Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Guidance on Breach and Incident Reporting for MiFID Firms

August 2024

Contents

Back to “Contents”

General

1. This Guidance applies to all investment firms authorised under S.I. No. 375 of 2017, the European Union (Markets in Financial Instruments) Regulations 2017 (as amended) (referred to below as "MiFID firms" or simply "firms").
2. The reporting of breaches is required under Regulation 4(2) of S.I. No. 10/2023 - Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2023 ("The Central Bank Investment Firm Regulations").
3. The Breach and Incident Reporting Form for MiFID Firms ("the Form") is a form downloadable from the Central Bank website, which was developed to facilitate breach and incident reporting by MiFID firms. The Form is a word document in which firms are required to provide detailed information on the type of breach by answering specific questions and submit the document to the Central Bank of Ireland ("the Bank").
4. The scope of the reporting of breaches is also detailed under Regulation 4(2) of the Central Bank Investment Firm Regulations and the Form should be used for the reporting of all breaches, except for breaches relating to Client Assets (see next paragraph).
5. Any breaches relating to Client Assets[1] should be reported separately, further to the Client Asset Requirements/Investor Money Requirements, as set out on the Central Bank website.
6. Firms should download the Form and notify the Bank, through submission of the Form via the Central Bank Portal as soon as they become aware of any incident listed under regulation 4(2) of the Central Bank Investment Firm Regulations. Where necessary, firms should submit an updated Form after the initial Form is submitted, for instance where more relevant information becomes available on the background of how the issue occurred, its impact on the firm or the firm's action plan to address the issue.

[1] Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2023; SI 10/2023

Back to "Contents"

7. Firms should note that the Form is not a substitute for normal supervisory engagement. Firms should have regard to the urgency and significance of the matter and, if appropriate, contact their supervisor by telephone or email (as appropriate).
8. Firms should make their own assessment of the materiality of operational incidents.

Reporting Requirements

9. When a firm wishes to report a breach, potential future breach or operational incident, the Form template is set out in the Annex to this document and should be downloaded from the Bank's website, *Breach and Incident Reporting form for MiFID Investment Firms.* It should be completed and uploaded via the Central Bank Portal.
10. The Form should be completed with reference to one particular issue / incident and therefore the matter being reported should fall under one of the three categories:
    - Section (A) - Breach;
    - Section (B) - Potential future breach; and,
    - Section (C) - Operational incident.

    However, if appropriate, multiple categories may be selected. Additional information may be provided under Section (D) – Further Information.
11. Guidance on how to complete the Form for each type of issue: (A) Breach, (B) Potential future breach, and (C) Operational incident, is provided below.

A. Breach

12. When a firm is reporting a breach, it must provide details in Section (A) - Breach.

Back to "Contents"

13. Firms should provide comprehensive details about the breach. This includes reference to specific dates; background of the breach and its impact on the firm; how the breach was identified; whether it has been rectified; any actions taken or planned to resolve the issue; and any other changes made as a result of the breach.

B. Potential Future Breach

14. When a firm is reporting a potential future breach, it must provide details in Section (B) - Potential Future Breach.
15. Firms should give details about the potential future breach. It requests information including its probability; an estimate as to when the breach may occur; its estimated potential impact; and any mitigation or preventative actions taken or planned.
16. Examples where it would be appropriate for the firm to report a potential future breach are:
    - where it is likely that a firm will breach its capital requirements;
    - where an IT, systems or other issue within, or external to, the firm is likely to cause the firm to breach a legislative requirement.

C. Operational Incident

17. When a firm is reporting an operational incident, it must provide details in Section C - Operational Incident.
18. Firms should give comprehensive details of the incident; relevant dates; its impact; how it was identified; whether the issue has been rectified or how the firm plans to rectify the issue; and any further changes that have occurred as a result.
19. Examples of operational incidents which the firm should report to the Bank include but are not limited to:
    - business disruption and system failures;
    - litigation;
    - disciplinary proceedings against the firm;
    - internal fraud;
    - external fraud;
    - incidents around client products and business practice;
    - damage to physical assets.

Back to “Contents”

D. Further Information

20. Should a firm wish to detail any additional information pertaining to the breach, potential future breach or operational incident it should document this in Section (D) of the Form. Additionally, a firm may upload a document or documents containing further information as part of the submission process on the Central Bank Portal.

Back to "Contents"

Appendix

To be Downloaded from the Central Bank Website
https://www.centralbank.ie/regulation/industry-market-sectors/investment-firms/mifid-firms/reporting-requirements

Breach and Incident Reporting Form for MiFID Firms

1. This the Breach, Error and Incident Reporting Form for MiFID Firms[2].

2. Any breaches relating to Client Assets should be reported separately, further to the Client Asset Requirements/Investor Money Requirements, as set out on the Central Bank website.

3. The Form should be completed with reference to one particular issue / incident and therefore the matter being reported should fall under one of the three categories:
   - Section (A) - Breach;
   - Section (B) - Potential future breach; and,
   - Section (C) - Operational incident.

4. However, if appropriate, multiple categories may be selected. Additional information may also be provided under Section (D) – Further Information.

Section (A) - Breach

If reporting in relation to a breach that has occurred, please answer all questions in this section.

[2] The reporting of breaches is required under Regulation 4(2) of S.I. No. 10/2023 - Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2023 ("The Central Bank Investment Firm Regulations").

Back to "Contents"

When did the breach occur? Please specify the relevant date(s) and the time interval over which the breach occurred.

Please provide comprehensive details of the breach.

What is the impact of the breach? Please provide an assessment of (i) the financial impact to the firm, customers and other relevant stakeholders, (ii) the reputational impact and (iii) any other impact.

On what date was the breach identified? [dd/mm/yyyy]

How was the breach identified?

Has the breach been rectified? [Yes / No / Not Applicable]

Back to "Contents"

If yes, please explain how and when the breach was rectified.

If no, please detail the actions that are planned to rectify the breach. Include detail on the expected timeframe to complete these actions.

If not applicable, please explain why.

Please detail any further changes to the firm's systems, procedures or controls that have been made or are planned as a result of the identification of the breach.

Section (B) – Potential Future Breach

Back to "Contents"

If reporting in relation to a potential future breach, please answer all questions in this section.

Please provide comprehensive detail on the potential future breach.

What is the probability of the potential future breach occurring?

When do you estimate the potential future breach might occur?

What is the estimated impact of the potential future breach? Please provide an estimate of (i) the financial impact to the firm, customers and other relevant stakeholders, (ii) the reputational impact and (iii) any other impact.

Back to "Contents"

What actions have you taken or are planned in order to mitigate or prevent the potential future breach? Include detail on the expected timeframe to complete these actions.

Section (C) – Operational Incident

If reporting in relation to an operational incident, please answer all questions in this section.

When did the operational incident occur? Please specify the relevant date(s) and the time interval over which the incident occurred.

Please provide comprehensive details of the operational incident.

What is the impact of the operational incident? Please provide an assessment of (i) the financial impact to the firm, customers and other relevant stakeholders, (ii) the reputational impact and (iii) any other impact.

Back to "Contents"

On what date was the incident identified?
[dd/mm/yyyy]

How was the incident identified?

Has the incident been rectified? [Yes / No / Not Applicable]

If yes, please explain how and when the operational incident was rectified.

If no, please detail the actions that are planned to rectify the operational incident. Include detail on the expected timeframe to complete these actions.

Back to "Contents"

If not applicable, please explain why.

Please detail any further changes to the firm's systems, procedures or controls that have been made or are planned as a result of the identification of the operational incident.

Section (D) – Further Information

Please detail any additional information pertaining to this matter or upload in a separate document.

The Central Bank may process personal data provided by you in order to fulfil its statutory functions or to facilitate its business operations. Any personal data will be processed in accordance with the requirements of data protection legislation. Any queries concerning the processing of personal data by the Central Bank may be directed to dataprotection@centralbank.ie. A copy of the Central Bank's Data Protection Notice is available at www.centralbank.ie/fns/privacy-statement.

Back to "Contents"

Back to “Contents”

T: +353 (0)1 224 5800
E: publications@centralbank.ie
www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem