Operational and Security Incident Reporting

1 Purpose

This process details how Roark Holdings Ltd. (the Firm) will deal with reporting operational and security incidents.
This process is based on the guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) published by European Banking Authority (EBA).

2 Review of Process

This process will be reviewed regularly, at least once a year, and amended as considered necessary by the Firm's Management Body in the event of changing circumstances or regulations.

3 Definitions

3.1 Operational and security incidents
The Firm defines operational or security incidents as an event, or a series of linked events, unplanned by the Firm which has, or is likely to have, an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.

4 Identification of an incident (will need to be amended for each client)

Upon identification of a possible operational and/or security incident, in relation to the services of the Firm, immediate notification must be made to the nominated member of staff, to ensure an assessment of the incident is conducted.
The initial notification provided to the nominated member of staff can be via email/phone, to ensure the incident can be addressed as a matter of urgency but

will then be logged via the incident reporting form/internal incident reporting procedure.

5 Incident assessment

The Firm will conduct an assessment following receipt of notification of a possible operational and/or security incident.
The nominated member of staff (MLRO) must conduct the initial assessment.
If the assessment finds that either payment services are estimated to be down for at least 2 hours, the back-office system is down for at least 2 hours, or transactions/payment services users are affected in any way then the Compliance Officer must be informed immediately. It is the responsibility of the nominated member of staff to inform the Management Body.
Following this, further assessment of incident needs to be conducted to establish if the incident should be classified as ‘major’ or ‘non-major’ based on the thresholds, published under Article 96 of PSD2, in the appendix to this document.
Where the incident is not classified as ‘non-major’, responsibility for monitoring and resolution will remain with the nominated member of staff(MLRO). This monitoring and resolution will include update of an ‘Issue Log’ (see Appendix 1) to take any ‘non-major’ issue to successful conclusion.
1.1 Incident classification
The Firm classifies incidents based on the thresholds provided in the Appendix 2. The criteria below will be used to establish if an incident should be classified as “Major”, and as such notification will be made to the FCA. The following criteria apply:

- If an incident meets or will probably meet one or more ‘Higher impact level’ thresholds, it qualifies as ‘major’.
- If an incident does not meet and probably will not meet any ‘Higher impact level’ thresholds but meets or will probably meet 3 or more ‘Lower impact level’ thresholds, it qualifies as major.

- If an incident does not meet and probably will not meet any ‘Higher impact level’ thresholds and does not meet and probably will not meet at least three ‘Lower impact level’ thresholds, it does not qualify as major.

6 Incident response

The Firm will report incidents classified as major to the FCA via the Connect system, this allows the Firm to authenticate itself properly to the FCA.
The responsibility for filing the report to the FCA lies with the Compliance Officer. In case of absence of the Compliance Officer, it is the responsibility of the Management Body to ensure a report is filed.
If the incident identified has or may have an impact on payment service users, the Firm will inform the payment service users immediately of the incident and make the payment service users aware of all measures they can take to mitigate the adverse effects of the incident.

Initial report

The Firm will send an initial report to the FCA when a major operational and/or security incident is first detected.
The Firm will send the initial report within 4 hours from the moment the incident was first detected, or, if the reporting channels to the FCA are not available at that time, as soon as they become available. This initial notification will be completed using the FCA’s incident reporting form (https://www.handbook.fca.org.uk/handbook/SUP/15/Annex11D.html).
The Firm will also immediately submit an initial report to the FCA when a previously non-major incident becomes a major incident.
The Firm will include some basic characteristics and consequences of the incident based on the information available immediately after it was detected or reclassified (referred to as headline-level information i.e. section A of the template). The Firm will resort to estimations when actual data are not available.

The Firm will also include in their initial report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days.

Intermediate report

The Firm will submit intermediate reports 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).
The first intermediate report will contain a more detailed description of the incident and its consequences than given previously. the Firm will then produce further intermediate reports following any updates to the information previously provided.
As previously, with each intermediate report the Firm will indicate when the next update will be given. This will be as soon as possible and within no more than 3 business days. If the next update is not submitted by the date given, then the Firm will contact the FCA to explain the reasons for the delay and propose a new submission deadline.
The Firm will send the last intermediate report once regular activities have been recovered and business is back to normal, informing the FCA of this circumstance. The Firm should consider that business is back to normal when activity/operations are restored to the same level of service/conditions as defined by the Firm.
If business is back to normal within 4 hours of detection of the incident, the Firm will aim submit both the initial report and last intermediate report together, and within 4 hours of the initial detection.

Final Report

The Firm sends a final report once the root cause analysis has taken place and actual figures have replaced any previous estimates. The final report will not contain estimates and will be delivered within 2 weeks of the return to business

as usual, if an extension is required the Firm will contact the FCA. The Firm will provide a complete and final report to the FCA, as such Section A, Section B and Section C will all be complete with actual figures.
If an identified incident no longer satisfies the criteria to be considered major and is not expected to fulfil the criteria before the incident is resolved, a final report must be sent. In this case Section C will require an explanation as to why the incident is no longer classified as major and for the Firm to tick the box stating, 'incident reclassified as 'non-major'.

7 Appendix

7.1 Appendix 1 - Issue log

Ref. No.	Date	**Details of Issue**	**Status of investigation**	**Investigation Results**	**Further Action**

Appendix 2 – Major Incident 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	> 5 000 **and** > 10% of the payment service provider's payment	> 50 000 **or** > 25% of the payment service provider's payment service users

	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 called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable