Subsidiary Legislation made under s.626A of the Financial Services Act 2019 and r.79A of the Financial Services (Payment Services) Regulations 2020.

Financial Services (Strong Customer Authentication Etc.) (Technical Standards) Regulations 2021

LN.2021/230

Commencement **15.4.2021**

Amending enactments	Relevant current provisions	Commencement date
LN.2024/166	ANNEX - Articles. 10, 10A, 18(2)(a)-(b), 19(1), 20(1)-(2), 30(6), (9), 31(1)-(5), 33(5)-(6), (6A)-(6B), (7), 36(7)	5.9.2024

ARRANGEMENT OF REGULATIONS.

ANNEX

TECHNICAL STANDARDS ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE METHODS OF COMMUNICATION

CHAPTER 1
GENERAL PROVISIONS

CHAPTER 2
SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

CHAPTER 3
EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Financial Services (Strong Customer Authentication Etc.) (Technical Standards) Regulations 2021 2021/230

In exercise of the powers conferred on the Minister by section 626A of the Financial Services Act 2019 and regulation 79A of the Financial Services (Payment Services) Regulations 2020, the Minister has made these Regulations-

Title.

1. These Regulations may be cited as the Financial Services (Strong Customer Authentication Etc.) (Technical Standards) Regulations 2021.

Commencement.

2. These Regulations come into operation on the day of publication.

Technical Standards.

3.(1) The Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication, set out in the Annex to these Regulations, have effect.

Revocation.

4. 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 is revoked.

ANNEX

TECHNICAL STANDARDS ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE METHODS OF COMMUNICATION

CHAPTER 1
GENERAL PROVISIONS

Subject matter.

1. These Standards establish the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to do the following–

(a) apply the procedure of strong customer authentication in accordance with regulation 79 of the Financial Services (Payment Services) Regulations 2020;

(b) exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and of the payment channel used for its execution;

(c) protect the confidentiality and the integrity of the payment service user's personalised security credentials;

(d) establish common and secure open standards for the communication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers in relation to the provision and use of payment services in Chapter 2 of Part 3 of the Financial Services (Payment Services) Regulations 2020.

General authentication requirements.

2.(1) Payment service providers must have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in Article 1(a) and (b).

(2) Those mechanisms must be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials.

(3) Payment service providers must ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors–

(a) lists of compromised or stolen authentication elements;

(b) the amount of each payment transaction;

(c) known fraud scenarios in the provision of payment services;

(d) signs of malware infection in any sessions of the authentication procedure;

(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

Review of the security measures.

3.(1) The implementation of the security measures referred to in Article 1 must be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework of the payment service provider by auditors with expertise in IT security and payments and operationally independent within or from the payment service provider.

(2) The period between the audits referred to in paragraph (1) must be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider.

(3) However, payment service providers that make use of the exemption referred to in Article 18 must be subject to an audit of the methodology, the model and the reported fraud rates at a minimum on a yearly basis. The auditor performing this audit must have expertise in IT security and payments and be operationally independent within or from the payment service provider. During the first year of making use of the exemption under Article 18 and at least every three years thereafter, or more frequently at the GFSC's request, this audit must be carried out by an independent and qualified external auditor.

(4) This audit must present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in these Standards.

(5) The entire report must be made available to the GFSC upon its request.

CHAPTER 2
SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Authentication code.

4.(1) Where payment service providers apply strong customer authentication in accordance with regulation 79(1) of the Financial Services (Payment Services) Regulations 2020, the authentication must be based on two or more elements which are categorised as knowledge, possession and inherence and must result in the generation of an authentication code.

(2) The authentication code must be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

(3) For the purpose of paragraphs (1) and (2), payment service providers must adopt security measures ensuring that each of the following requirements is met–

(a) no information on any of the elements referred to in those paragraphs can be derived from the disclosure of the authentication code;

(b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;

(c) the authentication code cannot be forged.

(4) Payment service providers must ensure that the authentication by means of generating an authentication code includes each of the following measures–

(a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraphs (1) and (2), it must not be possible to identify which of the elements referred to in those paragraphs was incorrect;

(b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in regulation 79(1) of the Financial Services (Payment Services) Regulations 2020 must be temporarily or permanently blocked, must not exceed five within a given period of time;

(c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter 5.

(d) the maximum time without activity by the payer after being authenticated for accessing its payment account online must not exceed five minutes.

(5) Where the block referred to in paragraph (4)(b) is temporary, the duration of that block and the number of retries must be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in Article 2(3).

(6) The payer must be alerted before the block is made permanent.

(7) Where the block has been made permanent, a secure procedure must be established allowing the payer to regain use of the blocked electronic payment instruments.

Dynamic linking.

5.(1) Where payment service providers apply strong customer authentication in accordance with regulation 79(2) of the Financial Services (Payment Services) Regulations 2020, in addition to the requirements of Article 4 of these Standards, they must also adopt security measures that meet each of the following requirements–

(a) the payer is made aware of the amount of the payment transaction and of the payee;

(b) 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;

(c) 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;

(d) any change to the amount or the payee results in the invalidation of the authentication code generated.

(2) For the purpose of paragraph (1), payment service providers must adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following–

(a) the amount of the transaction and the payee throughout all of the phases of the authentication;

(b) the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.

(3) For the purpose of paragraph (1)(b) and where payment service providers apply strong customer authentication in accordance with regulation 79(2) of the Financial Services (Payment Services) Regulations 2020 the following requirements for the authentication code apply–

(a) 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 regulation 52 of the Financial Services (Payment Services) Regulations 2020, the authentication code must be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction;

(b) in relation to payment transactions for which the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code must be specific to the total amount of the batch of payment transactions and to the specified payees.

Requirements of the elements categorised as knowledge.

6.(1) Payment service providers must adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

(2) The use by the payer of those elements must be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

Requirements of the elements categorised as possession.

7.(1) Payment service providers must adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

(2) The use by the payer of those elements must be subject to measures designed to prevent replication of the elements.

Requirements of devices and software linked to elements categorised as inherence.

8.(1) Payment service providers must adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the payment service providers must ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.

(2) The use by the payer of those elements must be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.

Independence of the elements.

9.(1) Payment service providers must ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.

(2) Payment service providers must adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.

(3) For the purposes of paragraph (2), the mitigating measures must include each of the following–

(a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

(b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;

(c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

CHAPTER 3
EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Payment account information accessed directly by a payment service user.

10.(1) This Article applies where a payment service user is not using an account information service provider to access payment account information.

(2) Payment service providers are allowed not to apply strong customer authentication, subject to compliance with the requirements in Article 2 and to paragraph (3) 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.

(3) For the purpose of paragraph (2), payment service providers are not exempt from the application of strong customer authentication where either of the following conditions are met–

(a) the payment service user is accessing online the information specified in paragraph (2) 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 (2)(b) and strong customer authentication was applied.

Payment account information accessed through an account information service provider.

10A.(1) This Article applies where a payment service user is accessing account information through an account information service provider.

(2) Payment service providers are allowed not to apply strong customer authentication, subject to compliance with the requirements in Article 2 and paragraph (3) where a payment service user is limited to accessing either or both of the following items 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.

(3) For the purpose of paragraph (2), payment service providers are not exempt 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.

Contactless payments at point of sale.

11. Payment service providers must 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.

Unattended terminals for transport fares and parking fees.

12. Payment service providers must be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, 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.

Trusted beneficiaries.

13.(1) Payment service providers must 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 must 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.

Recurring transactions.

14.(1) Payment service providers must 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 must 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).

Credit transfers between accounts held by the same individual or legal person.

15. Payment service providers must be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates a credit transfer in circumstances where the payer and the payee are the same individual or legal person and both payment accounts are held by the same account servicing payment service provider.

Low-value transactions.

16. Payment service providers must 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 £25; 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 £85; 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 five consecutive individual remote electronic payment transactions.

Secure corporate payment processes and protocols.

17. Payment service providers must 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 GFSC is satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for the Financial Services (Payment Services) Regulations 2020.

Transaction risk analysis.

18.(1) Payment service providers must 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).

(2) An electronic payment transaction referred to in paragraph (1) must 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 Schedule 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 Schedule;

(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 must 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.

(4) The assessment made by a payment service provider must 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.

Calculation of fraud rates.

19.(1) For each type of transaction referred to in the table set out in the Schedule, the payment service provider must 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 Schedule.

(2) The overall fraud rate for each type of transaction must 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).

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

(4) The methodology and any model used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves, must be adequately documented and made fully available to the GFSC, at its request.

Cessation of exemptions based on transaction risk analysis.

20.(1) Payment service providers that make use of the exemption referred to in Article 18 must immediately report to the GFSC where one of their monitored fraud rates, for any type of payment transactions indicated in the table set out in the Schedule, exceeds the applicable reference fraud rate and must provide to the GFSC a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.

(2) Payment service providers must immediately cease to make use of the exemption referred to in Article 18 for any type of payment transactions indicated in the table set out in the Schedule in the specific exemption threshold range where their monitored fraud rate exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that exemption threshold range.

(3) Following the cessation of the exemption referred to in Article 18 in accordance with paragraph (2), payment service providers must not use that exemption again, until their

calculated fraud rate equals to, or is below, the reference fraud rates applicable for that type of payment transaction in that exemption threshold range for one quarter.

(4) Where payment service providers intend to make use again of the exemption referred to in Article 18, they must notify the GFSC in a reasonable timeframe and must before making use again of the exemption, provide evidence of the restoration of compliance of their monitored fraud rate with the applicable reference fraud rate for that exemption threshold range in accordance with paragraph (3).

Monitoring.

21.(1) In order to make use of the exemptions set out in Articles 10 to 18, payment service providers must record and monitor the following data for each type of payment transaction, with a breakdown for both remote and non-remote payment transactions, at least on a quarterly basis–

(a) the total value of unauthorised or fraudulent payment transactions in accordance with regulation 41(3) of the Financial Services (Payment Services) Regulations 2020, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;

(b) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;

(c) the number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions.

(2) Payment service providers must make the results of the monitoring in accordance with paragraph (1) available to the GFSC at its request.

CHAPTER 4
CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS

General requirements.

22.(1) Payment service providers must ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.

(2) For the purpose of paragraph (1), payment service providers must ensure that each of the following requirements is met–

(a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;

(b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text;

(c) secret cryptographic material is protected from unauthorised disclosure.

(3) Payment service providers must fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.

(4) Payment service providers must ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter 2 take place in secure environments in accordance with strong and widely recognised industry standards.

Creation and transmission of credentials.

23.(1) Payment service providers must ensure that the creation of personalised security credentials is performed in a secure environment.

(2) They must mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.

Association with the payment service user.

24.(1) Payment service providers must ensure that only the payment service user is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software.

(2) For the purpose of paragraph (1), payment service providers must ensure that each of the following requirements is met–

(a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure

environments under the payment service provider's responsibility comprising at least the payment service provider's premises, the internet environment provided by the payment service provider or other similar secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;

(b) the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.

Delivery of credentials, authentication devices and software.

25.(1) Payment service providers must ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.

(2) For the purpose of paragraph (1), payment service providers must at least apply each of the following measures–

(a) effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user;

(b) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet;

(c) arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel–

(i) no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;

(ii) the delivered personalised security credentials, authentication devices or software require activation before usage;

(d) arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation must take place in a secure environment in accordance with the association procedures referred to in Article 24.

Renewal of personalised security credentials.

26. Payment service providers must ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 23, 24 and 25.

Destruction, deactivation and revocation.

27. Payment service providers must ensure that they have effective processes in place to apply each of the following security measures–

(a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;

(b) where the payment service provider distributes reusable authentication devices and software, the secure re-use of a device or software is established, documented and implemented before making it available to another payment services user;

(c) the deactivation or revocation of information related to personalised security credentials stored in the payment service provider's systems and databases and, where relevant, in public repositories.

CHAPTER 5
COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

Section 1
General requirements for communication

Requirements for identification.

28.(1) Payment service providers must ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

(2) Payment service providers must ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

Traceability.

29.(1) Payment service providers must have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex-post of all events relevant to the electronic transaction in all the various stages.

(2) For the purpose of paragraph (1), payment service providers must ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following–

(a) a unique identifier of the session;

(b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;

(c) timestamps which must be based on a unified time-reference system and which must be synchronised according to an official time signal.

Section 2
Specific requirements for the common and secure open standards of communication

General obligations for access interfaces.

30.(1) Account servicing payment service providers that offer to a payer a payment account that is accessible online must have in place at least one interface which meets each of the following requirements–

(a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;

(b) account information service providers are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;

(c) payment initiation service providers are able to communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment transaction and all information accessible to the

account servicing payment service providers regarding the execution of the payment transaction.

(2) For the purposes of authentication of the payment service user, the interface referred to in paragraph (1) must allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.

(3) The interface must at least meet all of the following requirements–

(a) a payment initiation service provider or an account information service provider must be able to instruct the account servicing payment service provider to start the authentication based on the consent of the payment service user;

(b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service user concerned must be established and maintained throughout the authentication;

(c) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider must be ensured.

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

(5) Account servicing payment service providers must 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.

(6) Account servicing payment service providers must at a minimum, and no later than the date 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 GFSC or the UK Financial Conduct Authority for the relevant authorisation, and must make a summary of the documentation publicly available on their website.

(7) In addition to paragraphs (4) to (6), account servicing payment service providers must ensure that, except for emergency situations, any change to the technical specification of their interface is made available to 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 GFSC or the UK Financial Conduct Authority for the relevant authorisation, in advance as soon as possible and not less than three months before the change is implemented.

(8) Payment service providers must document emergency situations where changes were implemented and make the documentation available to the GFSC on request.

(9) Account servicing payment service providers must 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 the date of the market launch of the access interface.

(10) However, no sensitive information may be shared through the testing facility.

(11) The GFSC must ensure that account servicing payment service providers comply at all times with the obligations included in these Standards in relation to the interface(s) that they put in place. In the event that an account servicing payment services provider fails to comply with the requirements for interfaces laid down in these Standards, the GFSC must ensure that the provision of payment initiation services and account information services is not prevented or disrupted to the extent that the respective providers of such services comply with the conditions defined under Article 33(5).

Access interface options.

31.(1) Account servicing payment service providers must 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) Subject to paragraph (3), account servicing payment service providers must establish the interfaces referred to in Article 30 by means of a dedicated interface or by allowing the payment service providers referred to in Article 30(1) to use the interfaces used for authentication and communication with the account servicing payment service provider's payment services users.

(3) Account servicing payment service providers specified in paragraph (4) must establish the interfaces 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 paragraph 15 of Schedule 2 to the Act;

(b) an account operated for an SME that would be the type of account described in sub-paragraph (a) if it were operated for a consumer; or

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

(4) An account servicing payment service provider is specified for the purposes of paragraph (3) if it is not–

(a) a small payment institution;

(b) a small electronic money institution as defined in regulation 2(1) of the Financial Services (Electronic Money) Regulations 2020; or

(c) deemed to be authorised under the Financial Services (Passport Rights and Transitional Provisions) (EU Exit) Regulations 2020.

(5) For the purposes of this Article–

"consumer" has the meaning given in section 2(2) of the Act;

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

Obligations for a dedicated interface.

32.(1) Subject to compliance with Article 30 and 31, account servicing payment service providers that have put in place a dedicated interface must ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online.

(2) Account servicing payment service providers that have put in place a dedicated interface must define transparent key performance indicators and service level targets, at least as stringent as those set for the interface used by their payment service users both in terms of

availability and of data provided in accordance with Article 36. Those interfaces, indicators and targets must be monitored by the GFSC and stress-tested.

(3) Account servicing payment service providers that have put in place a dedicated interface must ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Part 4 of Schedule 2 to the Act and Part 2 and regulation 106 of the Financial Services (Payment Services) Regulations 2020, or regulations 4 and 6 of the Payment Services Regulations 2017 of the United Kingdom, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.

(4) For the purpose of paragraphs (1) and (2), account servicing payment service providers must monitor the availability and performance of the dedicated interface. Account servicing payment service providers must publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its payment service users.

Contingency measures for a dedicated interface.

33.(1) Account servicing payment service providers must include, in the design of the dedicated interface, a strategy and plans for contingency measures for the event that the interface does not perform in compliance with Article 32, that there is unplanned unavailability of the interface and that there is a systems breakdown. Unplanned unavailability or a systems breakdown may be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services are not replied to within 30 seconds.

(2) Contingency measures must include communication plans to inform payment service providers making use of the dedicated interface of measures to restore the system and a description of the immediately available alternative options payment service providers may have during this time.

(3) Both the account servicing payment service provider and the payment service providers referred to in Article 30(1) must report problems with dedicated interfaces as described in paragraph (1) to the GFSC without delay.

(4) As part of a contingency mechanism, payment service providers referred to in Article 30(1) must be allowed to make use of the interfaces made available to the payment service

users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32.

(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 must 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 must–

(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 43(4) and 44(3) of the Financial Services (Payment Services) Regulations 2020 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 GFSC;

(d) duly justify to the GFSC, 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) Subject to paragraph (6A), the GFSC may 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(9) 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 GFSC under paragraph (6) if, immediately before IP completion day, 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.

(6B) Paragraph (6A) applies to account servicing payment service providers deemed to be authorised under the Financial Services (Passport Rights and Transitional Provisions) (EU Exit) Regulations 2020.

(7) The exemption referred to in paragraph (6) (including any deemed exemption under paragraph (6A)) must be revoked where the conditions in paragraph (6)(a) and (d) are not met by the account servicing payment service providers for more than two consecutive calendar weeks. The GFSC must 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).

Certificates.

34.(1) For the purpose of identification, as referred to in Article 30(1)(a), account servicing payment service providers must accept both of the following electronic means of identification–

(a) qualified certificates for–

(i) electronic seals as referred to in Article 3(30) of the eIDAS Regulation; or

(ii) website authentication as referred to in Article 3(39) of that Regulation; and

(b) at least one other form of identification issued by an independent third party that is not unduly burdensome for payment service providers to obtain.

(2) Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments must rely on one of the above means of identification.

(3) For the purpose of these Standards, as referred to in paragraphs (1) and (2), the registration number as referred to in the official records in accordance with Annex III(c) or Annex IV(c) to the eIDAS Regulation and the registration number referred to in paragraph (9), must be the authorisation or registration number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available–

(a) in the register maintained by the GFSC in accordance with both Part 4 of the Act and, in relation to the provision of payment services, regulation 106 of the Financial Services (Payment Services) Regulations 2020; or

(b) in the case of payment service providers incorporated and registered or authorised in the United Kingdom, in the UK public register pursuant to regulation 4 of the Payment Services Regulations 2017 or section 347 of the Financial Services and Markets Act 2000 of the United Kingdom.

(4) For the purposes of these Standards, qualified certificates for electronic seals or website authentication referred to in paragraph (1)(a) must include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following–

(a) the role of the payment service provider, which may be one or more of the following–

(i) account servicing;

(ii) payment initiation;

(iii) account information;

(iv) issuing of card-based payment instruments;

(b) the name of the competent authorities where the payment service provider is registered.

(5) The attributes referred to in paragraph (4) must not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

(6) Where a form of identification under paragraph (1)(b) is used, account servicing payment service providers must–

(a) verify that the payment service provider is authorised or registered to perform the payment services relevant to its activities in a way that does not present an obstacle to the provision of payment initiation and account information services; and

(b) satisfy itself that the independent third party issuing that form of identification is suitable and has sufficient systems and controls to verify the information contained in the digital certificate referred to in paragraph (9).

(7) Account servicing payment service providers must make public the forms of identification they accept.

(8) Payment service providers relying on a form of identification under paragraph (1)(b) must notify the independent third party issuing that form of identification of any changes in identity information or regulatory authorisation in writing before such changes take effect or, where this is not possible, immediately after.

(9) A form of identification accepted under paragraph (1)(b) must be a digital certificate that–

(a) is issued upon identification and verification of the payment service provider's name, company number (if applicable) and its principal place of business;

(b) gives appropriate assurance to account servicing payment service providers in relation to the authenticity of the data and the identity of the payment service provider;

(c) represents the following information–

(i) name of the issuer of the form of identification;

(ii) the name of the payment service provider to whom the certificate is issued; and

(iii) the registration number and competent authority of the payment service provider to whom the certificate is issued; and

(d) is revoked where the payment service provider ceases to be authorised or registered or it would be inconsistent with its authorisation to carry on the relevant payment services.

(10) In this Article, the "eIDAS Regulation" means Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust

services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as it forms part of the law of Gibraltar.

Security of communication session.

35.(1) Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers must ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

(2) Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers must keep the access sessions offered by account servicing payment service providers as short as possible and they must actively terminate any such session as soon as the requested action has been completed.

(3) When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers must ensure that those sessions are securely linked to relevant sessions established with the payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

(4) Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider must contain unambiguous references to each of the following items–

(a) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service user or users;

(b) for payment initiation services, the uniquely identified payment transaction initiated;

(c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.

(5) Account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments must ensure that where they communicate personalised security credentials and authentication codes, these are not readable, directly or indirectly, by any staff at any time.

(6) In case of loss of confidentiality of personalised security credentials under their sphere of competence, those providers must inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials.

Data exchanges.

36.(1) Account servicing payment service providers must comply with each of the following requirements–

(a) they must provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;

(b) they must, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

(c) they must, upon request, immediately provide payment service providers with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.

(2) In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider must send a notification message to the payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error.

(3) Where the account servicing payment service provider offers a dedicated interface in accordance with Article 32, the interface must provide for notification messages concerning unexpected events or errors to be communicated by any payment service provider that detects the event or error to the other payment service providers participating in the communication session.

(4) Account information service providers must have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent.

(5) Payment initiation service providers must provide account servicing payment service providers with the same information as requested from the payment service user when initiating the payment transaction directly.

(6) Account information service providers must be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances–

(a) whenever the payment service user is actively requesting such information;

(b) where the payment service user does not actively request such information, no more than four times in a 24-hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user's consent.

(7) An account information service provider may only access information in the circumstances described in paragraph (6)(b) 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.

SCHEDULE

ETV	Reference Fraud Rate (%) for: Remote electronic card-based payments	Remote electronic credit transfers
£440	0.01	0.005
£220	0.06	0.01
£85	0.13	0.015