TECHNICAL STANDARDS (STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE METHODS OF COMMUNICATION) (AMENDMENT) INSTRUMENT 2025

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the powers and related provisions in or under:

(1) the following regulations of the Payment Services Regulations 2017 (SI 2017/752):

(a) regulation 106A (Technical standards); and
(b) regulation 120 (Guidance); and

(2) the following sections of the Financial Services and Markets Act 2000 ("the Act"):

(a) section 137T (General supplementary powers);
(b) section 138F (Notification of rules);
(c) section 138I (Consultation by the FCA);
(d) section 138P (Technical standards);
(e) section 138Q (Standards instruments);
(f) section 138R (Treasury approval); and
(g) section 138S (Application of Chapters 1 and 2).

B. The provisions referred to above are specified for the purpose of section 138Q(2) (Standards instruments) of the Act.

Pre-conditions to making

C. The FCA has consulted the Prudential Regulation Authority and the Bank of England as appropriate in accordance with section 138P of the Act.

D. A draft of this instrument has been approved by the Treasury in accordance with section 138R of the Act.

Modifications

E. The following technical standard is amended in accordance with the Annex to this instrument.

Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication

Commencement

F. This instrument comes into force on 19 March 2026.

Citation

G. This instrument may be cited as the Technical Standards (Strong Customer Authentication and Common and Secure Methods of Communication) (Amendment) Instrument 2025.

By order of the Board
18 December 2025

In this Annex, underlining indicates new text and striking through indicates deleted text.

Annex

Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication

…

Chapter -1

Guidance

…

11. Exemptions for ~~low-value~~ low-risk 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~~ low-risk 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 poses a slightly higher security risk.

…

14. In the case of real-time transaction risk analysis that categorises a remote electronic 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, as provided for under Article 18 (Transaction risk analysis) of these standards. ~~Those~~ For the purpose of Article 18, 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.

…

…

Chapter 3

Exemptions from strong customer authentication

…

Article 11

Contactless payments at point of sale

~~Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, 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 £100; 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 £300; 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.~~

Subject to compliance with Article 2, payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a contactless electronic payment transaction identified by the payment service provider as posing a low level of risk.