Single Rulebook Q&A

Question ID	2020_5133
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	97
Paragraph	2
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	5
Date of submission	17/02/2020
Published as Final Q&A	29/05/2020
Disclose name of institution / entity	Yes
Name of institution / submitter	European Banking Federation
Country of incorporation / residence	Belgium
Type of submitter	Industry association
Subject matter	Dynamic linking: transactions for which the final amount is unknown and may be lower or higher than authenticated amount
Question	For remote card transactions, is it acceptable that there are legitimate cases where the final amount may be lower or higher than the amount authenticated by the cardholder?
Background on the question	For remote card transactions, there are legitimate cases where the final amount may be lower or higher than the amount authenticated by the cardholder, if both of the following conditions are met: (1) prior to initiation of the payment transaction, the cardholder is aware that the final amount may increase/decrease after authentication and agrees to the card transaction on that basis; and (2) in case of increase, this does not exceed the cardholder's reasonable expectations within the meaning of Article 76(1) PSD2. During the check-out process it is common practice for the cardholder to agree to such movement in amount providing it

remains within their reasonable expectations for the goods or services being provided by the payee. At all times the cardholder retains their rights under Article 76(1) PSD2. When authorising such transactions, the issuing bank may also conduct a risk analysis which will consider any variance so as to always act in the best interests of the cardholder. Article 97(2) PSD2 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." The RTS require that, for remote transactions, the authentication code generated is "specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction" (Article 5(1)(b) RTS). The RTS also require that “any change to the amount or the payee results in the invalidation of the authentication code generated” (Article 5(1)(d) RTS). We understand this to explicitly cover changes during authentication and not, for example, authorisation of transactions. If this requirement is to be interpreted as extending beyond authentication, this poses significant technical challenges for payment transactions for which the final amount is unknown (i.e. where the final amount may vary upwards or downwards) after the cardholder/Payment Services User (PSU) authenticates the transaction for legitimate reasons. In these cases, the final amount is determined only after the transaction is authenticated. In many cases this may take place hours, days or (in some limited and 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. For example, when the PSU buys groceries online, s/he authenticates for a provisional amount and agrees to the final amount varying on the basis of the actual cost of weighed goods or substitutions. S/he may also agree to additions to basket or replacement of out-of-stock products. Requiring the PSU to authenticate for a second time when the final amount is determined (e.g., when the groceries are weighed) would create serious inconveniences for consumers and increased costs for merchants. The PSU is unable to conveniently authenticate for a second time because when the goods are picked (e.g., 4am) s/he will not be ‘in-session’ (e.g., logged out from the merchant’s website and not sitting anymore in front of her/his computer). The purchase or shipping will be delayed or more likely, aborted if the PSU needs to authenticate for a second time. This will result in a poor customer experience, higher costs for merchants, wastage and in distrust in e-commerce and electronic payments for consumers. Requiring the PSU to authenticate for a second time will also not increase security. The PSU has already authenticated the transaction once and for the legitimate transaction. The transaction is therefore legitimate and secure. A second authentication by the PSU is therefore redundant from a security perspective. This is also the approach expressly 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)(a) RTS reads: "in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of that Directive, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction". Although, this provision applies to pre-authorisations for which funds are blocked, we believe the same principle (i.e., the authorised amount may be lower than the authenticated amount) should apply for transactions where funds are not blocked. This shows that if the PSU has already authenticated with SCA a transaction for which the final amount is unknown, this final amount may be different from the authenticated amount. The issue is therefore not about security under Article 97 PSD2, but about consent to the possible different amount under the consumer rights of PSD2. Article 76(1) PSD2 envisages that for transactions for which the final amount is unknown the final amount may vary and the payer is entitled to a refund if the final amount exceeds what s/he could reasonably have expected. Therefore, if prior to initiation of the payment transaction the PSU 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 this increase is within the PSU's reasonable expectations, as previously agreed, a second authentication by the PSU is therefore not needed from a consumer rights perspective. Please note that the pre-authorisation model envisaged by Article 75 PSD2 does not cover the present case. With pre-authorisation, the PSU is generally required to authenticate the expected transaction amount plus a certain margin (e.g., at an unattended petrol station). The funds are blocked on the PSU's account until the issuer is informed of the exact final amount (and at the latest immediately after receipt of the payment order). For the use cases where the pre-authorisation model is not foreseen, this may result in the PSU's funds being blocked for a period of time, which may result in serious inconvenience/detriments for the PSU. Finally, please note that treating payment of the incremental amount as a separate transaction to the original transaction is not an appropriate solution either, not least as it would duplicate transaction costs, fees and data for merchants. It will also be confusing to the customer, seeing two transactions on their bank statement for one transaction and this would still not solve for the fact that the customer may not be 'in-session'.
EBA answer	Article 97(1)(b) of Directive 2015/2366/EU (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) when the payer initiates an electronic payment transaction. In the case of electronic remote payment transactions, Article 97(2) PSD2 requires PSPs to apply SCA that includes elements, which dynamically link the transaction to a specific amount and a specific payee.

Article 5(1)(a) of the Delegated Regulation (EU) 2018/389 specifies that "where payment service providers apply strong customer authentication in accordance with Article 97(2) of PSD2, the payer shall be made aware of the amount of the payment transaction and of the payee". Further, Article 5(1)(b) and (c) of the Delegated Regulation require respectively that "the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction" and that "the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer". Furthermore, according to Article 5(1)(d) of the Delegated Regulation, "any change to the amount or the payee results in the invalidation of the authentication code generated".

Therefore, for remote electronic payment transactions where the exact transaction amount is known in advance, in line with the requirements of Article 5(1) of the Delegated Regulation, the final amount shall be the same as the amount the payer was made aware of and agreed to when initiating the transaction.

In the cases where the exact amount of a card-based payment transaction is not known at the moment when the payer gives consent to execute the payment transaction, Article 75(1) of PSD2 provides that "the payer's PSP may block funds on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked". In this regard, Article 5(3)(a) of the Delegated Regulation further provides that, "in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of that Directive, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction". Further, Recital 5 of the Delegated Regulation states that "it is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to".

With regard to the above, for card-based payment transactions where the exact transaction amount is not known in advance, if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction, the payer's PSP shall apply SCA to the final amount of the transaction or decline the transaction. If the final amount is equal to or lower than the amount agreed in accordance with Article 75(1) of PSD2, the transaction can be executed and there is no need to re-apply SCA, as the authentication code would still be valid in accordance with Article 5(3)(a) of the Delegated Regulation. This applies also to card-based payment transactions where the exact amount is not known in advance

	and funds are not blocked by the payer's PSP in accordance with Article 75(1) of PSD2.
Link	https://eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5133

European Banking Authority, 15/08/2020
www.eba.europa.eu