TECHNICAL STANDARDS ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE METHODS OF COMMUNICATION (AMENDMENT) (NO 2) INSTRUMENT 2021

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:

(a) Regulation 106A (Technical Standards);
(b) Regulation 120 (Guidance); and

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

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

Pre-conditions to making

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

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

Modifications

D. The FCA makes the amendments to the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication in accordance with the Annex to this instrument

Commencement

E. This instrument comes into force as follows:

(1) Articles 10A and 36(6) in the Annex, and the amendments to Article 10 in the Annex come into force on 26 March 2022.
(2) The amendments to Article 31 in the Annex come into force on 26 May 2023.
(3) The remainder of the Annex comes into force on 30 November 2021.

Citation

F. This instrument may be cited as the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication (Amendment) (No 2) Instrument 2021.

By order of the Board
26 November 2021

Annex

Amendments to the Technical Standards on strong customer authentication and common and secure methods of communication

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

Chapter -1

Guidance

1. …

…

19. …

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. The effect of Articles 30(3) and (5) is that the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions ~~at least six months prior to~~ by 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 standardisation organisations.

22. …

…

…

Chapter 3

Exemptions from strong customer authentication

Article 10

Payment account information <u>accessed directly by a payment service user</u>

<u>(-1) This Article applies where a payment service user is not using an account information service provider to access payment account information.</u>

(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) …

<u>Article 10A</u>

<u>Payment account information accessed through an account information service provider</u>

<u>(1) This Article applies where a payment service user is accessing account information through an account information service provider.</u>

<u>(2) Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and paragraph 3 of this Article, where a payment service user is limited to accessing either or both of the following items without disclosure of sensitive payment data:</u>

<u>(a) the balance of one or more designated payment accounts;</u>

<u>(b) the payment transactions executed in the last 90 days through one or more designated payment accounts.</u>

<u>(3) For the purpose of paragraph 2, payment service providers shall not be exempted from the application of strong customer authentication unless strong customer authentication has been applied on at least one previous occasion where the account information service provider accessed the information specified in paragraph 2 on behalf of the payment service user.</u>

…

Chapter 5

Common and secure open standards of communication

Section 1

…

Section 2

Specific requirements for the common and secure open standards of communication

Article 30

General obligations for access interfaces

(1) …

(2) …

(3) Account servicing payment service providers shall ensure that their interfaces follow standards of communication which are issued by international standardisation organisations.

Account servicing payment service providers shall also ensure that the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers.

Account servicing payment service providers shall at a minimum, and no ~~less than six months before the target~~ later than the date ~~for~~ of the market launch of the access interface, make the documentation available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied to the FCA or the Gibraltar Financial Services Commission for the relevant authorisation, and shall make a summary of the documentation publicly available on their website.

(4) …

(5) Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. This testing facility should be made available no later than ~~six months before~~ the ~~target~~ date ~~for~~ of the market launch of the access interface.

However, no sensitive information shall be shared through the testing facility.

(6) …

Article 31

Access interface options

(1) ~~Account~~ Subject to paragraph 2 of this Article, account servicing payment service providers shall establish the interface(s) referred to in Article 30 by means of a dedicated interface or by allowing the use by the payment service providers referred to in Article 30(1) of the interfaces used for authentication and communication with the account servicing payment service provider's payment services users.

(2) Account servicing payment service providers specified in paragraph 3 of this Article shall establish the interface(s) referred to in Article 30 by means of a dedicated interface in respect of all payment accounts that fall within one or more of the following descriptions:

(a) a payment account as defined in regulation 2(1) of the Payment Accounts Regulations 2015 (SI 2015/2038);

(b) an account operated for an SME that would be the type of account described in paragraph 2(a) of this Article if it were operated for a consumer; and

(c) a credit card account operated for a consumer or an SME.

(3) An account servicing payment service provider is specified for the purposes of paragraph 2 of this Article if it is not:

(a) a small payment institution;

(b) a small electronic money institution as defined in regulation 2(1) of the Electronic Money Regulations 2011 (SI 2011/99); or

(c) deemed to be authorised under paragraph 1, 12B, 14(2(a)(i) or 24(4)(a)(i) of Schedule 3 of the Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 or regulation 8, 11, 28 or 34 of the EEA Passport Rights (Amendment, etc., and Transitional Provisions) (EU Exit) Regulations 2018.

(4) For the purposes of this Article:

(a) consumer means a consumer as defined in regulation 2(1) of the Payment Accounts Regulations 2015 (SI 2015/2038); and

(b) SME means an enterprise as defined in Article 1 and Article 2(1) of the Annex to the Recommendation 2003/361/EC of 6th May 2003 concerning the definition of micro, small and medium-sized enterprises.

…

Article 33

Contingency measures for a dedicated interface

(1) …

…

(5) For this purpose, and from no later than six months after the date of the market launch of the interface, account servicing payment service providers shall ensure that the payment service providers referred to in Article 30(1) can be identified and can rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. Where the payment service providers referred to in Article 30(1) make use of the interface referred to in paragraph 4 they shall:

(a) take the necessary measures to ensure that they do not access, store or process data for purposes other than for the provision of the service as requested by the payment service user;

(b) continue to comply with the obligations following from Regulations 69(3) and 70(3) of the Payment Services Regulations 2017 (SI 2017/752) respectively;

(c) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request and without undue delay, the log files to the FCA;

(d) duly justify to the FCA, upon request and without undue delay, the use of the interface made available to the payment service users for directly accessing its payment account online;

(e) inform the account servicing payment service provider accordingly.

(6) ~~The~~ Subject to paragraph 6A of this Article, the FCA will exempt account servicing payment service providers that have opted for a dedicated interface from the obligation to set up the contingency mechanism described under paragraph 4 where the dedicated interface meets all of the following conditions:

(a) it complies with all the obligations for dedicated interfaces as set out in Article 32;

(b) it has been designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein;

(c) it has been widely used for at least three months by payment service providers to offer account information services, payment initiation services and to provide confirmation on the availability of funds for card-based payments;

(d) any problem related to the dedicated interface has been resolved without undue delay.

(6A) An account servicing payment service provider to whom this paragraph applies is deemed to have been exempted by the FCA under paragraph 6 of this Article if, at

11pm on 31 December 2020, it was exempted from the obligation to set up a contingency mechanism by its home state competent authority under Article 33(6) of 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 communications.

This paragraph applies to account servicing payment service providers deemed to be authorised under paragraph 1, 12B, 14(2(a)(i) or 24(4)(a)(i) of Schedule 3 of the Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 or regulation 8, 11, 28 or 34 of the EEA Passport Rights (Amendment, etc., and Transitional Provisions) (EU Exit) Regulations 2018.

(7) The exemption referred to in paragraph 6 (including any deemed exemption under paragraph 6A) will be revoked where the conditions 6(a) and 6(d) are not met by the account servicing payment service providers for more than two consecutive calendar weeks. The FCA will ensure that the account servicing payment service provider establishes, within the shortest possible time and at the latest within two months, the contingency mechanism referred to in paragraph 4.

…

Article 36

Data exchanges

(1) …

…

(5) …

(6) An account information service provider may only access information in the circumstances described in paragraph 5(b) of this Article, if the payment service user has confirmed with the account information service provider within the previous 90 days that the payment service user continues to consent to such access.