FINANŠU UN KAPITĀLA TIRGUS KOMISIJA

KUNGU IELA 1 • RĪGA • LV-1050 • TĀLRUNIS +371 6777 4800 • E-PASTS FKTK@FKTK.LV • WWW.FKTK.LV

Riga, 14 July 2020

Regulations No 93
(Min.28, p. 13 of the Board of the Financial and Capital Market Commission)

Regulations on major incident reporting related to payment services

Issued in accordance with Article 104.[1] (1) Clause 4 of the Law on Payment Services and Electronic Money

I. General provisions

1. "Regulations on major incident reporting related to payment services" (hereinafter – the Regulations) shall be binding on Latvia-registered credit institutions, licensed payment institutions and licensed electronic money institutions (hereinafter – the payment service provider). The Regulations shall specify criteria for the classification of major operational or security incidents by the payment service provider as well as requirements and procedures they shall observe in reporting above incidents to the Financial and Capital Market Commission (hereinafter – the Commission).

2. The Regulations shall apply to all major operational and security incidents.

3. The Commission shall forward the reports received from the payment service provider to the European Banking Authority.

4. The Commission shall have the right to notify law enforcement authorities of the reports submitted by the payment service provider in cases specified in laws and regulations.

5. The payment service provider shall ensure that all obligations of the payment service provider related to reporting of operational or security incidents pursuant to the implementation of the Law on Payment Services and Electronic Money and processes are specified in its internal control system in order to comply with the requirements laid down in the Regulations.

II. Terms

6. Operational or security incident (hereinafter – an incident) – a singular event or a series of events unplanned by the payment service provider, which have or probably will have an adverse impact on the integrity, availability or confidentiality of payment-related services.

7. Integrity – accuracy, correctness and completeness of information and its handling methods.

8. Availability – the possibility to use services at the fixed location and defined time by the authorised persons.

9. Confidentiality – enabling access to information only by authorised persons.

III. Classification of major incidents

10. The payment service provider shall classify as major an incident that meets one or more criteria at the "higher impact level" or three or more criteria at the "lower impact level" as laid out in paragraph 11 hereof and pursuant to the assessment set out in the Regulations.

11. The payment service provider shall assess an incident against each individual criterion, determining whether the relevant thresholds specified in Table 1 are or will probably be reached before the incident is resolved.

Table 1 Criteria and their thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) and > EUR 100 000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) or > EUR 5 million
Payment service users affected	> 5000 un > 10% of the payment service provider's payment service users	> 50 000 or > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital *, EUR 200 000) or > EUR 5 million
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be imposed
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

* Tier 1 capital as defined in Article 25 of Regulation (EU) No 575/2013 of the European Parliament and of the Council, of 26 June 2013, on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

12. The payment service provider shall assess an incident against the criteria and their underlying indicators:

12.1. transactions affected – the total value of all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services – to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident.The previous year shall be taken as a reference period. If the payment service

provider does not consider this indicator to be representative (e.g. because of seasonality), more representative indicator shall be used providing underlying justification for this approach in the relevant field of Annex to the Regulations;

12.2. payment service users affected – their number both in absolute terms and as a percentage of the total number of payment service users, including all customers that have access to the payment service affected and that have suffered or will probably suffer the consequences of the incident. The payment service provider shall base estimations on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident. In case the payment service provider offers operational services to other payment service providers, it shall consider only its own payment service users (if any), and the payment service provider receiving the above operational services shall assess the incident in relation to their own payment service users. The total number of payment service users is the aggregated figure of payment service users that have been contractually bound at the time of the incident (or the most recent figure available) and who have access to the affected payment service regardless of their size or whether they are considered as active or passive payment service users;

12.3. service downtime – the period of time when the service will probably be unavailable for the payment service user or when the payment order cannot be executed by the payment service provider in the meaning of Article 1, paragraph 11 of the Law on Payment Services and Electronic Money. The payment service provider shall consider the period of time that any task, process or channel related to the provision of services is or will probably be unavailable. The service downtime shall be calculated from the moment the downtime starts, considering both the time intervals when they are open to the execution of services and closing hours and maintenance periods, where relevant and applicable. If it is impossible to determine when the downtime started, it shall be calculated from the moment the downtime is detected;

12.4. economic impact – monetary costs associated with the incident, taking into account both the absolute figure and, where applicable, the relative importance of these costs in relation to the size of the payment service provider (i.e. to the payment service provider's Tier 1 capital). The payment service provider shall consider both the costs that can be connected to the incident directly (already known) and those which are indirectly related to the incident (expected), as well as expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues;

12.5. high level of internal escalation – whether the management of the payment service provider has been or will probably be informed about the incident. The payment service provider shall assess whether the management is likely to be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident as a result of its impact on payment-related services and consider whether or not, as a result of this impact, a crisis mode has been or is likely to be triggered;

12.6. Other payment service providers or relevant infrastructures potentially affected – systemic implications that the incident will probably have, i.e. its potential to influence also other payment service providers, financial market infrastructures and/or card payment schemes. The payment service provider shall assess the impact of the incident on the financial market, assessing whether or not the incident has been affected or will probably affect other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the sound operation of the financial system as a whole. The payment service provider shall take into account various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or

external and whether or not the payment service provider has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member;

12.7. reputational impact – how the incident can undermine users' trust in the payment service provider itself and in the underlying payment service or the market as a whole.

13. The payment service provider shall use estimations if it does not have actual facts to support its judgement, regardless of whether or not a given threshold is or will probably reached before the incident is resolved.

14. The payment service provider shall carry out this assessment on a continuous basis during the lifetime of the incident to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major).

IV. Notification process

15. The payment service provider shall collect all relevant information, prepare report on an incident using the template provided in Annex to the Regulations and submit it to the Commission electronically (e-mail address mps.incidents@fktk.lv).

16. The payment service provider shall use the template provided in Annex to the Regulations to inform the Commission throughout the lifetime of the incident (i.e. to prepare initial, intermediate and final reports, as specified in paragraphs 21–27 hereof). The payment service provider shall fill out the template in an incremental manner, on a best effort basis, updating information that becomes available in the course of their internal investigation.

17. The payment service provider shall provide the Commission with any additional information, if available and deemed relevant for the Commission, by appending supplementary documentation to the standardised template as one or various annexes.

18. The payment service provider shall indicate the date for the next update, which has to be as soon as possible, but no later than three business days.

19. The payment service provider shall communicate to the Commission the possible failure to comply with the date indicated for the next update.

20. If the payment service provider is able to provide all the information necessary for the final report (i.e. section C of the template) within 4 hours from the moment the incident was detected, it shall provide information in its initial report related to the initial, last intermediate and final reports.

V. Initial report

21. The payment service provider shall submit an initial report (section A of the template) to the Commission within four hours from the moment a major incident is detected, or, where that is not possible, as soon as it is possible.

22. The payment service provider shall submit an initial report to the Commission when the previously non-major incident becomes a major incident.

VI. Intermediate report

23. The payment service provider shall submit intermediate reports (section B of the template) every time it considers that there is a relevant status update, and as a minimum by the date for the next update indicated in the previous report (either the initial report or the previous intermediate report).

24. The payment service provider, submitting additional intermediate reports, shall update the information already provided in sections A and B of the template when it becomes aware of new relevant information or significant changes since the previous notification.

25. In case the business activities are recovered back to normal before four hours have passed since the incident was detected, the payment service provider shall submit both the initial and intermediate reports simultaneously (i.e. filling out sections A and B of the template) by the four-hour deadline.

VII. Final report

26. The payment service provider shall submit the final report (section C of the template) when the root cause analysis has been conducted, regardless of whether or not mitigation measures have already been taken, within a maximum of ten business days after the business activities are recovered back to normal. The payment service provider shall contact the Commission before the deadline has lapsed, and if an extension of the deadline is needed, provide a justification for the delay, as well as new estimated date for the final report.

27. The payment service provider shall also submit the final report when as a result of the assessment of the incident it is established that the already reported incident no longer meets the criteria according to which it was recognised as major, and is not expected to fulfil the criteria before the incident is resolved. The payment service provider shall submit the final report as soon as this circumstance is detected, but no later than the estimated date for the next report. The payment service provider shall, in filling out section C of the template, tick the box "incident reclassified as non-major" and explain the reasons justifying this downgrading.

VIII. Closing provision

28. Upon these Regulations take effect the Regulations No 157 on Regulations on major incident reporting related to payment services of 26 September 2018 shall become null and void.

Chairwoman
Financial and Capital Market Commission S. Purgaile