in a (lower risk) corporate context, where they would otherwise struggle to achieve SCA. This approach can be justified as avoiding poor consumer outcomes and is in keeping with the spirit of the RTS from a general policy perspective. In any event, UK Finance recognises that there are risks in the delivery of OTPs and therefore encourages all PSPs to make a thorough assessment of how OTPs will be delivered to customers.

EBA Guidance

5.11 The table below, which is identical to the EBA's in the June 2019 EBA Opinion, sets out a non-exhaustive list of possible possession elements. Noting the requirements of Article 7 RTS, the EBA has also confirmed that static card details are not sufficient to constitute a possession element for approaches currently

observed in the market, although a dynamic CVV meets the requirements for a possession-based authentication element.

Element	**Compliant with SCA?*** *Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	Yes
App or browser with possession evidenced by device binding – such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	Yes
Card evidenced by a card reader	Yes[9]
Card with possession evidenced by a dynamic card security code	Yes
App installed on a device	No
Card with possession evidenced by card details (printed on card)	No (for approaches currently observed on the market)
Card with possession evidenced by a printed element (such as an OTP list)	No (for approaches currently on the market)

5.12 In UK Finance's view, the following are also possible possession elements.

Element	**Compliant with SCA?*** *Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements
Possession of an email account evidenced by an OTP received by the email account, provided that it can be associated, bound or linked adequately to the particular cardholder and provided the requirements of Article 7 of the RTS are met	Yes
Possession of a landline evidence by an OTP received by the landline number, provided that it can be associated, bound or linked adequately to the particular cardholder and provided the requirements of Article 7 of the RTS are met	Yes

6. Requirements of the elements categorised as inherence

6.1 The authentication process can include an authentication element that is something the user 'is'.

6.2 PSPs must mitigate the risk of this element being replicated by unauthorised parties.

Behavioural biometrics

6.3 In the EBA Opinions, the EBA confirmed that inherence may include behavioural biometrics identifying the specific authorised user (emphasis added): "*The EBA is of the view that inherence, which includes*

[9] The EBA has confirmed that magnetic stripe cards are not compliant with SCA. In other words, the use of a magnetic stripe and signature is not compliant with SCA and should not be used (EBA Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of PSD2 (23 February 2017), Q2 and Q272 in EBA Feedback Table)

biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these"[10].

6.4 The EBA additionally confirmed that it is *"the quality of the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element"*[11], noting that any implemented approach must provide a *"very low probability of an unauthorised party being authenticated as the payer"*, and any devices and software used must be subject to measures ensuring that they *"guarantee resistance against unauthorised use of the elements through access to the devices and software"* in accordance with Article 8 of the RTS.

6.5 Provided these conditions are met, it is clear that behavioural biometrics identifying a specific user can constitute inherence as a compliant SCA-factor.

6.6 Some issuers may, in relation to a specific transaction, choose to 'layer' behavioural biometrics with other circumstantial evidence relevant to the transaction, such as the user's transaction history or their location data etc. However, this does not undermine or preclude the reliability of behavioural biometrics as an inherence factor in itself (and therefore a compliant SCA-factor per se).

6.7 Any additional 'layering' therefore operates to assist card issuers in providing stronger evidence that there is a very low probability of an unauthorised party being authenticated as the payer. Such layering is therefore recommended, though it is not necessary provided the issuer is confident the behavioural biometrics collected are sufficient to satisfy the requirements summarised above. Each issuer will, naturally, wish to consider its own position, taking into account all the relevant circumstances, including its own risk analysis.

6.8 For online e-commerce transactions, the recommended industry position is the use of behavioural biometrics as the second factor (in addition to the use of an OTP) in authentication, with no fall back (for scenarios where the use of behavioural biometrics is not feasible). The FCA supports the development of strategic solutions that are good for customers and businesses and has welcomed the industry's suggestion to focus on behavioural biometrics as second factor to an OTP solution.

Behavioural biometrics – GDPR considerations

6.9 The use of behavioural biometrics as an SCA factor and any circumstantial evidence used for the purpose of 'layering' will require careful consideration to combat other challenges, particularly GDPR. UK Finance through its SCA PMO is leading discussions around the application of GDPR to behavioural biometrics in the context of SCA.

EBA Guidance

6.10 The table below, which is identical to the EBA's in the June 2019 EBA Opinion, sets out a non-exhaustive list of possible inherence elements

Element	**Compliant with SCA?*** *Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes

[10] Paragraph 18, June 2019 EBA Opinion
[11] Paragraph 18, June 2019 EBA Opinion

Heart rate or other body moment patter identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

6.11 In UK Finance's view, the following are also possible inherence elements.

Element	**Compliant with SCA?*** *Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements
Behavioural biometrics identifying a specific user	Yes

7. Other requirements

Independence of the elements

7.1 PSPs must ensure that a breach of one of the elements of knowledge, possession or inherence does not compromise the other elements e.g. if accessed through a single device.

7.2 PSD2 provides that payment service providers therefore need to devise an authentication method that uses two separate elements overall, from two different categories, for instance one element categorised as knowledge (such as a password) and one as inherence (such as fingerprints)[12].

7.3 Independence of the elements constituting SCA does not require the use of different devices and the different elements can be carried out or hosted on the same device.

7.4 Firms take a different approach to managing this risk and it is not possible to develop an industry standard. For example, each firm will have a different approach to a customer using 'jailbroken' or 'rooted' mobile devices.

Authentication code and mechanisms

7.5 The RTS require that PSPs put in place arrangements to ensure that "*no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software delivered through the same channel*".

7.6 There are certain elements which will be outside of a PSP's control. For example, issuers separate out PINs, cards, card readers, and ensure that they are sent to the customer's address separately. They cannot, however, ensure that a third party does not collect all of these elements where the customer has left them unopened or failed to update their correspondence address when moving, for example.

7.7 Regarding online banking, as per the June 2018 EBA Opinion[13], the general position is that SCA has to be applied to access payment account information and to every subsequent payment initiation by the payer, including within a session in which SCA was performed to access the account data, unless an exemption under the RTS applies. However, in its June 2019 EBA Opinion, the EBA clarified that an element used for the purpose of SCA may be reused within the same session for the purpose of applying SCA at the time that a payment is initiated, provided that the other element required for SCA is carried out

[12] Paragraph 34, June 2018 EBA Opinion
[13] Paragraph 36, June 2018 EBA Opinion

at the time of the payment initiation and that the dynamic linking element is present and linked to that latter element.

7.8 Multipurpose devices such as mobile phones and tablets may be used for both initiating a transaction and authenticating the PSU, meaning the customer transaction can take place in the same user journey without the need to use a separate device.

Particular issues
• **Visibility to payer:** There is no requirement for the authentication code to be visible to the payer or for the payer to input it themselves: UK Finance's view is that the authentication code is typically generated by the PSP behind the scenes as a record of a successful SCA process and so is 'internal' to the PSP. The authentication code must also meet the requirements of Article 4, RTS.
• **Communications channel:** It is up to the PSP to decide whether the communications channel used to distribute customer authentication credentials is sufficiently secure and robust. Communication channels are vulnerable to interception and/or manipulation, and the requirement is for firms to have in place security solutions to mitigate such risks. However, some communication channels are more secure than others, therefore, good security practices should be followed as far as possible[14].

8. Dynamic Linking

8.1 This section gives further detail regarding dynamic linking.

What is dynamic linking?

8.2 PSD2 requires (Article 97(2)) that for electronic remote payment transactions, PSPs apply SCA that includes elements which dynamically link the transaction to a specific amount and a specific payee, explaining[15] that this is in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising.

8.3 The RTS add[16] that as electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the SCA of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction. Against this background and in addition to the requirement to apply SCA to the transaction, the RTS requires (see Article 5) that:

a) the payer is made aware of the amount of the payment transaction and of the payee;

b) the authentication code generated for an authenticated transaction is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the payment transaction;

c) the authentication code accepted by the PSP corresponds to the original specific amount and the identity of the payee; and

d) any change to the amount or the payee results in the invalidation of the authentication code generated.

To which payment transactions does dynamic linking apply?

8.4 Dynamic linking is a specific additional requirement of SCA which applies only to the initiation of electronic remote payment transactions. Examples of such transactions include when a user is initiating a funds

[14] National Institute for Standards and Technology (NIST) https://pages.nist.gov/800-63-3/sp800-63b.html
[15] Recital 95, PSD2
[16] Recital 3, PSD2

transfer through their banking app or a card-based payment on a merchant's website. This requirement would not apply to credit transfers performed at ATMs, given those transactions are not remote.[17]

What are examples of dynamic linking?

8.5 Dynamic linking refers to the additional aspects of the authentication of a payment transaction which links the transaction to a specific amount and a specific payee and mitigates the risk of 'man in the middle' attacks. For clarity, examples of dynamic linking include when authentication codes are generated and validated based on authentication solutions such as one-time passwords (OTPs), digital signatures and other cryptographically underpinned validity assertions using keys or cryptographic material, all of which are transaction-specific. In a cards context, the authentication code can include cryptograms which represent the digital signature of the transaction. There is no specific requirement for the authentication codes generated through dynamic linking to be visible to or shared with payers, however it must meet the requirements of Article 4, RTS.

8.6 To remain technologically neutral the RTS does not require the use of a specific technology for the generation of authentication codes and dynamic linking.

Does dynamic linking apply in all scenarios?

8.7 Article 5(3) of the RTS recognises certain scenarios where the application of dynamic linking may be more challenging:

a) Banking context – the RTS recognises that where a payer is authenticating, remotely and electronically, a batch of payment transactions, the authentication code can be generated by reference to the total amount of the batch (not by reference to each individual amount and each individual payee within the batch).

b) Card-based payment transactions – the RTS also recognises that a card may be used to block funds. In this case, the authentication code must be specific to the amount the customer gave consent to be blocked, within 'reasonable expectations'. This is because PSD2 (Article 76(1)) grants a payer the right to a refund where the authorisation does not specify the exact amount of the payment transaction and the amount debited exceeds the amount the payer could reasonably have expected. This indicates that there are circumstances in which the amount of a payment transaction may be varied, though it must always be within the reasonable expectations of the payer. In these circumstances, the payee will typically take authorisation for a specific amount (and the dynamic linking requirements will apply to that authorisation), but the payer is aware that the actual amount which may be processed could be higher or lower than this amount. UK Finance's view is that this practice is not precluded by these SCA requirements.

8.8 UK Finance notes that SCA applies to the initiation of a payment transaction and evidences the payer's consent, and that initiation of a payment transaction should be distinguished from the processing stages of such a transaction which happen subsequent to authentication by the payer (referred to in a cards context as 'authorisation' and 'submission'). These are separate from and subsequent to such authentication and accordingly the SCA and additional dynamic linking requirements do not apply to this subsequent processing. In light of this, UK Finance has set out below its view on how the dynamic linking requirements apply in numerous other challenging scenarios.

Delays between authentication and subsequent processing

8.9 If there is a delay between payment authentication and subsequent processing (authorisation and submission) during which time a 'dynamically linked' authentication code may expire, so long as it was correctly applied at the time of authentication, this would not invalidate the authentication code generated earlier.

Final amount of transaction is unknown at the time of authentication or changes for legitimate reasons

[17] Paragraph 37, June 2019 EBA Opinion

8.10 UK Finance's view is that for remote card transactions, there are legitimate cases where the final amount may be higher or lower than the amount authenticated by the customer, if both of the following conditions are met:

a) prior to the initiation of the payment transaction, the customer is aware that the final amount may increase or decrease after authentication and agrees to the card transaction on that basis; and

b) in case of an increase, this does not exceed the customer's 'reasonable expectations' within the meaning of Article 76(1), PSD2.

8.11 In arriving at this view, UK Finance notes that the primary objective of authentication is to address fraud and in the context of card-based payment transactions this approach does not detract from the payer's consumer protection rights under PSD2.

8.12 In many scenarios, the final amount of the transaction is determined only after the transaction is authenticated. This may take place hours, days or (in some limited or legitimate cases) weeks after authentication. This is the case for a significant number of use cases, including for online grocery shopping, travel and hospitality, for shipping and miscellaneous charges.

8.13 For example:

a) Online grocery shopping – here, the customer authenticates for a provisional amount and agrees to the final amount varying on the basis of the actual costs of weighed goods or substitutions. The customer may also agree to additions to their basket or replacement of out-of-stock products. Requiring the customer to authenticate for a second time when the final amount is determined would create serious inconveniences for customers (who will no longer be 'in session') and increased costs for merchants.

b) Split shipments - here, a customer purchases multiple items from a merchant in a single transaction. The total amount is authenticated but the different items are shipped as and when they become available, and separate multiple payments are taken at different times.

8.14 As such, UK Finance's view is that a payer's authorisation can provide consent for the actual payment transaction to be higher or lower than the amount authenticated (and that the subsequent change in amount does not invalidate the original authentication code) so long as it is within the payer's reasonable expectations and takes into account the relevant circumstances.

8.15 This is also consistent with the approach taken by the RTS for pre-authorisations, whereby a decrease in amount does not invalidate the authentication code and does not require a second authentication (Article 5(3), RTS). Although this provision applies to pre-authorisations for which funds are blocked, we believe the same principle (i.e. the authorised amount may differ from the authenticated amount) should apply for transactions where funds are not blocked. This shows that if the customer has already authenticated with SCA a transaction for which the final amount is unknown, this final amount may be different from the authenticated amount.

8.16 In arriving at this view, UK Finance notes that the primary objective of authentication is to address fraud and in the context of card-based payment transactions this approach does not detract from the payer's consumer protection rights under PSD2: if prior to initiation of the payment transaction, the customer is aware that the final amount may vary (within a certain limit) after authentication and agrees to the card transaction on that basis, and in the event of an increase of amount, this increase is within the customer's reasonable expectations (as previously agreed), a second authentication is not needed from a consumer rights perspective.

8.17 Multiple payments, as in the case of split payments, should similarly be permitted in the same way as batch payments are, as the payer will have consented to and authenticated the total amount (rather than the individual payments).

Higher final amount permitted

8.18 UK Finance also notes that this view, specifically that the final amount may be a higher amount, may not be consistent with the EBA's view as expressed in its EBA Single Rulebook: Q&A 2020_5133 published

on 29 May 2020[18] and the view adopted elsewhere in Europe. UK Finance's view, shared by the UK industry, is that this approach is justified: the EBA's response in this Q&A can be read so as to support the UK's view and furthermore the UK's pragmatic view avoids the alternative approach which would preclude such higher amounts and so would result in poor customer experience, added friction in the customer journey, and added complications.[19] Furthermore, the UK's approach only impacts UK issuers and cardholders, is consistent with concepts used elsewhere in PSD2 (based on the payer's awareness that the final amount could be higher and their agreement to proceed with a particular card transaction on that basis), and does not limit or exclude any of the payer's rights under PSD2.

8.19 The UK approach reflects the view that there should be differentiation between where funds are blocked and not blocked, with more latitude in the latter case. Accordingly, there are three core scenarios, as shown in the table below:

- Where the exact amount is known in advance, the final amount must be the same.
- Where the payer's PSP blocks funds on the payer's payment account – the payer must have given consent to the exact amount of the funds to be blocked: this can be a maximum amount, with the final amount being equal to or lower than (but not exceeding) this amount.
- Where the exact amount is not known in advance and the funds are not blocked by the payer's PSP - the final amount could be higher than the amount authenticated, so long as the payer was made aware of and agreed to this when initiating the transaction (i.e. at the point of authentication), so SCA would only need to be re-applied if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction.

Scenarios – Exact amount not known in advance and …	**Final amount of the transaction is lower or equal to amount agreed at authentication**	**Final amount of the transaction is higher than the amount agreed at authentication**
Payer's PSP block funds	No need to re-apply SCA	PSP should apply SCA to the final amount of the transaction or decline it
Payer's PSP does not block funds	No need to re-apply SCA	No need to re-apply SCA if the cardholder was aware that the final amount could be higher and agreed to proceed on this basis

8.20 It is already common practice for a cardholder to be made aware of and agree to such fluctuations, as part of the customer journey, check-out process or at point of sale, particularly within online grocery shopping and where there is currency conversion/exchange. In this context, UK Finance notes that the card schemes operate on the principle of allowing tolerances up to 15% or 20% above the initial amount authenticated (5% for technical differences such as currency conversion), with a liability shift to the retailer above these tolerances through the chargeback process. Accordingly, UK Finance's view is that each actor has a role to play in ensuring that the execution of transactions whose final amount may be higher is not abused, as shown in the table below.

[18] EBA Single Rulebook Q&A: 2020_5133

[19] If the final amount cannot be higher, then the following three options would be available when the exact amount is not known in advance, the funds are not blocked and the 'final' authorization amount is higher than 'initial' authentication amount: (1) a single Merchant Initiated Transaction (MIT) is used for the full payment amount – an MIT is excluded from SCA, though SCA is required on cardholder set-up, liability with merchant; (2) split payments are used, with: (i) first a regular payment for expected amount (SCA required for the expected amount with liability shift unless an exemption applies), if needed followed by (ii) a second payment for the incremental amount (no SCA either in reliance upon an exemption or as an MIT, liability shift with MIT and possibly exemption) – this would necessitate as part of the single transaction both SCA for payment and for the subsequent MIT set-up; or (3) regular SCA is applied for the expected amount plus margin for the incremental amount (like pre-authorization, but with no blocking of funds).

Actor	Role to Play
Merchant	Ensuring the payer's awareness that the amount may vary, within the customer journey, check-out process or at point of sale, and securing the payer's agreement on that basis.
Acquirer	Monitoring the merchant's behaviour (including through chargebacks), sharing best practice
Scheme	Providing the ability for Issuers to chargeback transactions if tolerances are exceeded
Issuer	Assuming no exemption, accepting SCA applied on authentication and in particular the authentication code generated, with no need to re-apply SCA on authorisation nor to match initial and final amounts. Dealing with any payer claims arising from variations in amounts in accordance with payer's rights under PSD2.

8.21 If a difference in approach towards higher amounts does emerge between the UK and the EU, then this will mean that UK merchants selling to customers with EEA issued cards could well experience declines if the authorisation amount is higher than the initial amount authenticated; similarly, UK cardholders buying from EEA merchants may experience a different approach with respect to higher amounts and issuers with both UK and EEA books may need to apply differentiated approaches.

Changes to the payee's name

8.22 The RTS requires that the authentication code is linked to both an amount and a payee agreed by the payer. In our view, a 'payee' does not need to be the merchant's legal entity name but can be a trading name, provided it is clear to the customer. In other words, the customer understands, and consents to, who they are intending to pay. Similarly, a payee's name can also be represented by a unique identifier, again, if it is clear to the customer who they are intending to pay.[20]

8.23 In UK Finance's view, a change in name should also be acceptable, so long as it is within the payer's reasonable expectations; a trade name to a legal name is clearly acceptable. In the same way, changes which take place during subsequent processing (after authentication) to the merchant's name, e.g. to its MID (merchant ID) and further to a specific store, should not of themselves invalidate the authentication code. However, UK Finance does note that any subsequent change to any of the inputs to the authentication code generated during a dynamically-linked SCA transaction would give the payer a right to challenge/repudiate the transaction. Therefore, PSPs should be careful in choosing the inputs of the authentication code, so that these do not have to change during subsequent processing.

8.24 In an e-commerce and marketplace context, there may be a change from the intermediary to the underlying merchant (e.g. when booking a hotel through an intermediary marketplace, the payer will confirm a payment to the marketplace, but in the payer's statement, the transaction will show the payee as the relevant hotel). Clearly this should be acceptable and such changes should not invalidate the payer's authentication; the payer's (user) experience should reflect this, provide transparency and not preclude the payer's rights (but these are matters outside of the scope of PSD2 and the RTS).

9. Exemptions to the requirement to apply SCA

9.1 The RTS specify the exemptions to the application of SCA in accordance with the Article 98(1)(b) PSD2. The RTS exemptions are based on the following broad criteria set out in Article 98(3): *"(a) the level of risk*

[20] EBA Single Rulebook Q&A: 2019_4556

involved in the service provided; (b) the amount, the recurrence of the transaction, or both; (c) the payment channel used for the execution of the transaction."

9.2 This section of the Guidance considers the exemptions to SCA as set out in the RTS provisions and, where relevant, the EBA Opinions.

9.3 Exemptions will be applied by the payer's PSP (ASPSP) where required. A number of exemptions can only be applied by an authorised or registered PSP. The term 'PSP' includes issuers, acquirers or other authorised parties (as defined under PSD2) in the payment chain.

9.4 Merchants cannot apply SCA exemptions in their own right.

9.5 The table below, which is identical to the EBA's table in its June 2018 EBA Opinion, outlines the basis for the SCA exemption (RTS reference Article), the exemption and who can apply (or request) the exemption.

RTS Article	**Exemption**	**Payer's PSP**	**Payee's PSP**	
			Credit transfers	**Cards**
Article 10	Access to payment account information	Yes	N/A	
Article 11	Contactless payments at POS	Yes	No	Yes*
Article 12	Unattended terminals for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payment processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether or not to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction if technically feasible or decline the initiation of the transaction

9.6 PSD2 and the RTS are worded to imply that firms can choose whether to exercise these exemptions or not based on their own assessment of the risk associated with a payment transaction i.e. a firm can apply SCA in all cases if it decides to.

9.7 Only one exemption type can be applied for any given transaction, even if the given transaction could qualify for more than one exemption types. This means that for Articles 11 or 16, for example, the limit of

five consecutive transactions needs to be calculated not on the basis of all transactions where the exemption could have been applied but on the basis of transactions where the particular exemption was applied.

9.8 PSPs that make use of any of the exemptions are allowed at any time to choose to step up and apply SCA, as per recital 17 of the RTS.

10. Access to Payment Account Information (Article 10)

10.1 Article 10 of the RTS is self-explanatory, however we have covered here for completeness. Article 10 of the RTS provides as follows:

"1. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article and, where a payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:

(a) the balance of one or more designated payment accounts;

(b) the payment transactions executed in the last 90 days through one or more

designated payment accounts.

2. For the purpose of paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication where either of the following condition is met:

(a) the payment service user is accessing online the information specified in paragraph 1 for the first time;

(b) more than 90 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1(b) and strong customer authentication was applied."]

SCA is not required where the PSU's access is limited (without disclosure of sensitive payment data) to checking the balance or payment transactions executed in the last 90 days. This exemption does not apply the first time the PSU accesses the information online, or where more than 90 days have elapsed since the PSU last accessed their last 90 days of transaction history online.

10.2 In respect of AISPs, the June 2018 EBA Opinion states that the 90-day period is specific to each AISP and is also separate to the 90-day period that applies to direct access by the user (meaning SCA needs to be applied separately to the different types of access).

10.3 The June 2018 EBA Opinion also states that the application of SCA for the purpose of the user making a payment directly or via a PISP will not re-start the 90-day counter for the purpose of the Article 10 exemption.

11. Contactless Payments at Point of Sale (POS) (Article 11)

11.1 Article 11 of the RTS provides as follows:

"Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 [General authentication requirements]*, where the payer initiates a contactless electronic payment transaction provided that the following conditions are met:*

(a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50; and

(b) the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed EUR 150; or

(c) the number of consecutive contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five."

11.2 The conditions to apply the contactless exemption are therefore twofold: (a) the amount of the transaction must not exceed EUR50/GBP45; and (b) the transaction must not result in the relevant cumulative limit since the last application of SCA being exceeded, where this limit is based on the monetary amount (EUR150/GBP130) or the number of consecutive transactions (five) (but not both), in either case determined at payment instrument level.

11.3 In order to benefit from this exemption, all contactless payments must be included in a card-based PSP's counter (whether value or volume based) for the relevant contactless device. Typically, an initial activation transaction with SCA will be executed before a contactless transaction without SCA may be undertaken, however, this is not a requirement of the RTS.

11.4 UK Finance is of the view that providers do not have to have both a means of counting volume and value of consecutive transactions. This is especially as the June 2018 EBA Opinion states "*in many situations the provider will not be able to identify a cumulative amount*", thereby recognising that it will not always be possible to have a volume and value count.

11.5 In the UK, most contactless cards do not rely on counts of numbers of transactions but use cumulative value counts to manage risk on domestic transactions. Counters on the number of transactions are used to manage risk on international transactions. In our view, the EBA Opinions do not require a change to this position.

11.6 For mobile contactless payments, in most cases, each transaction is subject to SCA by virtue of the use of the Cardholder Device CVM (e.g. Touch ID). This applies equally to a card based and credit transfer-based transactions as, e.g., Touch ID coupling possession and inherence can meet the requirements of SCA.

11.7 The cumulative limit is either the limit based on the number of transactions or the monetary amount (but not both). This means that it may be preferable for PSPs to decide at the outset which cumulative limit they use (rather than on a transaction-by-transaction basis), though the EBA has clarified[21] a transaction-by-transaction approach is also permitted, provided PSPs are able simultaneously to check whether either of the volume or value limits have been reached and to apply SCA as soon as one or both of the limits are exceeded.

11.8 UK Finance's view is that contactless limits should be applied at device/token level rather than account level[22], meaning that the limits are applied to each contactless instrument used by a payer (e.g. contactless card, mobile, etc.) with respect to the same payment account. If the limits were to be managed at the account level, this would not adequately take into account that the same payment card can be used as a plastic card or it can be registered in one or more digital/mobile wallet(s) and/or devices (e.g. smartwatches and wristbands). The application of the limits at account level implies that performing SCA on any device would reset the counter/accumulator. This would have the effect of allowing lost or stolen devices to be used if the owner is not aware of the loss and continues to use other devices and perform SCA.

11.9 Issuers should make their own risk assessment to decide how the cumulative counters (value or volume) will be managed (via the card chip versus host/back office systems). If the issuer decides to manage the counters via the chip, it is UK Finance's view that all cards in issue should be allowed to run to their end date, ready for natural reissuance; put another way, cards existing as at September 2019 which may not have these controls attached to them (e.g. the aggregate limit) should be capable of continuing to be used without SCA (e.g. beyond the aggregate limit) until their expiry (effectively providing for a run-off period after September 2019). If the issuer's approach is to comply by managing the counters via the host/back office, the issuer could still choose in the future to issue cards with these controls attached to them.

11.10 Similarly, payment terminals (POS) will also need updating. UK Finance also believe that this should be subject to natural replacement dates allowing for a run-off period after September 2019.

[21] EBA Single Rulebook Q&A: 2018_4182
[22] This view is confirmed by EBA Single Rulebook Q&A: 2018_4036

11.11 The EBA has confirmed[23] that when the cumulative monetary amount or the maximum number of transactions without SCA is reached, the limit will be reset at the next non-remote payment transaction, contactless or not, where SCA is applied. This means that the counter could be reset either at a point of sale or an ATM transaction. The application of SCA for a remote transaction would not reset this limit.

12. Transport and parking (Article 12)

12.1 Unattended terminals for transport fares (at transport gates) and parking fees are exempted from the requirement to apply SCA. In these cases, it is not feasible to apply SCA. Article 12 of the RTS provides as follows:

a. *"Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2* [General authentication requirements]*, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee."*

12.2 Article 12 exempts from SCA all transactions at unattended terminals for electronic payment transactions for the purpose of paying a transport fare or a parking fee. If an unattended terminal enables contactless payments, the PSP can choose to apply the Article 12 exemption so that the limits referred to in the context of the Article 11 contactless exemption do not include payments initiated under this exemption. In other words, the transport and parking exemption takes precedence over the contactless exemption in order to avoid poor customer experience.

13. Trusted beneficiaries (Article 13)

13.1 Article 13 covers a list of trusted beneficiaries, whereby payments to these beneficiaries do not need to have SCA applied. This is often called 'whitelisting'. Article 13 of the RTS provides as follows:

> *"1. Payment service providers shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider.*
>
> *2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer."*

13.2 A payer can create a list of trusted beneficiaries, or 'white list', held by the payer's PSP or ASPSP on the PSU's account. When a payer creates or amends this list, SCA must be applied. For future transactions to those on the list, SCA need not be applied at the discretion of the payer's PSP or ASPSP. As per the June 2018 EBA Opinion whitelisting is not limited to credit transfers and may apply to cards through the payer's PSP, upon the payer's confirmation. The payee's PSP cannot apply this exemption, and a payee could not have such a list for the purpose of the exemption (e.g. cards on file).

13.3 It is clear that retailers would not be able to manage this same list of trusted beneficiaries. In other words, retailers cannot whitelist themselves without involving the ASPSP/issuer.

13.4 Credit transfers are in scope; however, it is down to the ASPSP to manage the process of creating or amending the list of trusted beneficiaries.

13.5 Card payments are in scope; however, it is down to the issuer to manage the process of creating or amending the list of trusted beneficiaries.

13.6 UK Finance's view is that an 'amendment' in this context includes, for example, the addition of a new payee to the list of trusted beneficiaries or any changes to the details of an existing trusted beneficiary,

[23] EBA Single Rulebook Q&A: 2018_4226

but that it would not include the removal of a payee from the list of trusted beneficiaries (there is no fraud risk associated with such a removal). For clarity, if a PSU wished to re-add a payee to the list of trusted beneficiaries (having previously removed that payee from the list), SCA would need to be applied.

13.7 As per the June 2018 EBA Opinion, PISPs are not able to create a generic list of trusted beneficiaries.

13.8 For existing lists of trusted beneficiaries (i.e. those created before 14 September 2019), there is no requirement to apply SCA to reconfirm these with customers, nor is there a requirement to re-create the list: SCA should be required only where there is an amendment to the list of trusted beneficiaries.[24] Additionally, application of the exemption is not limited to remote transactions.[25]

13.9 Trusted beneficiaries added to the list held by the ASPSP requested via telephone or fax are considered outside of the scope of the RTS. However, UK Finance is of the view that conditions similar to the requirements to the RTS should, when appropriate, be applied in these circumstances to ensure the beneficiary is being added with sufficient certainty, especially when those beneficiaries are able to make payments via remote channels.

14. Recurring transactions (Article 14)

14.1 Article 14 of the RTS provides as follows:

> *"1. Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee.*
>
> *2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred to in paragraph 1."*

14.2 The RTS provides an exemption for recurring transactions which are defined as a series of payments of the same amount made to the same payee. Recurring transactions as defined by the RTS in the context of this exemption are distinct from (out of scope) payee-initiated transactions. UK Finance considers that these recurring transactions are initiated by the payer's PSP on behalf of the payer (for example a standing order) whereas payee-initiated transactions are initiated by the payee only.

14.3 A PSP must apply SCA when a payer creates, amends or initiates for the first time, a series of recurring transactions; any future transactions to that payee for the same amount can be exempted.

14.4 As explained above, PSPs do not need to rely upon the recurring transactions exemption for Direct Debits or card payments which are payee-initiated and rely upon a pre-existing authority given by the payer to the payee, with the transaction taking place without the direct intervention of the payer.

15. Credit transfers between accounts held by the same natural or legal person (Article 15)

15.1 Article 15 of the RTS is self-explanatory, however we have covered here for completeness. Article 15 of the RTS provides as follows:

> *"Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2* [General authentication requirements]*, where the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider."*

[24] EBA Single Rulebook Q&A: 2018_4120
[25] EBA Single Rulebook Q&A: 2018_4056

16. Low value remote payments (Article 16)

16.1 Article 16 of the RTS provides as follows:

> *"Payment service providers shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction provided that the following conditions are met:*
>
> *(a) the amount of the remote electronic payment transaction does not exceed EUR 30; and*
>
> *(b) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not, exceed EUR 100; or*
>
> *(c) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed 5 consecutive individual remote electronic payment transactions."*

16.2 The conditions to apply the low value transaction exemption are therefore twofold: (a) the amount of the transaction must not exceed EUR30/GBP30; and (b) the transaction must not result in the relevant cumulative limit since the last application of SCA being exceeded, where this limit is based on the monetary amount (EUR100/GBP90) or the number of consecutive transactions (five) (but not both)[26], in either case determined at payment instrument level. The EBA suggests that PSPs should decide and inform customers at the outset which cumulative limit (or counter) they intend to use.

16.3 Either the issuer or acquirer can apply the exemption for low value transactions: the EBA confirmed this in the June 2018 EBA Opinion[27]. The EBA also confirmed however that the payer's PSP (i.e. the issuer) will always have the ultimate decision on whether or not to accept or apply an exemption. So, if an acquirer applies a low value transaction exemption flag, the issuer could decide to 'step-up' the transaction and require SCA. The issuer should also 'step-up' the transaction if the relevant limit has been reached.

16.4 From a regulatory perspective, it is necessary to determine which of the two parties has the regulatory liability for a fraudulent transaction. This goes not only to the PSP's regulatory compliance but also affects the PSP's calculation of its fraud rates for the purposes of making use of the TRA exemption under Article 18 of the RTS (as it is the PSP that bears liability for the fraud which must include it in their TRA exemption fraud rate calculation).

16.5 In practice, however, whilst both the issuer and the acquirer will be aware of the transaction amount in respect of any given remote electronic card-based payment transaction, the issuer will be in control of which cumulative limit (i.e. monetary amount or number of consecutive transactions) is being applied and whether such cumulative limit has been reached such that SCA need be applied. Put another way, although the acquirer can opt to flag a transaction as 'low value', the acquirer does not have any visibility over which cumulative limit is being applied or whether a particular transaction will cause such limit to be exceeded. The issuer must always check these limits irrespective of the flag applied by the acquirer.

16.6 With the operation of these limits (or counters), the liability framework in respect of the low value transaction (LVT) exemption is complicated to disentangle. UK Finance is of the view that the liability structure can be summarised in the table below.[28]

Scenario	**Who's liable? Whose TRA? Acquirer or Issuer**
Acquirer applies LVT exemption flag or requests low value exemption; Issuer accepts (i.e. issuer does not step up and apply SCA)	Acquirer Note this is the case notwithstanding that the particular

[26] Paragraph 43, June 2018 EBA Opinion

[27] Paragraph 40, June 2018 EBA Opinion. See also EBA Single Rulebook Q&A: 2018_4242, in which the EBA clarified that this is because Article 16 refers broadly to PSPs and does not restrict the application of the exemption to the payer's PSP.

[28] The liability position set out in the table is for the purposes of the PSP's calculation of its fraud rates in relation to the TRA exemption under Article 18 of the RTS.

	transaction may have resulted in the relevant cumulative limit (value or volume) being exceeded[29]
Acquirer applies LVT exemption flag; Issuer steps up (either because the relevant limit or counter has been reached or on a risk basis it decides to apply SCA to the particular transaction)	Issuer
Acquirer does not apply LVT exemption flag nor request low value exemption; Issuer applies low value exemption	Issuer

17. Secure corporate payment processes and protocols (Article 17)

17.1 Article 17 of the RTS provides as follows:

"Payment service providers shall be allowed not to apply strong customer authentication, in respect of legal persons initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by Directive 2015/2366 [PSD2]*."*

17.2 UK Finance agrees with the FCA's interpretation that the exemption may only be applied where the payer using the dedicated payment processes or protocols is a legal person. This means the payer must be a body corporate, which would include companies and limited liability partnerships.

17.3 It is also our view that the term 'dedicated payment processes or protocols' refers to payment processes and the exchange or transmission of data between devices carried out within closed networks or access-controlled environments. Examples include the use of proprietary automated host-to-host (machine-to-machine) restricted networks, and lodged or virtual cards, such as those used within the corporate travel management industry.

17.4 PSPs that make use of this exemption are required to notify the FCA through existing notifications under their assessments under operation and security risks. This assessment includes demonstrating that where payments are initiated through the use of dedicated payment processes and protocols, their fraud rate, as monitored at least on a quarterly basis, is below that recorded for equivalent payment transactions made via channels where strong customer authentication is applied.

18. Transaction risk analysis

18.1 Article 18 of the RTS provides as follows:

"1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

[29] The liability position stated here is based on the expected contractual position under the scheme rules, which in turn is based on the fact that the acquirer has no visibility of the relevant limit (or counter). Under the regulatory framework, the issuer will be in contravention of the requirement to apply SCA where the relevant limit (or counter) has been exceeded because in these circumstances, notwithstanding the LVT exemption flag applied by the acquirer, the issuer should have stepped up the transaction and applied SCA. Where this is the case, e.g. a 6th transaction executed without SCA, the issuer may decide not to pass on liability to the acquirer even if the acquirer applied an LVT exemption flag or requested low value exemption.

2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

(a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for 'remote electronic card-based payments' and 'remote electronic credit transfers' respectively;

(b) the amount of the transaction does not exceed the relevant Exemption Threshold Value ('ETV') specified in the table set out in the Annex;

(c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

(i) abnormal spending or behavioural pattern of the payer;

(ii) unusual information about the payer's device/software access;

(iii) malware infection in any session of the authentication procedure;

(iv) known fraud scenario in the provision of payment services;

(v) abnormal location of the payer;

(vi) high risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

(a) the previous spending patterns of the individual payment service user;

(b) the payment transaction history of each of the payment service provider's payment service users;

(c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

(d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication."

	Reference fraud rate (%) for:	
ETV	Remote electronic card-based payments	Remote electronic credit transfers
EUR500/GBP430	0.01	0.005
EUR250/GBP215	0.06	0.01
EUR100/GBP90	0.13	0.015

18.2 Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for a remote transaction provided the applied risk analysis does not identify any risks if the PSP's observed fraud rates fall below certain thresholds (Article 18 of the RTS) and the amount of the payment transaction does not exceed EUR500/GBP430.

18.3 UK Finance through its SCA PMO is leading discussions around the detailed implementation of the TRA exemption.

19. Resilience in e-commerce card transactions

19.1 Under PSD2, there is a legal requirement on PSPs to apply SCA in the scenarios defined in Article 97(1), PSD2. For e-commerce card transactions, the common industry practice[30] to facilitate SCA is 3DSecure (3DS[31]). This technology is also required in order to facilitate the use of certain SCA exemptions and the establishment of certain out of scope transactions when SCA may be needed.

19.2 This has exposed a key reliance on the availability of the 3DS protocol: unless the merchant can leverage an exemption, they are reliant on authentication via 3DS to complete a transaction for all remote card payments. Put another way, if the merchant does not access 3DS or if it cannot reach the 3DS service, it is highly likely that the issuer will decline the transaction, unless the issuer can rely on applying issuer exemptions. Often the value of the transaction available for exemption is capped by the thresholds specified by the RTS.

19.3 In light of this, UK Finance has identified three scenarios in which issuers would not be able to apply SCA in respect of e-commerce card transactions and for which a resilience framework is recommended in order to minimise negative customer outcomes, i.e. where:

a) the Access Control Server (ACS) is unavailable;

b) the merchant cannot access the 3DS service due to a 'merchant problem' (e.g. because there is a gateway failure or a network issue); or

c) the merchant cannot access the 3DS service due to a 'major outage' (e.g. because a card scheme is unable to support authentication of e-commerce card transactions).

19.4 UK Finance's recommended resilience framework in each of the scenarios is set out in more detail below. It should be noted that the framework is only applicable for the limited scope and scenarios, as described below, seeking to apply the principle of proportionality to regularise and strengthen existing practice designed to achieve business continuity. The framework should be applied only in respect of 'standard' e-commerce card transactions: UK Finance would not, for example, recommend it is used to set up a new card on file or recurring transaction given the additional fraud risk associated with these types of actions.

19.5 The resilience framework is designed for use in extraordinary circumstances after merchants and gateways have exhausted all other options prescribed by the RTS to comply with the SCA requirements. In addition, it does not change existing practices: when leveraging the resilience framework, PSPs (and other parties) should continue with the robust fraud screening and transaction and risk monitoring, as required by PSD2 and the RTS, so that transactions sent using the resilience framework are protected against fraud. Alongside this, the framework provides for various tiers of controls to ensure it is applied appropriately by all players.

Access Control Server (ACS) is unavailable

19.6 Where the Access Control Server is unavailable, UK Finance recommends the continued use of the schemes' Authentication Stand-In protocol[32] for the issuer to assess the transaction and decide on a risk-based approach whether to approve or decline the transaction.

19.7 Use of the Authentication Stand-In protocol means the issuer knows that there has been a genuine attempt by the merchant to authenticate the customer because of the presence of the ECI code and cryptogram which is sent to the issuer by the merchant.

19.8 Liability for such transactions will remain with the issuer.

[30] There are other SCA compliant solutions available in the market, such as those provided by Payment Initiation Service Providers (e.g. through Open Banking), Apple Pay or Google Pay as well as other potential solutions.

[31] EMV Three-Domain Secure (3DS) is a messaging protocol developed by EMVCo to enable consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorised CNP transactions and protects the merchant from CNP exposure to fraud. The three domains consist of the merchant/acquirer domain, issuer domain, and the interoperability domain (e.g. Payment Systems).

[32] This assumes normal authorisation processing is in effect, including issuer stand-in limits for approval.

Merchant problem or major outage

19.9 Where the merchant cannot access the 3DS service due either to a 'merchant problem' or 'major outage', UK Finance recommends the use by the merchant or gateway of a resilience code in the authorisation message (this flag will indicate to the issuer that the merchant was unable to authenticate the customer due to a technical issue), for the issuer to assess the transaction and decide on a risk-based approach whether to approve or decline the transaction with the value of the transaction not a limiting factor preventing the approval of the transaction.

19.10 Use of the resilience code means the issuer knows that there has been a genuine attempt by the merchant to authenticate the customer but that there was an issue preventing this.

19.11 If the use of the resilience code is due to a merchant problem, liability for the transaction will remain with the merchant.

19.12 If the use of the resilience code is due to a major outage, liability for the transaction is to be agreed between the merchant and acquirer.

Monitoring and reporting

19.13 The resilience framework relies on existing multi-level controls including controls managed by issuers, acquirers and the scheme.

a) Issuers: UK Finance recommends that issuers continue to carry out real-time risk assessments of individual transactions and to decline transactions considered high risk according to those risk assessments.

b) Acquirers: Acquirers are expected to monitor merchant use of the resilience framework and to support merchant performance improvement plans when performance management thresholds are exceeded.

c) Scheme: Scheme rules will set out further detail and standardise implementation and use of the resilience framework, with monitoring of merchant usage through acquirers.

19.14 UK Finance's view is that reporting in respect of use of the resilience framework should fall within existing regulatory reporting and notification requirements for PSPs, namely the REP017 Payments Fraud Report and the requirements in relation to major incident reporting under Article 95, PSD2 (Notification of Major Operational or Security Incidents).

20. Vulnerable customers

20.1 UK Finance recognises that there will be certain customers in relation to which the application of SCA will present a number of challenges. These include vulnerable customers, defined by the FCA as somebody who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.

20.2 UK Finance has set out below its views on how considerations vis-à-vis vulnerable customers should be applied with respect to two specific SCA-related matters. However, as a general principle, UK Finance's view is that where, having exhausted all of its existing solutions to apply SCA taking into account the customer's potential vulnerability, an issuer cannot physically apply SCA, then the issuer may apply one SCA factor where possible (to complete the transaction) or where this too is not possible, execute the particular electronic transaction or take the particular action nonetheless. It is expected, however, that the issuer will apply some fraud risk mitigation measures (i.e. risk-based assessments of individual transactions, declining high risk transactions) and monitor the level of fraud, adjusting its approach as necessary.

Chip and signature: Chip and paper-based signature is not an alternative to Chip & PIN for the purposes of SCA and should only be used for financial inclusion purposes for people who have difficulty remembering or typing in a PIN. This is required in order to allow for compliance with the Equality Act (to ensure customers with a disability are not discriminated against). Card terminals in shops are designed to automatically prompt shop staff to ask for a signature when one is needed.

UK Finance notes that the RTS do not provide for any exceptions and that all of the requirements are subject to audit under Article 2, however, it considers these to be good reasons for adopting a more flexible approach than the RTS expressly permits.

Session time out: UK Finance is of the view that there are circumstances where allowing longer than the 5 minutes time out required by Article 4(3)(d) could be reasonably justified in an online banking context: (a) vulnerable customers may need a longer session time, likewise others for financial inclusion purposes, and a longer time out period would be a reasonably adjustment under the Equality Act also; (b) corporate customers often require extended sessions to effectively manage and administer their corporate accounts; and (c) customers generally need sufficient time for customers to read longer documents such as terms and conditions. UK Finance notes that the RTS do not provide for any exceptions and that all of the requirements are subject to audit under Article 2, however considers these to be good reasons for adopting a more flexible approach than the RTS expressly permits.

1 October 2020