FINANSTILSYNET
The Financial Supervisory Authority of Norway

Translation as of September 2021

This translation is for information purposes only. Legal authenticity remains with the official Norwegian version as published in Norsk Lovtidend.

Regulations on payment services systems

Regulations of 15 February 2019 no. 152 (last amended 1 July 2021)

Legal basis: Laid down by the Ministry of Finance payment systems on 15 February 2019 in pursuance of Act of 17 December 1999 No. 1 on payment systems etc., Section 3-3, first subsection, second sentence and Act of 10 April 2015 No. 17 on financial institutions and financial groups (Financial Institutions Act), Section 2-10a (5). Amended by regulations of 31 May 2021 No. 1715 (entered into force on 1 July 2021).

Section 1. ***Scope of application***

These regulations apply to banks, credit institutions, e-money institutions, payment institutions, account information service providers and branches of such institutions headquartered in another EEA state, cf. Section 2.3 of the Financial Institutions Act. The regulations nevertheless do not apply to payment institutions with limited authorisation, cf. Section 2-10 (4) of the Financial Institutions Act.

Section 2. ***Risk assessment and compliance with the legislation***

Payment service providers shall implement risk and vulnerability analyses before a new payment service is launched and in connection with incidents or changes with an impact on the level of security.

Payment service providers shall have systems and control mechanisms in place for operational and security risks related to the provision of payment services, as well as effective procedures for handling incidents, including serious operational and security incidents. The systems shall ensure compliance with legislation, agreements and internal procedures. Data traffic in electronic payment services shall be monitored to ensure an adequate level of security and be able to identify and prevent unauthorised use of the service.

Payment service providers shall at least annually present an overall assessment to Finanstilsynet of the operational and security risks associated with the provider's payment services, as well as whether the measures taken by the provider are adequate.

Payment service providers shall at least annually report statistics on fraud related to its payment services to Finanstilsynet in the manner specified by Finanstilsynet.

Section 3. ***Notification of incidents***

If incidents as specified in regulations of 21 May 2003 No. 630 on use of information and communication technology (ICT), Section 9, third subsection have or may have an impact on the payment service users' financial interests, the payment service provider shall notify users of the incident without undue delay. The notification should specify measures that can be implemented by the user.

Section 4. ***Requirements for the safe provision of payment services***

Payment service providers shall, on the basis of the risk and vulnerability analyses, establish measures to ensure the necessary confidentiality, integrity and availability of the services. Compliance with current national standards and internationally recognised standards shall be ensured.

The payment service provider is responsible for ensuring that the entire service (end to end) is protected by logical and physical safeguards.

Section 5. ***Strong customer authentication requirements***

A payment service provider shall use strong customer authentication when a payer

a) accesses its payment account online,
b) initiates an electronic payment transaction, or
c) carries out any action which may imply a risk of fraud or other abuses.

With respect to transactions mentioned in the first subsection, letter b, the payment service provider shall, for electronic remote payment transactions, apply strong customer authentication that links the transaction to a specific amount and a specific payee.

'Strong customer authentication' means a solution based on the use of two or more elements that are independent in that the breach of one does not compromise the reliability of the other elements.

The payment service provider shall introduce appropriate measures to protect the user's personalised security credentials. Furthermore, the institution shall ensure that the customer can adequately protect its authentication credentials, and establish solutions that enable the customer to block further use of the authentication credentials.

The account servicing payment service provider (ASPSP) shall authorise payment initiation service providers (PISPs) and account information service providers (AISPs) to make use of the authentication procedures that the account servicing payment service provider has made available to the user.

Section 6. ***Payment initiation services***

In connection with payment initiation services, the payment initiation service provider shall

a) not hold at any time the payer's funds
b) not modify the payee, the amount or any other feature of the transaction
c) identify itself towards the account servicing payment service provider of the payer every time a payment is initiated

d) communicate with the account servicing payment service provider, the payer and the payee in a secure way
e) ensure that the personalised security credentials (authentication credentials) of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted through safe and efficient channels
f) not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer
g) not store sensitive payment data of the payment service user
h) not request from the payment service user any data other than those necessary to provide the payment initiation service
i) ensure that any other information about the payment service user, obtained when providing payment services, is only provided to the payee and only with the payment service user's explicit consent

The payment initiation service provider shall make the payment reference available to the account servicing payment service provider when initiating a payment order.

Section 7. ***Account information services***

In connection with account information services, the account information service provider shall

a) identify itself towards the account servicing payment service provider of the payer for each communication session
b) communicate securely with the account information service provider and the user
c) ensure that the personalised security credentials (authentication credentials) of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted through safe and efficient channels
d) access only the information from designated payment accounts and associated payment transactions
e) not request sensitive payment data linked to the payment account
f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user

Section 8. ***Duties of the account servicing payment service provider***

In accordance with the provisions of the regulations on payment services, Section 5 (1), in pursuance of the Financial Contracts Act, Section 9a, the execution of a payment initiation service or account information service cannot be made conditional on on the existence of an agreement between the account servicing payment service provider and the payment initiation service provider or the account information service provider.

The account servicing payment service provider shall give the payment initiation service provider the necessary access to the user's online payment accounts, unless there are objectively justified and documented reasons to believe that the required authorisation for executing payment initiation or account information services is missing. The account servicing payment service provider shall promptly notify Finanstilsynet if access has been denied for the payment initiation

service provider or the account information service provider. The notification should include the reasons why access has been denied.

The account servicing payment service provider shall treat payment orders transmitted by a payer through a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges, vis-à-vis payment orders initiated directly by the payer.

The account servicing payment service provider shall treat requests for information transmitted through the services of an account information service provider without any discrimination other than for objective reasons.

The account servicing payment service provider shall immediately after receipt of the payment order from a payment initiation service provider, make available all information on the initiation and execution of the payment transaction to the service provider.

The account servicing payment service provider shall communicate securely with the payment initiation service providers and account information service providers.

Section 9. ***Card-based payment transactions***

The account servicing payment service provider shall, upon the request of a payment service provider issuing card-based payment instruments, immediately confirm whether an amount necessary for the execution of the transaction is available on the payment account, provided that the account is accessible online. This applies only if the payment service user has given explicit consent to the account servicing payment service provider to respond to requests from another payment service provider issuing card-based payment instruments to confirm that the amount corresponding to a specific card-based payment transaction is available on the payer's payment account.

The account servicing payment service provider's response to whether the amount necessary is available on the account shall be an affirmative 'yes' or a negative 'no'. The request shall not allow for the blocking of funds on the payer's payment account.

At the request of the payment service user, the account servicing payment service provider shall always communicate to the payer the identification of the payment service provider who has requested such confirmation and the answer provided.

The payment service provider shall identify itself towards the account servicing payment service provider before each confirmation request, and securely communicate with the account servicing payment service provider.

The provisions of this section do not apply to card-based payment instruments on which electronic money is stored.

Section 10. ***Acceptance of card-based electronic money instruments issued outside the EEA***

Acquirers defined as obliged entities pursuant to Section 4 of the Anti-Money Laundering Act shall only accept payment transactions using electronic money instruments issued outside the EU/EEA when these have been issued on terms and conditions that are at least as strict as set out in

Section 4-2, first subsection, letter b and second subsection of the Anti-Money Laundering Regulations.

Section 11. ***Access to the user's security credentials***

Payment service providers shall ensure that the user's personalised security credentials for electronic authentication and signature are not available to anyone other than the user and the issuer when the authentication or signature provides access to online services from the public sector covered by rules corresponding to the European Parliament and Council Regulation (EU) No. 910/2014.

Section 12. ***Entry into force***

The regulations enter into force on 1 April 2019. As of the same date, the regulations of 17 December 2015 No. 1731 on payment services systems will be revoked.

As of 14 September 2019, rules in accordance with Commission Delegated Regulation (EU) 2018/389 will also apply.