STATUTORY INSTRUMENTS

2017 No. 752

The Payment Services Regulations 2017

PART 7

Rights and Obligations in Relation to the Provision of Payment Services

Authorisation of payment transactions

Consent and withdrawal of consent

67.—(1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—

(a) the execution of the payment transaction; or

(b) the execution of a series of payment transactions of which that payment transaction forms part.

(2) Such consent—

(a) may be given before or, if agreed between the payer and its payment service provider, after the execution of the payment transaction;

(b) must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider; and

(c) may be given via the payee or a payment initiation service provider.

(3) The payer may withdraw its consent to a payment transaction at any time before the point at which the payment order can no longer be revoked under regulation 83 (revocation of a payment order).

(4) Subject to regulation 83(3) to (5), the payer may withdraw its consent to the execution of a series of payment transactions at any time with the effect that any future payment transactions are not regarded as authorised for the purposes of this Part.

Confirmation of availability of funds for card-based payment transactions

68.—(1) This regulation does not apply to payment transactions initiated through card-based payment instruments on which electronic money is stored.

(2) Where the conditions in paragraph (3) are met, a payment service provider which issues card-based payment instruments may request that an account servicing payment service provider confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer.

(3) The conditions are that—

(a) the payer has given explicit consent to the payment service provider to request the confirmation;

(b) the payer has initiated a payment transaction for the amount in question using a card-based payment instrument issued by the payment service provider making the request;

(c) the payment service provider making the request complies, for each request, with the authentication and secure communication requirements set out in the **[**F1technical standards made under regulation 106A**]** in its communications with the account servicing payment service provider.

(4) If the conditions in paragraph (5) are met, an account servicing payment service provider which receives a request under paragraph (2) must provide the requested confirmation, in the form of a 'yes' or 'no' answer, to the requesting payment service provider immediately.

(5) The conditions are that—

(a) the payment account is accessible online when the account servicing payment service provider receives the request; and

(b) before the account servicing payment service provider receives the first request under paragraph (2) from the requesting payment service provider in relation to the payer's payment account, the payer has given the account servicing payment service provider explicit consent to provide confirmation in response to such requests by that payment service provider.

(6) If the payer so requests, the account servicing payment service provider must also inform the payer of the payment service provider which made the request under paragraph (2) and the answer provided under paragraph (4).

(7) An account servicing payment service provider must not—

(a) include with a confirmation provided under paragraph (4) a statement of the account balance; or

(b) block funds on a payer's payment account as a result of a request under paragraph (2).

(8) The payment service provider which makes a request under paragraph (2) must not—

(a) store any confirmation received under paragraph (4); or

(b) use the confirmation received for a purpose other than the execution of the card-based payment transaction for which the request was made.

F1 Words in reg. 68(3)(c) substituted (31.12.2020) by The Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 (S.I. 2018/1201), reg. 1(3), **Sch. 2 para. 40** (with reg. 4, Sch. 3 Pt. 2) (as amended by S.I. 2020/56, regs. 1, 8); 2020 c. 1, Sch. 5 para. 1(1)

Access to payment accounts for payment initiation services

69.—(1) This regulation applies only in relation to a payment account which is accessible online.

(2) Where a payer gives explicit consent in accordance with regulation 67 (consent and withdrawal of consent) for a payment to be executed through a payment initiation service provider, the payer's account servicing payment service provider must—

(a) communicate securely with the payment initiation service provider in accordance with the **[**F2technical standards made under regulation 106A**]**;

(b) immediately after receipt of the payment order from the payment initiation service provider, provide or make available to the payment initiation service provider all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction;

(c) treat the payment order in the same way as a payment order received directly from the payer, in particular in terms of timing, priority or charges, unless the account servicing payment service provider has objective reasons for treating the payment order differently;

(d) not require the payment initiation service provider to enter into a contract before complying with the preceding sub-paragraphs.

(3) A payment initiation service provider must—

(a) not hold a payer's funds in connection with the provision of the payment initiation service at any time;

(b) ensure that a payer's personalised security credentials are—

(i) not accessible to other parties, with the exception of the issuer of the credentials; and

(ii) transmitted through safe and efficient channels;

(c) ensure that any other information about a payer is not provided to any person except a payee, and is provided to the payee only with the payer's explicit consent;

(d) each time it initiates a payment order, identify itself to the account servicing payment service provider and communicate with the account servicing payment service provider, the payer and the payee in a secure way in accordance with the **[**[F3]technical standards made under regulation 106A**]**;

(e) not store sensitive payment data of the payment service user;

(f) not request any information from a payer except information required to provide the payment initiation service;

(g) not use, access or store any information for any purpose except for the provision of a payment initiation service explicitly requested by a payer;

(h) not change the amount, the payee or any other feature of a transaction notified to it by the payer.

F2 Words in reg. 69(2)(a) substituted (31.12.2020) by The Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 (S.I. 2018/1201), reg. 1(3), **Sch. 2 para. 41** (with reg. 4, Sch. 3 Pt. 2) (as amended by S.I. 2020/56, regs. 1, 8); 2020 c. 1, Sch. 5 para. 1(1)

F3 Words in reg. 69(3)(d) substituted (31.12.2020) by The Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 (S.I. 2018/1201), reg. 1(3), **Sch. 2 para. 41** (with reg. 4, Sch. 3 Pt. 2) (as amended by S.I. 2020/56, regs. 1, 8); 2020 c. 1, Sch. 5 para. 1(1)

Access to payment accounts for account information services

70.—(1) This regulation applies only in relation to a payment account which is accessible online.

(2) Where a payment service user uses an account information service, the payment service user's account servicing payment service provider must—

(a) communicate securely with the account information service provider in accordance with the **[**[F4]technical standards made under regulation 106A**]**;

(b) treat a data request from the account information service provider in the same way as a data request received directly from the payer, unless the account servicing payment service provider has objective reasons for treating the request differently;

(c) not require the account information service provider to enter into a contract before complying with the preceding sub-paragraphs.

(3) An account information service provider must—

(a) not provide account information services without the payment service user's explicit consent;

(b) ensure that the payment service user's personalised security credentials are—

(i) not accessible to other parties, with the exception of the issuer of the credentials; and

(ii) transmitted through safe and efficient channels;

(c) for each communication session, identify itself to the account servicing payment service provider and communicate securely with the account servicing payment service provider and the payment service user in accordance with the **[**F5technical standards made under regulation 106A**]**;

(d) not access any information other than information from designated payment accounts and associated payment transactions;

(e) not request sensitive payment data linked to the payment accounts accessed;

(f) not use, access or store any information for any purpose except for the provision of the account information service explicitly requested by the payment service user.

F4 Words in reg. 70(2)(a) substituted (31.12.2020) by The Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 (S.I. 2018/1201), reg. 1(3), **Sch. 2 para. 42** (with reg. 4, Sch. 3 Pt. 2) (as amended by S.I. 2020/56, regs. 1, 8); 2020 c. 1, Sch. 5 para. 1(1)

F5 Words in reg. 70(3)(c) substituted (31.12.2020) by The Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 (S.I. 2018/1201), reg. 1(3), **Sch. 2 para. 42** (with reg. 4, Sch. 3 Pt. 2) (as amended by S.I. 2020/56, regs. 1, 8); 2020 c. 1, Sch. 5 para. 1(1)

Limits on the use of payment instruments and access to payment accounts

71.—(1) Where a specific payment instrument is used for the purpose of giving consent to the execution of a payment transaction, the payer and its payment service provider may agree on spending limits for any payment transactions executed through that payment instrument.

(2) A framework contract may provide for the payment service provider to have the right to stop the use of a payment instrument on reasonable grounds relating to—

(a) the security of the payment instrument;

(b) the suspected unauthorised or fraudulent use of the payment instrument; or

(c) in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.

(3) The payment service provider must, in the manner agreed between the payment service provider and the payer and before carrying out any measures to stop the use of the payment instrument—

(a) inform the payer that it intends to stop the use of the payment instrument; and

(b) give its reasons for doing so.

(4) Where the payment service provider is unable to inform the payer in accordance with paragraph (3) before carrying out any measures to stop the use of the payment instrument, it must do so immediately after.

(5) Paragraphs (3) and (4) do not apply where provision of the information in accordance with paragraph (3) would compromise reasonable security measures or is otherwise unlawful.

(6) The payment service provider must allow the use of the payment instrument or replace it with a new payment instrument as soon as practicable after the reasons for stopping its use cease to exist.

(7) An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for reasonably justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction.

(8) If an account servicing payment service provider denies access to a payment account under paragraph (7)—

(a) the account servicing payment service provider must notify the payment service user of the denial of access and the reason for the denial of access, in the form agreed with the payment service user;

(b) the notification under sub-paragraph (a) must be provided before the denial of access if possible, or otherwise immediately after the denial of access;

(c) the account servicing payment service provider must immediately report the incident to the FCA in such form as the FCA may direct, and such report must include the details of the case and the reasons for taking action;

(d) the account servicing payment service provider must restore access to the account once the reasons for denying access no longer justify such denial of access.

(9) Paragraph (8)(a) and (b) do not apply if notifying the payment service user—

(a) would compromise reasonably justified security reasons; or

(b) is unlawful.

(10) When the FCA receives a report under paragraph (8)(c), it must assess the case and take such measures as it considers appropriate.

Obligations of the payment service user in relation to payment instruments and personalised security credentials

72.—(1) A payment service user to whom a payment instrument has been issued must—

(a) use the payment instrument in accordance with the terms and conditions governing its issue and use; and

(b) notify the payment service provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) Paragraph (1)(a) applies only in relation to terms and conditions that are objective, non-discriminatory and proportionate.

(3) The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service.

Obligations of the payment service provider in relation to payment instruments

73.—(1) A payment service provider issuing a payment instrument must—

(a) ensure that the personalised security credentials are not accessible to persons other than the payment service user to whom the payment instrument has been issued;

(b) not send an unsolicited payment instrument, except where a payment instrument already issued to a payment service user is to be replaced;

(c) ensure that appropriate means are available at all times to enable the payment service user to notify the payment service provider in accordance with regulation 72(1)(b) (notification of loss or unauthorised use of payment instrument) or to request that, in accordance with regulation 71(6), the use of the payment instrument is no longer stopped;

(d) on request, provide the payment service user at any time during a period of 18 months after the alleged date of notification under regulation 72(1)(b) with the means to prove that such notification to the payment service provider was made;

(e) provide the payment service user with an option to make a notification under regulation 72(1)(b) free of charge, and ensure that any costs charged are directly attributed to the replacement of the payment instrument;

(f) prevent any use of the payment instrument once notification has been made under regulation 72(1)(b).

(2) The payment service provider bears the risk of sending to the payment service user a payment instrument or any personalised security credentials relating to it.

Notification and rectification of unauthorised or incorrectly executed payment transactions

74.—(1) A payment service user is entitled to redress under regulation 76, 91, 92, 93 or 94 (liability for unauthorised transactions, non-execution or defective or late execution of transactions, or charges and interest), only if it notifies the payment service provider without undue delay, and in any event no later than 13 months after the debit date, on becoming aware of any unauthorised or incorrectly executed payment transaction.

(2) Where the payment service provider has failed to provide or make available information concerning the payment transaction in accordance with Part 6 of these Regulations (information requirements for payment services), the payment service user is entitled to redress under the regulations referred to in paragraph (1) notwithstanding that the payment service user has failed to notify the payment service provider as mentioned in that paragraph.

Evidence on authentication and execution of payment transactions

75.—(1) Where a payment service user—

(a) denies having authorised an executed payment transaction; or

(b) claims that a payment transaction has not been correctly executed,

it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency in the service provided by the payment service provider.

(2) If a payment transaction was initiated through a payment initiation service provider, it is for the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment initiation service.

(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including a payment initiation service provider where appropriate, is not in itself necessarily sufficient to prove either that—

(a) the payment transaction was authorised by the payer; or

(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72 (user's obligations in relation to payment instruments and personalised security credentials).

(4) If a payment service provider, including a payment initiation service provider where appropriate, claims that a payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72, the payment service provider must provide supporting evidence to the payer.

Payment service provider's liability for unauthorised payment transactions

76.—(1) Subject to regulations 74 and 75, where an executed payment transaction was not authorised in accordance with regulation 67 (consent and withdrawal of consent), the payment service provider must—

(a) refund the amount of the unauthorised payment transaction to the payer; and

(b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place.

(2) The payment service provider must provide a refund under paragraph (1)(a) as soon as practicable, and in any event no later than the end of the business day following the day on which it becomes aware of the unauthorised transaction.

(3) Paragraph (2) does not apply where the payment service provider has reasonable grounds to suspect fraudulent behaviour by the payment service user and notifies a person mentioned in section 333A(2) of the Proceeds of Crime Act 2002 (tipping off: regulated sector) [M1] of those grounds in writing.

(4) When crediting a payment account under paragraph (1)(b), a payment service provider must ensure that the credit value date is no later than the date on which the amount of the unauthorised payment transaction was debited.

(5) Where an unauthorised payment transaction was initiated through a payment initiation service provider—

(a) the account servicing payment service provider must comply with paragraph (1);

(b) if the payment initiation service provider is liable for the unauthorised payment transaction (in relation to which see regulation 75(2)) the payment initiation service provider must, on the request of the account servicing payment service provider, compensate the account servicing payment service provider immediately for the losses incurred or sums paid as a result of complying with paragraph (1), including the amount of the unauthorised transaction.

Marginal Citations

M1 2002 c. 29. Section 333A was inserted by S.I. 2007/3398 and amended by paragraph 132 of Schedule 8 to the Crime and Courts Act 2013 (c. 22).

Payer or payee's liability for unauthorised payment transactions

77.—(1) Subject to paragraphs (2), (3) and (4), a payment service provider which is liable under regulation 76(1) may require that the payer is liable up to a maximum of £35 for any losses incurred in respect of unauthorised payment transactions arising from the use of a lost or stolen payment instrument, or from the misappropriation of a payment instrument.

(2) Paragraph (1) does not apply if—

(a) the loss, theft or misappropriation of the payment instrument was not detectable by the payer prior to the payment, except where the payer acted fraudulently; or

(b) the loss was caused by acts or omissions of an employee, agent or branch of a payment service provider or of an entity which carried out activities on behalf of the payment service provider.

(3) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—

(a) has acted fraudulently; or

(b) has with intent or gross negligence failed to comply with regulation 72 (obligations of the payment service user in relation to payment instruments and personalised security credentials).

(4) Except where the payer has acted fraudulently, the payer is not liable for any losses incurred in respect of an unauthorised payment transaction—

(a) arising after notification under regulation 72(1)(b);

(b) where the payment service provider has failed at any time to provide, in accordance with regulation 73(1)(c) (obligations of the payment service provider in relation to payment instruments), appropriate means for notification;

(c) where regulation 100 (authentication) requires the application of strong customer authentication, but the payer's payment service provider does not require strong customer authentication; or

(d) where the payment instrument has been used in connection with a distance contract (other than an excepted contract).

(5) In paragraph (4)(d)—

"distance contract" means a distance contract as defined by regulation 5 of the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (other definitions) [M2];

"excepted contract" means a contract that—

(a) falls to any extent within regulation 6(1) of those Regulations (limits of application: general); or

(b) falls within regulation 6(2) of those Regulations.

(6) Where regulation 100 requires the application of strong customer authentication, but the payee or the payee's payment service provider does not accept strong customer authentication, the payee or the payee's payment service provider, or both (as the case may be), must compensate the payer's payment service provider for the losses incurred or sums paid as a result of complying with regulation 76(1).

Marginal Citations

M2 S.I. 2013/3134. Regulation 6 was amended by S.I. 2015/1629.

Payment transactions where the transaction amount is not known in advance

78. Where a card-based payment transaction is initiated by or through the payee and the amount of the transaction is not known when the payer authorises the transaction—

(a) the payer's payment service provider may not block funds on the payer's payment account unless the payer has authorised the exact amount of the funds to be blocked; and

(b) the payer's payment service provider must release the blocked funds without undue delay after becoming aware of the amount of the payment transaction, and in any event immediately after receipt of the payment order.

Refunds for payment transactions initiated by or through a payee

79.—(1) Where the conditions in paragraph (2) and the requirement in regulation 80(1) are satisfied, the payer is entitled to a refund from its payment service provider of the full amount of any authorised payment transaction initiated by or through the payee.

(2) The conditions are that—

(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was given in accordance with regulation 67 (consent and withdrawal of consent); and

(b) the amount of the payment transaction exceeded the amount that the payer could reasonably have expected taking into account the payer's previous spending pattern, the conditions of the framework contract and the circumstances of the case.

(3) The payer is entitled to an unconditional refund from its payment service provider of the full amount of any direct debit transactions of the type referred to in Article 1 of Regulation (EU) 260/2012 of the European Parliament and of the Council of 14th March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 [M3].

(4) When crediting a payment account under paragraph (1), a payment service provider must ensure that the credit value date is no later than the date on which the amount of the unauthorised payment transaction was debited.

(5) For the purposes of paragraph (2)(b), the payer cannot rely on currency exchange fluctuations where the reference exchange rate provided under regulation 43(2)(d) or paragraph 3(b) of Schedule 4 was applied.

(6) The payer and payment service provider may agree in the framework contract that the right to a refund does not apply where—

(a) the payer has given consent directly to the payment service provider for the payment transaction to be executed; and

(b) if applicable, information on the payment transaction was provided or made available in an agreed manner to the payer for at least four weeks before the due date by the payment service provider or by the payee.

Marginal Citations

M3 OJ L 94, 30.3.2012, p.22.

Requests for refunds for payment transactions initiated by or through a payee

80.—(1) The payer must request a refund under regulation 79 from its payment service provider within 8 weeks from the date on which the funds were debited.

(2) The payment service provider may require the payer to provide such information as is reasonably necessary to prove that the conditions in regulation 79(2) are satisfied.

(3) The payment service provider must either—

(a) refund the full amount of the payment transaction; or

(b) provide justification for refusing to refund the payment transaction, indicating the bodies to which the payer may refer the matter if the payer does not accept the justification provided.

(4) Any refund or justification for refusing a refund must be provided within 10 business days of receiving a request for a refund or, where applicable, within 10 business days of receiving any further information requested under paragraph (2).

(5) If the payment service provider requires further information under paragraph (2), it may not refuse the refund until it has received further information from the payer.

Changes to legislation:
The Payment Services Regulations 2017, Cross Heading: Authorisation of payment transactions is up to date with all changes known to be in force on or before 19 March 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.
View outstanding changes

Changes and effects yet to be applied to :

– Regulations power to amend conferred by 2021 c. 22 s. 23