**MNB identification number: P64**

**Completion instructions**

**Reporting of major operational or security incidents by the payment service provider**

### **I. General requirements**

1. For the purpose of the reporting requirement, operational and security incident means a single event or a series of linked events unplanned by the payment service provider which has a negative impact on the integrity, availability, confidentiality, authenticity and continuity of the payment services or on the technical support duties necessary for the rendering of those in adequate quality (hereinafter together: payment-related services), irrespective of the source (external/internal) and wilfulness (wilful/accidental). The reporting requirement also covers the situations and events as a result of which the operational or security incidents occurred outside the European Union (hereinafter: EU) (for example at a parent company or subsidiary established outside the EU), but it impacts directly (the payment-related services is rendered by the affected non-EU financial service provider) or indirectly (as a result of the event the financial service provider's ability to fulfil its payment activity is prejudiced in another way) the payment services of the payment service provider within the EU.
2. Classification of the operational or security incidents
   1. The payment service providermust only report the major operational and security incidents.Those operational and security incidents are deemed major that satisfy
3. one or more criteria of the "higher impact level", or
4. three or more criteria of the "lower impact level", as specified in the table below

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Lower impact level** | **Higher impact level** |
| Affected payment transactions | > 10 percent of the payment service provider’s usual level of payment transactions (expressed as the number of transactions)  **and**  > EUR 100,000 | > 25 percent of the payment service provider’s usual level of payment transactions (expressed as the number of transactions)  **or**  > EUR 5 million |
| The number of the affected users of the payment services | > 5,000 persons  **and**  > 10 percent (compared to the total number of the users of the payment services) | > 50,000 persons  **or**  > 25 percent (compared to the total number of the users of the payment services) |
| Duration of the service downtime | > 2 hours | Not applicable |
| Economic impact | Not applicable | > 0.1 percent of the Tier 1 capital, but minimum EUR 200,000  **or**  > EUR 5 million |
| High level of internal escalation | Yes | Yes, and the emergency mode of operation (or equivalent) is likely to be implemented |
| Potential effect on other financial service providers or relevant infrastructures | Yes | Not applicable |
| Reputational impact | Yes | Not applicable |

* 1. Terms used in the table:
* *affected payment transactions*:all those domestic and cross-border payment transactions that the operational or security event directly or indirectly affected or is likely to affect, and particularly those payment transactions that could not be initiated or processed, as well as those in which the message related to the payment has been altered or for the execution of which fraudulent order has been given (irrespective whether the amount of the payment transaction has been recovered or not).
* *usual level of payment transactions:* the daily average of domestic and cross-border payment transactions, in annual terms, that were carried out using the payment services affected by the operational or security incident. For the purpose of the calculation, the reference period shall be the year preceding the operational or security incident. If in the opinion of the financial service provider this measure is not representative (e.g. due to seasonality), other, more representative indicator should be used and the justification for this must be indicated in the "comments field" of the "Affected transaction" row of Table B – Intermediate report .
* *affected users of the payment services:* all clients (resident or non-resident, household or corporate clients) that have a contract with the affected payment service provider for the provision of payment services, and that suffer or are likely to suffer the consequences of the operational or security incident (in absolute value and also as a percentage of the total number of the users of the payment services). The payment service provider must resort to estimations based on past activity to determine the number of payment service users that used the payment service during the operational or security incident. In the case of groups, the individual payment service provider should take into consideration only its own users. The payment service provider rendering operational services to other payment service providers should take into consideration only its own users (if any), while the financial service provider using such operational services should assess the operational or security incident only from the perspective of its own users.
* *total number of the users of the payment services:* the aggregate number of the users of domestic and cross-border services (or the latest available figures), with whom the payment service provider had, at the time of the operational or security incident, a contract for the provision of payment services and had access to the respective payment services, irrespective of their size and whether they were active or passive users.
* *duration of the service downtime:* the time during which the payment-related service is likely to be unavailable to the users of the payment services or when the payment service provider is unable to execute the payment order. The payment service provider must take into consideration the period when any task, process or channel related to the payment service is down or likely to be down, and due to this it is not possible to initiate or execute the respective payment service or the respective payment account cannot be accessed. The duration of the service downtime must be calculated from the moment when the service goes down and for this purpose the period open for the execution of payment services, the closing hours and the maintenance period, if these latter two are relevant, should be taken into consideration. If the payment service provider is unable to determine the start of the service downtime, as a temporary rule the duration of the downtime must be calculated from the detection of the breakdown.
* *economic impact:* defining – as comprehensively as possible – the costs entailed by the operational or security incident, considering the absolute value of such costs, and also – as the case may be – the significance thereof compared to the size of the payment service provider (e.g. compared to the tier 1 capital of the payment service provider).
* *high level of internal escalation:* the fact that the operational or security incident was reported or is likely to be reported to the chief executives of the financial service provider. Furthermore, the payment service provider must take into consideration whether, due to the operational or security incident's impact on the payment-related services, the Chief Information Officer (or any person of similar position) has continuously received or is likely to receive information – apart from the regular information – of the operational or security incident during the existence thereof. The payment service provider must also consider whether – due to the impact of the operational or security incident on the payment-related services – the emergency mode of operation has been implemented or is likely to be implemented in the future.
* *effect on the other financial service provider or relevant infrastructures:* determining the probable systemic impact of the operational or security incident, i.e. whether there is any chance that the operational or security incident infects other payment service providers, financial infrastructures or card payment systems apart from the initially affected payment service provider. The payment service provider must assess the impact of the operational or security incident on the affected financial market – the financial infrastructure supporting the respective payment service provider and other payment service providers, as well as the card payment systems – and thus particularly the following: whether the operational or security incident has already occurred or is likely to recur in the future at other payment service providers as well, it has influenced or is likely to influence in the future the smooth operation of the financial infrastructures or whether in the future it is likely to jeopardise the stable operation of the entire financial system. When determining the degree of the effect, the payment service provider must take into consideration, e.g. whether the respective component or software is of exclusive use or is generally available, whether the network at risk is internal or external, the financial service provider has suspended or is likely to suspend the fulfilment of its obligations in a financial infrastructure where it is a member.
* *reputational impact:* determining the way the operational or security incident may undermine confidence specifically in the financial service provider and – more generally – in the underlying service or even in the entire financial market. The payment service provider must take into consideration, to the best of its knowledge, to what degree the operational or security incident has become or is likely to become public knowledge in the financial market. The payment service provider must particularly take into consideration the likelihood of the detrimental social impact of the operational or security incident. The payment service provider must take into consideration whether the operational or security incident has affected a process visible for the public and is therefore likely to receive or has already received media coverage [considering not only traditional media, such as newspapers, but also blogs, social networks, etc.], whether statutory or regulatory obligations have been or are likely to be omitted, and whether the same type of operational or security incident has occurred before.

1. If the payment service provider has no such actual data that are suitable for proving that any of the criteria has reached a threshold value or is likely to reach it before resolving the incident (which may be the case in the initial phase of the investigation), it should rely on estimates.
2. The payment service provider must perform the assessment of the criteria listed in subsection 2 during the lifecycle of the incident on a continuous basis to be able to decide whether the status of the incident has changed either to negative (from minor to major) or to positive (from major to minor) direction.
3. The methodological guidelines for the completion of the tables are included in the technical manual specified in subsection 9 of Annex 3, published on the website of the MNB.

**II. Detailed filling instructions**

1. The "0 – Header" table must be filled in for all reports. The payment service provider must fill in the additional tables of the report depending on the phase of the processing of the major operational or security incident.
2. A – Initial report:
   1. The purpose of the table is to submit the first notification on major operational or security incidents to the MNB.
   2. The payment service provider must submit the table within 4 hours from the detection of the major operational or security incident.
   3. The initial report must be also submitted by the payment service provider when a previously detected minor operational or security incident becomes a major operational or security incident. In this case the payment service provider must submit the initial report immediately after identifying the change of status.
   4. If the "Report type" is consolidated, table "D - Affected PSP" must be also submitted, specifying the payment service providers included in the initial report.
3. B – Intermediate report:
   1. The intermediate report must be submitted regularly – except for the cases specified in subsection 3.2 – not later than the time that the payment service provider specified in its previous report (i.e. in the initial report or the previous intermediate report) as the date of the next update, with the proviso that the date of next update must not be later than 3 working days.
   2. The payment service provider must always submit an intermediate report when according to its assessment a relevant change of status occurred in the reported major operational or security incident.
   3. The last intermediate report must be submitted when the daily usual course of business has been recovered and the payment service provider' operation is back to normal. The payment service provider may consider that business is back to normal when the activities and transactions have been restored to the same level of service and conditions that were defined by the payment service provider or laid down externally in a service level agreement in terms of processing times, capacity, security requirements, etc., and emergency measures are no longer in place.
   4. Should business be back to normal before 4 hours have passed since the detection of the major operational or security incident, the payment service providers must submit both the initial and the last intermediate report simultaneously within the deadline specified for the submission of the initial report in subsection 2.2 .
4. C – Final report:
   1. With the exception of the case specified in subsection 4.2, the payment service provider must submit the final report 2 weeks after that business is deemed to be back to normal in accordance with subsection 3.3.
   2. If after the detection of the major operational or security incident the payment service provider has all information necessary for the compilation of the final report within 4 hours, it must submit the final report together with the initial report.
   3. The payment service provider must provide comprehensive information in the final report (e.g. actual figures with regard to the impact rather than estimates).
5. Additional data and documents to be submitted together with the report

Upon submitting the first report after preparing the notice in accordance with Section 55/B(2) of the Payment Services Act, the payment service provider must – irrespective of the report type (initial, intermediate, final) – attach a copy thereof to the respective report.