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 apply from 14 September 2019.

UK Finance is a trade association representing nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, based in the UK and overseas, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities, from our members. The interests of our members' customers are at the heart of our work.

This guidance is written and provided for general information purposes only and does not constitute legal advice. 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 Addleshaw Goddard LLP and Osborne Clarke LLP accept any liability to any third party in relation to the contents of this document. Any opinions expressed in this document are the opinions of UK Finance only and may not reflect the views or advice of Addleshaw Goddard LLP or Osborne Clarke LLP.

In due course, the European Banking Authority (EBA) PSD2 Q&A tool will provide further clarification on a number of issues raised in the guidance document. We also expect that national competent authorities, such as the Financial Conduct Authority (FCA) will provide further guidance.

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), 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 UK PSRs 2017 refer to "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*

[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*"

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 will apply from 14 September 2019.

1.3 The EBA has also published an opinion dated 13 June 2018 which aims to provide clarity on the implementation of certain aspects of the RTS (EBA Opinion).

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 Opinion. It then goes on to deal with the exemptions from the application of SCA.

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 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.

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.

- **What does strong customer authentication apply to?**

2.5 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 much broader than that of the 2014 EBA Guidelines on the Security of Internet Payments (which will be superseded by the RTS from 14 September 2019) 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.

2.6 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.

2.7 SCA should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse. The scope of this SCA requirement does not apply to all transactions and in addition, there are certain exemptions, further details of which are given below.

2.8 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, 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 are known as 'Merchant Initiated Transactions' or MITs)	These Direct Debit payments are initiated by the payee; 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; 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]. For clarity, Interactive Voice Response (IVR) mechanisms and voice commerce are generally treated as electronic transactions and therefore are in scope of strong customer authentication. UK Finance recognises there are no mechanisms to perform SCA for IVR transactions at present.
Telephone banking (e.g. paying a credit card bill via telephone conversation)	Out of scope as it is a telephone transaction.

[2] Please see EBA Feedback Table Q46

Paper-based transactions (e.g. fax)	Out of scope of PSD2 as it is a paper-based transaction.
Card payments where EEA cardholder is using their card outside of the EEA (one leg out)	As one of the PSPs is outside the EEA (acquirer), the 'best efforts' principle applies (please see "Geographic scope" below).
Card payments where non-EEA cardholder is using their non-EEA issued card in the UK/EEA	Out of scope (as non-EEA issuers are not in scope), so SCA does not apply.
Payments made through anonymous payment instruments	Due to their very nature, these transactions need to be out of scope[3].

- **Why are 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 is not in scope if given on paper. The EBA has expressly confirmed this position.

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.
- 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 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 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.

2.16 Direct Debit and certain card transactions can both be considered as a Merchant Initiated Transaction, provided the conditions for MIT are met.

- **When can exemptions be applied?**

2.17 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 summarised in the table below and are discussed in more detail further below.

2.18 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.

[3] Please see Recital 8 of the RTS

2.19 The PSP applying SCA will be the PSP 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[4].

2.20 In a cards context, the EBA has clarified in its 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.

2.21 The table below outlines the exemptions and how they work.

Exemption	**Description**
Access to payment account information (Article 10)	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.
Contactless payments at point of sale (Article 11)	SCA is not required for contactless transactions not exceeding €50, subject to certain value/volume counters (€150 or 5 transactions respectively) applied at a payment instrument level.
Unattended transport and parking fees (Article 12)	SCA is not required at unattended transport/parking terminals, e.g. transport gates, road tolls, car parking fee terminals. In these cases, application of SCA is not feasible.
Trusted beneficiaries (Article 13)	SCA is not required where the payee is on a list of 'trusted beneficiaries' managed through the payer's PSP/ASPSP. This is also known as 'whitelisting'. This exemption can be used in both a cards context and online banking context, so long as the whitelist is held by the issuer (meaning that a user may add a trusted merchant to a whitelist held by the issuer so that SCA is at the issuer's discretion). SCA will need to be applied when a beneficiary is first added to such a list, and when a beneficiary's details are amended.
Recurring transactions (Article 14)	SCA is not required if the transaction is one of a series of transactions made with the same payee and the same amount (subject to applying SCA when the payer creates, amends or initiates a series of transactions).
Credit transfers to self (Article 15)	SCA is not required when the PSU is sending a credit transfer to themselves and both sending and receiving accounts are held by the same ASPSP.
Low value transactions (Article 16)	SCA is not required for remote transactions not exceeding €30, subject to certain value/volume counters (€100 or 5 transactions respectively) applied at the payment account level.
Secure corporate payments (Article 17)	SCA is not required for payments initiated in respect of legal persons using dedicated payment processes or protocols that are limited to payers who are not consumers (e.g. host to host, some SWIFT services and some corporate card products).
Transaction Risk Analysis (Article 18)	SCA is not required where a PSP analyses the risk associated with a transaction and deems it to be low risk provided the PSP is operating within permitted reference fraud rates.

[4] Please see EBA Opinion Paragraph 38

3. Geographic scope

3.1 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. Similarly, when a payer initiates an electronic payment transaction or carries out any other action through a remote channel. There is a separate and broader section on geographic scope in other parts of the UK Finance industry guidance which should answer questions which are not addressed here.

3.2 In a cards context, however, the EBA recognises in its Opinion that there are natural geographical limits and states that where card payment transactions are initiated through a payee (merchant) outside of the EEA, the SCA requirement applies only on a 'best efforts' basis for such cross-border one leg out transactions. This is 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 (the card issuer knows where the payee merchant is located, but not where its PSP acquirer is located). In such cases, the EBA Opinion expresses the view that the liability regime stated by Article 74(2) PSD2 applies.

3.3 So in a cards context, SCA is only required to be applied where both the payer's PSP (issuer) and the payee's PSP (acquirer) are located in the EEA, i.e. for all intra-EEA transactions. Typically, the location of the merchant is the same as the acquirer at least within the EEA. European merchants must be acquired by EEA located acquirers (for both scheme and regulatory reasons). Where an EEA acquirer acts as payee's PSP for a merchant located outside of the 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 3D Secure or similar.

3.4 Where a UK cardholder is using their card abroad, outside of the EEA, the requirement to apply SCA does not apply (unless the non-EEA merchant is using an EEA based acquirer) and where a non-EEA cardholder is using their non-EEA issued card in the UK, the requirement to apply SCA also does not apply. In both such cases, the payment transactions concerned do not need to be included in the relevant PSP's calculation of its fraud rates[5].

4. Dynamic Linking

This section gives further detail regarding dynamic linking.

- **What is dynamic linking?**

4.1 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[6] 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.

4.2 The RTS add[7] 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, Article 5 of the RTS requires 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?**

4.3 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 transfer through their banking app or a card-based payment on a merchant's website.

---

[5] Please see EBA Feedback Table Q55
[6] Please see Recital 95 of the RTS
[7] Please see Recital 3 of the RTS

- **What are examples of dynamic linking?**

4.4 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 allows it to be 'tracked' through its journey. There are multiple ways that a PSP may choose to authenticate. 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.

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?**

4.5 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); and

(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 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.

4.6 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. So, for example changes during this subsequent processing 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 do note that any subsequent change to any of the inputs to the authentication code generated during a dynamically-linked SCA transaction would give the PSU 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.

4.7 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.

4.8 Examples of scenarios where the final amount is unknown or where the final amount or the payee may change for legitimate reasons include:

(a) Online grocery shopping – here, the customer may add items, or the merchant may substitute unavailable items with higher priced alternatives, after the transaction has been authenticated.

(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.

4.9 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. In a similar way, a payer's authorisation to block a certain amount of funds does not preclude that the actual payment transaction may be higher or lower. We further believe that this can apply in both a card and credit transfer context. 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.

4.10 UK Finance also notes that there are clearly scenarios – such as the grocery home shopping one – where all parties would wish to enable the transaction to be processed so long as the amount being authorised is within the tolerance (higher or lower value) reasonably expected by the PSU (online grocery shops have different approaches to such scenarios). 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).

4.11 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, it if is clear to the customer who they are intending to pay.

4.12 So a change in name should be acceptable, so long as it is within the payer's reasonable expectations; a trade name to a legal name is clearly acceptable. 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).

5. Requirements of the elements for SCA

5.1 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 (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.

5.2 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 focussing on innovating to ensure the best customer experience. We have therefore deliberately remained less specific in the cases listed below.

5.3 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.

6. Requirements of the elements categorised as knowledge

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

6.2 PSPs have to mitigate the risk of this element being accessed by unauthorised parties.

Guidance:

• A banking password is appropriate, but a user's ID or username is not.
• Static items are able to be used and are sufficient for the use of knowledge requirements, however, there are separate requirements for authentication elements and dynamic linking as part of SCA. Answer to Q22 in the EBA Analysis states*: 'The EBA believes that such prescriptive terminologies would undermine the objectives of technology neutrality and future proofing and has therefore decided to delete all the specific features, focusing purely on the outcome instead'*. This suggests that the RTS is ambivalent to whether the element is static or dynamic as long as risk mitigation is in place.
• If card number, expiry date and CVV are used (as an example) there needs to be a separate factor in addition. As per the EBA's Opinion these three static factors cannot be used as knowledge, UK Finance is of the view that provided sufficient behavioural characteristics have been taken into account and that sufficient risk mitigation is in place (as above), that card number, expiry date and CVV can be considered as knowledge provided there is a clearly separate factor in addition. This is referred to as a 'layered

approach' which considers multiple dynamic factors in addition to the static card details, such as behaviour factors taken into consideration alongside biometric (inherence) or possession authentication. UK Finance are of the view that static card credentials which utilise a 'layered approach' in addition to the use of a one-time passcode is sufficient for the requirements of SCA, provided that sufficient risk mitigation is put in place. A dynamic CVV also meets the requirements for knowledge.

7. Requirements of the elements categorised as possession

7.1 The authentication process can include an authentication element that is something only the user 'has'.

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

Guidance:

• The card number, expiry date and CVV are not sufficient by themselves to be considered as possession elements (because they can be recorded by an unauthorised party that has access to the card). However, card data can potentially be considered as a possession-based element provided they are tokenised[8] in a secure fashion and are used as part of a "layered approach" alongside Risk Based Authentication and other independent factors. For example, tokenised card credentials can be provisioned remotely on to a registered customer device and used as a possession-based authentication element for transactions that require SCA. • A dynamic CVV also meets the requirements for a possession-based authentication element.
• A card reader provided to the PSU or other token generator can be used to demonstrate possession.
• A random code generated or sent to a previously registered mobile device can be used to demonstrate continued possession. A mobile/other device should be linked securely with the payment service user (e.g. provisioning a card through a mobile app or device profiling). This applies equally in the context of credit transfers and card payments.
• Access to an IP address, on its own, is not an appropriate possession-based element even once linked to a card, card reader or device.

8. Requirements of the elements categorised as inherence

8.1 The authentication process can involve the payee offering something that they 'are'.

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

Guidance:

• Biometric credentials associated with a payment service user can be used as inherence, even when stored at device level, provided that the device is linked securely with the PSU and that unauthorised parties cannot receive access to stored biometric customer authentication data. In other words, a biometric on a device e.g. Touch ID on an iOS mobile phone, is can act as an inherence authentication element provided the PSP is sufficiently factoring in risks.

[8] Tokenisation is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token that has no extrinsic or exploitable meaning or value. Practically, the customer's primary account number (PAN) is replaced with a series of substitute numbers, which is called the "token." These tokens can then be passed through the internet or the various wireless networks needed to process the payment without any physical card or underlying payment account details being exposed.

- Behavioural biometrics can be used as an inherence element as outlined in the EBA Opinion on the implementation of the RTS. It is advisable that the customer's profile be established over time to improve accuracy/reduce false positives.

9. Independence of the elements

9.1 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.

9.2 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)[9].

9.3 Practically we are of the view that provided the ASPSP knows the user ID (e.g. registry through mobile banking) both a fingerprint (inherence) and holding of the registered PSU's phone (possession) can be considered as appropriate SCA elements.

9.4 Independence of the elements constituting SCA does not require the use of different devices and the different elements can be carried out on the same device[10].

9.5 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.

10. Authentication mechanisms

10.1 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*".

10.2 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.

10.3 Regarding online banking, as per the EBA's Opinion (Paragraph 36) 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. The table below gives further clarity on specific authentication mechanisms.

10.4 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.

- **Magnetic stripe**: Magnetic stripe cards are not compliant with SCA according to the EBA, even as a fall-back. Indeed, a magnetic stripe card (and an EMV Static Data Authentication (SDA) chip card) does not create an authentication code that can be used only once.[11]

  Magnetic stripe cards that are issued in non-EEA countries will still be permitted as there is the option that the payer's PSP cannot facilitate SCA).[12]

  In other words, for cards issued by the EEA PSP, the use of a magnetic strip and signature is <u>not</u> compliant with SCA and should not be used.

  UK Finance supports the EBA's view (stated in its February 2017 consultation – see Q272(1), below) that: "*where payment instruments issued under a national legal framework that does not require the use of SCA (such as magnetic stripe cards) are used within the EU or when the payment service provider of the*

[9] Please see Paragraph 34 of the EBA Opinion on implementation of the RTS
[10] Please see answer to question 10 in EBA's Analysis
[11] Please see answer to question 272 in EBA's Analysis
[12] Please see Answer to question 1 in EBA's Analysis

acquirer is established in a jurisdiction where it is not legally required to support the SCA procedure designed by the European issuing PSP, the European PSPs shall make every reasonable effort to determine the legitimate use of the payment instrument. As specified in paragraph 16 of the rationale, 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 under the new Article 16." (emphasis added).
• **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, we consider these to be good reasons for adopting a more flexible approach than the RTS expressly permits.
• **Session time out:** UK Finance are 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; (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.
• **One time passcodes:** We are of the view that SMS and email can be used for One Time Passcode (OTP) delivery and that PSPs should make their own assessment of the risks. This means that individual PSPs may decide that an SMS OTP satisfies the requirement for SCA, in particular when combined with additional security technology and processes (for example, SIM swap detection, device profiling, registration process, etc). Similarly, an OTP on a mobile app or an OTP delivered through a landline telephone could be used. However, there will be and are other solutions in the market. UK Finance recognises that there are risks in the delivery of one time passcodes and therefore encourage all PSPs to make a thorough assessment of how one time passcodes are delivered to customers.
• **Visibility to payer:** We are of the view that neither the authentication nor the authentication code needs to be visible to a payer. The EBA does not specify whether the authentication must be visible to the payer. Question 274[13] of EBA Analysis suggests: '*The RTS do not define the elements that should constitute the authentication code and therefore remain as technology neutral as possible. The payer's PSP needs to authenticate the payer to make sure that it is really the payer and thus gives its consent through something tangible.'* It is therefore assumed that the authentication itself and the authentication code can be invisible to the payer. Examples of this may include digital signatures, invisible tokens and others.
• **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].

[13] Please see answer to question 274 in EBA's Analysis

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

11. Exemptions to the requirement to apply SCA

11.1 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 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.*"

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

11.3 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.

11.4 Merchants cannot apply SCA exemptions in their own right.

11.5 The table below, which is identical to the EBA's table in its 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

11.6 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.

11.7 Only one exemption type can be applied for any given transaction, even if the given transaction could qualify for more than one exemption . 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.

11.8 PSPs that make use of any of the exemptions are allowed at any time to choose to step up and apply SCA[15].

12. Access to Payment Account Information (Article 10)

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.

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

13.1 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."*

13.2 This exemption applies from 14 September 2019 and so contactless payments on and from this date 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.

13.3 UK Finance are of the view that providers who do not have to have both a means of counting volume and value of consecutive transactions. This is especially as the 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.

[15] Please see Recital 17 of the RTS

13.4 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 Opinion does not require a change to this position.

13.5 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 e.g. Touch ID coupling possession and inherence can meet the requirements of SCA.

13.6 The cumulative limit is either the limit based on the number of transactions or the monetary amount (but not both). This means that PSPs may decide at the outset which cumulative limit they use (rather than on a transaction-by-transaction basis), as it may otherwise be confusing for consumers.

13.7 UK Finance's view is that contactless limits should be applied at device/token level rather than account level, 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.

13.8 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 the full requirements of the counter (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.

13.9 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.

13.10 For sake of clarity, the limits (EUR150 or 5 transactions) apply separately, so SCA must be applied as soon as the limit selected by the issuer is exceeded.

14. Transport and parking (Article 12)

14.1 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:

> *"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."*

14.2 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. However, members have raised a concern that if a volume counter was required on the device as well as a value counter, this could result in the five-transaction limit being met in the transit environment and a requirement for PIN at a transport gate. UK Finance therefore believe that in the context of a transit or parking environment, the counter referred to in the context of the contactless exemption does 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.

15. Trusted beneficiaries (Article 13)

15.1 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."

15.2 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 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).

15.3 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.

15.4 Credit transfers are in scope; however, it is down to the ASPSP to manage the process of adding or removing trusted beneficiaries.

15.5 Card payments are in scope; however, it is down to the issuer to manage the process of adding or removing trusted beneficiaries.

15.6 As per the EBA Opinion on application of the RTS, PISPs are not able to create a generic list of trusted beneficiaries.

15.7 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 when the RTS apply, though PSPs may wish to seek confirmation using SCA of an existing list. All trusted beneficiaries added from the application date of the RTS will need to be subject to SCA.

15.8 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 are 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.

16. Recurring transactions (Article 14)

16.1 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."

16.2 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.

16.3 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.

16.4 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.

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

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."*

18. Low value remote payments (Article 16)

18.1 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."

18.2 PSPs can choose not to apply SCA where a remote transaction does not exceed EUR 30, and where the cumulative value and number of previous transactions without SCA do not exceed EUR 100, or 5 times.

18.3 For sake of clarity, the limits (EUR100 or 5 transactions) apply separately, so SCA must be applied as soon as the selected one is exceeded.

18.4 Unlike the Article 11 (Contactless) exemption, this exemption must be applied at payment account (not payment instrument) level, meaning that the count applies cumulatively to the payment type, irrespective of the particular channel used to initiate each remote payment.

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

19.1 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]*."*

19.2 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.

19.3 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.

19.4 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 SCA is applied.

20. Transaction risk analysis

20.1 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.

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
EUR 500	0.01	0.005
EUR 250	0.06	0.01
EUR 100	0.13	0.015

20.2 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 EUR 500.

- **Transaction risk analysis (TRA)**

20.3 A PSP can choose not to apply SCA where the transaction poses a low level of risk, according to:

- The transaction monitoring mechanism set out in Article 2.
- Where an additional risk analysis that takes into account the risk factors set out in Article 18 of the RTS are met (as outlined above).

20.4 This includes a requirement that the fraud rate for that type of transaction meets the Exemption Threshold Values set out in the Annex and detailed in the table above (i.e. is equal to or lower than the ETV).

20.5 PSPs with a fraud rate that is equal to or falls below the values detailed in the table above can apply the TRA exemption.

20.6 The calculation of the fraud rate includes both unauthorised transactions and fraudulent transactions resulting from the manipulation of the payer[16]. Please see the section below 'Who can apply transaction risk analysis' for more detail. The calculation is set out as:

"the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under an exemption. The fraud rate is calculated on a rolling 90-day basis"

- **Allocation of fraud between the issuer and the acquirer for the calculation of the reference fraud rate**

20.7 In the case of transactions processed by more than one PSP (e.g. card transactions), the fraudulent transactions included in the calculation for a given PSP's fraud rate should be based on (i) the unauthorised transactions for which the given PSP has borne liability, as determined in accordance with Article 74 of PSD2, and (ii) other fraudulent transactions which have not been prevented by that PSP[17].

20.8 The fraud rate as defined in Annex A of the RTS is calculated for all credit transfer transactions and all card payment transactions and cannot be defined per individual payee (e.g. merchant) or per channel (whether app or web interface). The fraud rate that determines whether or not a PSP qualifies for the SCA exemption cannot be calculated for specific merchants only, i.e. where the payer wants to make a payment to a specific merchant and this specific merchant has a fraud risk that is below the threshold.

20.9 While the payee's PSP (acquirer) may contractually agree to 'outsource' its transaction risk analysis monitoring to a given merchant, or allow only certain predefined merchants to benefit from that PSP's exemption (based on a contractually agreed low fraud rate), the fraud rate making a given PSP eligible for an exemption under Article 18 would still need to be calculated on the basis of the payee PSP's executed or acquired transactions, rather than on an individual merchant's transactions[18].

20.10 The EBA has clarified in its Opinion that for card transactions, which are processed by more than one PSP (an acquirer and issuer), the fraudulent transactions included in the calculation for a PSP's fraud rate should be based on:

- The unauthorised transactions for which the given PSP has liability, as determined by Article 74 of PSD2, and
- Other fraudulent transactions which have not been prevented by that PSP.

20.11 UK Finance is of the view that in the case that one of the PSPs (the issuer or the acquirer) applies an exemption, any fraud from that given transaction is only attributable the PSP that applied or requested the exemption. For sake of clarity, if an acquirer applies the TRA exemption and a transaction is fraudulent, the value of that transaction is only added to the fraud calculation of the acquirer, not the issuer.

- **Who can apply the transaction risk analysis (TRA) exemption?**

20.12 The TRA exemption must be applied by a PSP as outlined in Article 18(1) of the RTS. The term 'PSP' includes issuers, acquirers or other authorised parties in the payment chain.

20.13 For the sake of clarity, according to the EBA's Opinion, PISPs cannot apply the TRA exemption, this decision is down to the ASPSP and based on the ASPSP's fraud rate.

20.14 Merchants cannot apply the TRA exemption themselves.

20.15 However, according to the EBA Opinion, an acquirer may contractually agree to "outsource" its transaction risk analysis monitoring to a given merchant. This allows acquirers to benefit from the sophisticated risk profiling,

[16] Manipulation of the payer, in other words, circumstances where the payer issues a payment order or gives the instruction to do so to the payment service provider, in good-faith, to the fraudster as a beneficiary (e.g. the fraudster impersonates a payee to which the payer consents to transfer money to).
[17] Please see EBA Opinion Paragraph 46
[18] Please see EBA Opinion Paragraph 47

screening and fraud monitoring capabilities of some merchants and allows the acquirer to take that merchant assessment (of the risk of a transaction) into account when taking a decision over whether or not to apply the exemption.

20.16 In order to apply the exemption, a PSP is required to provide the competent authorities, upon request, with the methodology, model and fraud rates it is using for the application of the TRA exemption, upon their request. This effectively means PSPs will be required to monitor their fraud rates to continue to apply the TRA exemption and notify their competent authority once they go over the reference fraud rates.

20.17 In order to apply the exemption the PSP would need to be regulated by an EEA competent authority.

20.18 We are therefore of the view that an issuer and acquirer can both apply their TRA exemption. The final decision rests with the issuer. As stated above, a PISP cannot apply or request a TRA exemption in their own right, this decision is down to the ASPSP.

20.19 In practice, if the acquirer applies their TRA exemption, as per Article 74 (2) of PSD2, they are liable for any fraud loss and the liability shifts to the payee's PSP. If an acquirer requests the use of a TRA exemption, the issuer can choose whether to accept that and whether to make use of the acquirer exemption. In other words, even if the issuer's own fraud rates do not meet the relevant TRA requirements, they are not required to step up to SCA as the acquirer has exempted the transaction and performed the required fraud monitoring and checks.

20.20 As above, another party in the payment chain (payee's PSP, payee or payment facilitator) can suggest the need for the application of the TRA exemption, or provide fraud data to the payer's PSP, but the payer's PSP ultimately decides whether SCA should be applied. Page 10 of the EBA RTS Rationale states: "24. *….Some of the respondents that are merchants' acquirers or payees' PSPs, explain that they perform transaction risk analysis and are well positioned to identify any potential fraud or other abuse from a payee's perspective and should therefore not always have to perform SCA but should instead have the choice to use a (now new) exemption based on transaction-risk analysis. The EBA concurs with the views expressed by these respondents and has made it clearer in the RTS that both payees' and payers' PSPs could trigger such an exemption under their own and exclusive responsibility but with the payer's PSP having the final say.*"

20.21 To the greatest possible extent in a cards context, everyone should be technically capable (enrolled) in 3DSecure (3DS).

- **Calculation of fraud rates**

20.22 The RTS require PSPs to monitor their fraud rates on an ongoing basis in order to be able to apply TRA. Article 19 of the RTS provide that:

Article 19

1. *For each type of transaction referred to in the table set out in the Annex, the payment service provider shall ensure that the overall fraud rates covering both payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in Articles 13 to 18 are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in the Annex.*

   The overall fraud rate for each type of transaction shall be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Articles 13 to 18 on a rolling quarterly basis (90 days).

2. *The calculation of the fraud rates and resulting figures shall be assessed by the audit review referred to in Article 3(2), which shall ensure that they are complete and accurate.*

3. *The methodology and any model, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves, shall be adequately documented and made fully available to competent authorities and to EBA, with prior notification to the relevant competent authority(ies), upon their request.*

20.23 UK Finance view that 'rolling basis' as referred to under recital 14 of the RTS means that every quarter (i.e. every three months) the PSP is required to ensure that their reference fraud rate does not exceed those detailed in the calculation of TRA.

20.24 If a PSP exceeds the overall reference fraud rates, they should therefore notify the competent authority that they can no longer apply TRA and should also give notification if their rate then falls below the reference fraud rate and the PSP would therefore like to apply TRA once more.

20.25 For clarity, if a PSP moves between two different reference fraud rates e.g. 0.005% and 0.015% (for remote credit transfers), the PSP is not required to notify the competent authority.

20.26 The EBA and competent authorities are able to request to view a PSP's reference fraud rates at any time. As above, this covers rolling 90 day periods.

20.27 PSPs are required to audit the monitoring of their reference fraud rates.

20.28 The EBA's fraud reporting Guidelines are separate requirements.

19 October 2018