***Changes to legislation:*** *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2018/389. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2018 No. 389 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

# Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance)

## COMMISSION DELEGATED REGULATION (EU) 2018/389

## of 27 November 2017

## supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

## (Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC[(1)], and in particular the second subparagraph of Article 98(4) thereof,

Whereas:

(1) Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that 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, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

(2) As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality

**Changes to legislation:** *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2018/389. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2018 No. 389 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments and operationally independent. In order to allow competent authorities to monitor the quality of the review of these measures, such reviews should be made available to them upon their request.

(3) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication 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.

(4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes 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.

(5) 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 in Directive (EU) 2015/2366.

(6) In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as 'knowledge' (something only the user knows), such as length or complexity, for the elements categorised as 'possession' (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as 'inherence' (something the user is) such as algorithm specifications, biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device,namely a device such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

(7) The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.

(8) Due to their very nature, payments made through the use of an anonymous payment instruments are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from Directive (EU) 2015/2366 and this Regulatory Technical Standard.

***Changes to legislation:** There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2018/389. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2018 No. 389 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

(9) In accordance with Directive (EU) 2015/2366, exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

(10) Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider, pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

(11) Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user-friendly and low-risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

(12) Similar to the exemption for low-value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase is posing a slightly higher security risk.

(13) The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that Directive (EU) 2015/2366 aims to achieve through strong customer authentication. Where the competent authorities establish that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of Directive (EU) 2015/2366

**Changes to legislation:** *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2018/389. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2018 No. 389 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.

(14) In the case of real-time transaction risk analysis that categorise a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk-based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

(15) For the purpose of ensuring an effective enforcement, payment service providers that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to competent authorities and to the European Banking Authority (EBA), upon their request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

(16) The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the EBA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The EBA should review and submit draft updates to the Commission of these regulatory technical standards, where appropriate, by submitting new draft thresholds and corresponding fraud rates with the aim of enhancing the security of remote electronic payments, in accordance with Article 98(5) of Directive (EU) 2015/2366 and with Article 10 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[(2)].

(17) Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.

(18) The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

***Changes to legislation:** There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2018/389. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2018 No. 389 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

(19) In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availabilty of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. Directive (EU) 2015/2366 provides for the access and use of payment account information by account information service providers. This regulation therefore does not change the rules of access to accounts other than payment accounts.

(20) Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. To ensure technology and business-model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

(21) In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. Moreover, the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions at least 6 months prior to the application date of these regulatory standards or, if the launch takes place after the application date of these standards, prior to the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international or European standardisation organisations.

(22) The quality of the services provided by account information service providers and payment initiation service providers will be dependent on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of national competent authorities to ensure that account information service providers and payment intitation service providers are not blocked or obstructed in the provision of their services.