Finansinspektionen's Regulatory Code

Publisher: Finansinspektionen, Sweden, www.fi.se
ISSN 1102-7460

This translation is furnished solely for information purposes. Only the printed version of the regulation in Swedish applies for the application of the law.

Finansinspektionen's regulations regarding activities of payment service providers;

FFFS 2018:4
Published on 23 April 2018

decided on 17 April 2018.

Finansinspektionen prescribes[1] the following pursuant to Section 5, points 8–16 of the Payment Services Ordinance (2010:1008).

Chapter 1 Scope and definitions

Scope

Section 1 These regulations apply to the following payment service providers that provide payment services in Sweden

– credit institutions,
– payment institutions,
– registered payment service providers,
– institutions for electronic money, and
– registered issuer of electronic money.

The provisions in Chapter 6, Section 2 also apply to foreign payment service providers with branches in Sweden.

Section 2 The provisions in Chapter 4 only apply to payment service providers that provide payment accounts to consumers where the consumer is able to do the minimum of

1. deposit funds into a payment account,
2. withdraw cash from a payment account, and
3. make and receive payment transactions to and from a third party.

Definitions

Section 3 In these regulations, terms and expressions have the same meaning as in the Payment Services Act (2010:751). In addition, the following definitions apply:

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, and Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

accuracy: the information is not altered without authorisation, by mistake or as a result of an operational disturbance.

payment-related services: all business activities referred to in Article 4(3) of the Payment Services Directive and all technical support required in order to provide payment services correctly,

integrity: an assurance that a company's assets, including data, are accurate and complete,

confidentiality: the circumstance that information is not made available or disclosed to unauthorised persons,

continuity: the processes, information and assets an organisation requires in order to provide payment-related services are fully available and function at predetermined acceptable levels,

receiving payment service provider: the payment service provider that a consumer wished to switch a payment account to,

operational incidents or security incidents: an individual event or a series of connected events that have not been planned by the payment service provider that have or will probably have a detrimental impact on payment-related services in terms of integrity, availability, confidentiality, accuracy and continuity,

risk appetite: level and orientation of the risks that the company can accept in the pursuit of its strategic goals,

security risk: the risk that insufficient or defective internal processes or external events, including cyber-attacks or insufficient physical security, have a detrimental impact on the availability, integrity or confidentiality of
– information and communications technology systems, or
– the information that is used to provide payment services,

availability: payment-related services are available and can be used by payment service users.

transferring payment service provider: the payment service provider that a customer wishes to switch a payment account from.

Chapter 2 Payment service providers' handling of complaints

Section 1 A payment service provider shall have appropriate and effective procedures for handling and responding to a payment service user's complaints about operations in the countries in which the provider provides payment services.

The payment service provider shall respond to the complaint in a language that is an official language of the country where the payment service is provided, and supply this to the payment service user in paper form, unless the provider and the user have agreed otherwise.

Section 2 A payment service provider shall respond to a payment service user's complaint within 15 business days of the day the complaint is received.

If there are specific grounds that prevent the payment service provider from supplying a response within the time stated in the first paragraph, the provider shall

respond within 35 business days of the day the complaint is received. In such cases, the provider shall inform the payment service user within the time stated in the first paragraph of when the response will be supplied and of the specific grounds that have resulted in the delay.

Chapter 3 Information about services, charges and rights

Information for consumers

Section 1 The information that a payment service provider shall make available to consumers in accordance with Chapter 4 a, Section 5, second paragraph of the Payment Services Act (2010:751) shall be found on the payment service provider's website. The same applies to the brochure about consumer rights that is found on Finansinspektionen's website.

The information as per the first paragraph shall also be found in paper form at branches, agents and in those of the provider's premises that are accessible by consumers.

Section 2 If the information as per Section 1 is available on a payment service provider's website, the text shall also be made available for screen readers. Information that can be found in physical premises shall also be made available in Braille or another format that makes it accessible to people with disabilities.

Chapter 4 Procedures for switching payment accounts

Requirements for procedures for switching payment accounts

Section 1 The procedures for switching payment accounts that a payment service provider shall have pursuant to Chapter 4 a, Section 6 of the Payment Services Act (2010:751) shall, as a minimum, fulfil the requirements set out in Sections 3–10.

Section 2 The provisions in Sections 3–10 shall apply from the point at which the receiving payment service provider has opened the new payment account to which the switch is to take place.

Obligations for the receiving payment service provider

Section 3 A switch of payment account shall begin with all those who are holders of the payment account directing the receiving payment service provider in writing to conduct the switch and providing instructions as to how this is to be done. The receiving payment service provider shall ensure that it is possible for a consumer to do so in Swedish, unless the payment service provider and the consumer agree otherwise.

Section 4 The receiving payment service provider shall ensure that the consumer has the opportunity to provide instructions concerning which direct debit mandates, incoming payments and standing orders associated with the old payment account are to be associated with the new one.

The payment service provider shall also ensure that the consumer is able to provide instructions to the effect that any remaining balance in the payment account at the

transferring payment service provider is to be transferred, and that the payment account is to then be closed.

Section 5 The receiving payment service provider shall ensure that the consumer has the opportunity to decide the date on which the switch of payment account is to be initiated.

Section 6 The receiving payment service provider, provided there is no agreement otherwise between the providers, shall send the directions and the instructions as per Sections 3 and 4 in Swedish to the transferring payment service provider, at the latest, one business day after the date determined in accordance with Section 5.

Section 7 The receiving payment service provider shall ensure that the direct debit mandates and standing orders that are listed in the instructions are associated with the new payment account within three days of the date determined in accordance with Section 5.

Section 8 If the consumer has directed the receiving payment service provider to close the payment account at the transferring payment service provider, or to transfer a remaining balance, the receiving payment service provider shall inform the transferring payment service provider of how the remaining balance is to be transferred.

Section 9 Within three business days of the date determined in accordance with Section 5, the receiving payment service provider shall inform the consumer of the information required in order to make deposits into the payment account.

Obligations for the transferring payment service provider

Section 10 The transferring payment service provider shall terminate standing orders and direct debits within three business days of the date the provider has received the directions to terminate such.

If remaining funds in the payment account at the transferring payment service provider are to be transferred, or if the payment account is to be closed, the remaining balance shall be transferred within three business days of the date the consumer's directions have been received. The transferring payment service provider shall close the payment account within three business days of the date the provider has received the consumer's directions to close the account.

Chapter 5 System for operational risks and security risks

Section 1 The system that a payment service provider shall have pursuant to Chapter 5 b, Section 1 of the Payment Services Act (2010:751) shall be tailored to the provider's operations and consist of a framework of documented measures that manage or reduce the risk of operational incidents or security incidents occurring. Within the scope of this system, the provider shall, as a minimum

1. define and allocate the accountability functions that the supplier deems necessary in order to implement the security measures,

2. establish processes, procedures and systems for identifying, measuring, monitoring and managing the risks associated with the supplier's payment services business.

3. conduct a risk assessment of the payment services and draw up a description of the security measures that will protect payment service users from the risks that have been identified, including fraud and illegal use of sensitive information and personal data,

4. have an internal level-based model for managing and controlling risks in the payment services business,

5. draw up a description of how the provider ensures that the operational risks and security risks are managed when it outsources some aspect of the payment services business to another party,

6. establish a risk appetite for the payment services business and take stock of, classify and risk assess business functions, processes and assets that are deemed to be critical to operations,

7. draw up security measures that manage confidentiality, integrity and availability of computer and IT systems, as well as physical security and access control,

8. ensure that operations are monitored in order to identify unplanned events that lead to operational or security-related incidents and manage, follow up and report these incidents,

9. draw up a plan for continuity management that encompasses a description of how operations are to be maintained in various scenarios and how the provider is to communicate in the event of an emergency, test the continuity plans annually and update them when necessary,

10. draw up and regularly test inspection procedures that ensure security measures are up to date and effective,

11. draw up a threat analysis for the payment services business and regularly train staff in how they are to use contingency plans, continuity plans and recovery plans and

12. draw up and, when necessary, implement processes and procedures for guiding and informing payment service users about the security risks and error messages that are related to the payment services provided and payment service users' opportunities to deactivate specific payment functions.

Chapter 6 Information to Finansinspektionen

Overall assessment of operational risks, security risks and measures

Section 1 A payment service provider shall submit a report to Finansinspektionen each year that contains a current overall assessment of the operational risks and security risks associated with the payment services the provider provides and a description of the security measures the provider has implemented in order to manage these risks. The report shall also contain an assessment of the suitability of the security measures the provider has implemented in order to manage these risks.

Finansinspektionen shall have received the report no later than 21 February.

Statistical data concerning fraudulent proceedings

Section 2 A payment service provider shall submit statistical data to Finansinspektionen twice per year concerning fraudulent proceedings that have taken place in conjunction with the use of payment services. This data shall include

1. total transaction volume,

2. total transaction volume related to fraudulent proceedings, and

3. an account of data as per 1 and 2 distributed by

a) type of payment service,
b) authentication method in question
c) type of fraudulent proceeding, and
d) geographical location where the transaction took place.

This data shall refer to the preceding six calendar months and be divided up by quarter. The provider shall submit the data by using the reporting forms that can be found on Finansinspektionen's website. Finansinspektionen shall have received the data no later than 21 February and 21 August, respectively.

Registered payment service providers and registered issuers of electronic money shall submit data as per the first paragraph only once per year, no later than 21 February, by using the reporting forms that can be found on Finansinspektionen's website. The data shall refer to the preceding calendar year and be divided up by quarter.

Section 3 Data as per Section 2 shall encompass fraudulent proceedings that are related to completed payment transactions that

1. have not been authorised by the payer
2. the payer denies they have authorised, or
3. have been accomplished through the payer being manipulated.

Serious operational incidents or security incidents

Section 4 A payment service provider shall report to Finansinspektionen if a serious operational incident or a security incident has arisen in its operations. When reporting, the provider shall use the serious incidents form that is available on Finansinspektionen's website.

This information shall be submitted using sections A–C on the form, in the manner that is described in more detail on Finansinspektionen's website.

1. within four hours of the incident being detected (section A),
2. with updated information when this is available and no later than within three days of the information as per 1 having been received (section B), and
3. no later than two weeks after operations are functioning normally again (section C).

Section 5 A payment service provider shall inform their payment service users if a serious operational incident or security incident occurs that may have a detrimental impact on their financial interests. When a payment service provider informs payment service users, the following requirements shall be met:

1. The information shall also be available to the payment service user in a permanent medium after the occasion on which they were informed.

2. The payment service provider shall make the payment service user aware that there is information about a serious operational incident or security incident that may have a detrimental impact on the payment service user's financial interests.

3. When designing such a communication, the payment service provider shall take into account the importance of secure communication the origin of which the payment service user is able to check.

Information about charges for services

Section 6 A payment service provider that provides payment accounts with basic functions in accordance with Chapter 4 a, Section 2 of the Payment Services Act (2010:751) shall submit information to Finansinspektionen about the lowest charge the provider offers to all consumers for the services that appear on the list Finansinspektionen publishes of the most representative services linked to payment accounts in Sweden.

Section 7 Information as per Section 6 shall be submitted continually via Finansinspektionen's online service for continual reporting in the manner described in more detail there.

Section 8 Information as per Section 6 shall be submitted to Finansinspektionen no later than the same business day the charge starts being applied by the payment service provider.

Exemptions from application in certain cases

Section 9 Finansinspektionen may decide on exemptions from the provisions set out in Sections 1, 2, 4 and 6 if there are specific grounds to do so.

---

1. These regulations enter into force on 1 May 2018, at which point Finansinspektionen's regulations (FFFS 2017:1) regarding certain payment accounts shall be repealed.

2. Information as per Chapter 6, Section 2 shall be submitted for the first time no later than 21 August 2019 and refer to the period from 1 January 2019 to 30 June 2019, inclusive.

ERIK THEDÉEN

David Lothigius