

PUBLIC COMPLIANCE COMMUNICATION

**PUBLIC COMPLIANCE COMMUNICATION 50
(PCC 50)**

**GUIDANCE ON THE MEASURES REQUIRED
FOR THE MITIGATION OF LOSS OF
INTELLIGENCE DATA DUE TO REPORTING
FAILURES**

PCC SUMMARY

This PCC guides reporters on certain measures required for the mitigation of lost intelligence data due to the Financial Intelligence Centre (Centre), where a report ought to have been filed and the reporter fails to file the report, or where a reporter files a defective report. In both these instances the reporter is required to remediate the reporting failure as soon as possible. A defective report includes a rejected report owing to validation failures or where the data submitted in the report is inaccurate or false.

In addition, this PCC guides reporters on measures aimed at preventing, remediating, and mitigating reporting failures, and elaborates on the Directive 3 of 2014 process to be followed when applicable.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the users' legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

COPYRIGHT NOTICE

This PCC is copyright. The material in a PCC may be used and reproduced in an unaltered form only for personal and non-commercial use within your institution.

Apart from any use permitted under the Copyright Act, 1978 (Act 98 of 1978), all other rights are reserved.

OBJECTIVE

This PCC provides guidance to reporters on certain measures required for the mitigation of loss of intelligence data due to the Centre, where a report was ought to be filed and the reporter has failed to file this report with the Centre, or where a defective report is filed with the Centre. In addition, this PCC provides guidance to reporters on the prevention, remediation and mitigation measures relating to reporting failures and gives clarity on the Directive 3 of 2014 process.

GLOSSARY

“**ATMS**” automated transaction monitoring system as explained in Directive 5 of 2019 to the FIC Act.

“**Centre**” means the Financial Intelligence Centre established in terms of section 2 of the FIC Act.

“**Days**” refers to all days of the week excluding Saturdays, Sundays, and public holidays, as aligned with the definition as set out in the Money Laundering and Terrorist Financing Control (MLTFC) Regulations.

“**Defective report**” refers to a report that has been filed with the Centre with the incorrect or incomplete prescribed particulars, where such a report is either received or rejected by the Centre’s reporting platform. This would include where a report contains data that fails the validation process or where the report passes that validation process but contains inaccurate or false data. “**Submitted report that is defective**” and “**defectively filed report**” has a corresponding meaning.

“**Directive 3**” refers to the Directive 3 of 2014 on the notification of failure to report as required by the Financial Intelligence Centre in terms of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued in terms of section 43A of the FIC Act and published in Government Gazette Notice 783 of 12 September 2014.

“**FIC Act**” refers to the Financial Intelligence Centre Act, 2001 (Act 38 of 2001).

“**Prescribed particulars**” refers to the accurate information required to be captured by a reporter for the submission of regulatory reports as detailed in the MLTFC Regulations.

“**Reporter**” refers to the person or entity making the report, including accountable and reporting institutions and any other person required to submit a report in terms of the FIC Act.

“Report” refers to a regulatory report as envisaged in: section 28 of the FIC Act in relation to cash transactions above the prescribed threshold (CTR) and cash transaction aggregation report (CTRA); in relation to section 29 of the FIC Act which includes suspicious and unusual transaction report (STR), suspicious activity report (SAR), terrorist financing transaction report (TFTR) and terrorist financing activity report (TFAR) as well as terrorist property report (TPR) in relation to section 28A of the FIC Act.

“Reporting failure” refers to the general term where a report ought to be filed and the reporter either fails to submit such a report or files a defective report with the Centre.

1 INTRODUCTION

- 1.1 The objective of this PCC 50 is to provide guidance to reporters on the measures required for the mitigation of lost intelligence data due to the Centre, which includes the remediation and prevention of reporting failures.
- 1.2 The goal of remediation is to file a non-submitted report and correct a defectively filed report within the soonest possible time, to limit any further negative impact due to the loss of intelligence data to the Centre.
- 1.3 The remediation of reporting failures, as detailed in this PCC, does not amount to nor lead to condonation of any act of non-compliance of reporting obligations in terms of the FIC Act. Enforcement action may be taken by the Centre, or the appropriate supervisory body, as a result of non-compliance with reporting obligations.
- 1.4 Where the reporter becomes aware of a reporting failure, the reporter must immediately take steps to commence remediation of that reporting failure. The reporter must not wait for the Centre to indicate when remediation should begin.
- 1.5 This PCC will consider the reporting failure in three instances where a report ought to be filed with the Centre, but the report was:
 - 1.5.1 Not submitted (also referred to as a non-submission), as read with Directive 3; or
 - 1.5.2 Rejected by the Centre's reporting platform owing to validation failures; or
 - 1.5.3 Submitted to the Centre and contains inaccurate, incorrect, or false data.
- 1.6 A reporter will only discharge the reporter's reporting obligations in terms of the FIC Act where:
 - 1.6.1 A reportable event is identified/detected timeously;
 - 1.6.2 A reportable event is reported within the prescribed time period;
 - 1.6.3 All mandatory and readily available information is captured accurately; and
 - 1.6.4 The report is submitted according to the prescribed format.
- 1.7 Where there is a reporting failure the reporter has not discharged the reporters reporting obligation.

- 1.8 The Centre is of the view that the varying reasons for a reporting failure does not impact the fact that a reporting failure has occurred. The consequences, including any enforcement action that might flow from a reporting failure, does not fall within the ambit of this PCC. Non-compliance with reporting obligations are dealt with in accordance with sections 51, 51A and 52 of the FIC Act.
- 1.9 This PCC 50 must be read together with the provisions of [Directive 3](#) and [goAML Notice 4A](#).
- 1.10 This PCC consists of two parts namely:
PART A: Non-submitted report
PART B: Defective report

PART A

2 NON-SUBMITTED REPORT

- 2.1 A report that a reporter ought to have filed to the Centre but failed to do so, is considered a non-submitted report. Where a reporter becomes aware of a non-submitted report, the reporter must mitigate the loss of intelligence data to the Centre.
- 2.2 The reporter could become aware of this reporting failure either on the reporters own accord, as a result of a supervisory inspection, external audit or through other means.
- 2.3 Failure to identify reportable transactions or activities could be as a result of various factors including, but not limited to, poor product mapping, errors in the application and implementation of an ATMS as well as inadequate identification of all reporting streams as noted in the accountable institution's risk management and compliance programme (RMCP).

Directive 3 process

- 2.4 The Directive 3 process must only be followed when a reporter becomes aware of a non-submitted report(s).
- 2.5 The purpose of the Directive 3 process is for the reporter to notify the Centre of loss of intelligence data due to a non-submitted report, how this occurred, what the remediation action plan is and ensuring the non-submitted report is filed with the Centre.
- 2.6 Remediation of a non-submitted report includes, but are not limited to:
 - 2.6.1 Submission of all non-submitted reports; and
 - 2.6.2 Review and amend existing internal systems and reporting methodology as detailed in the reporters' RMCP (where the reporter is an accountable institution) to ensure that the reporting failure does not re-occur.

Example 1

Reporting failure identified by accountable institution, to be remediated through Directive 3 process

Accountable institution B conducted an internal audit and discovered that the accountable institution had monitored transactions incorrectly for a given product/service offered. As a result of this, the reporters audit revealed that there were reports that ought to have been submitted that had not been filed with the Centre.

Accountable institution B must disclose the non-submission of reports to the Centre through the Directive 3 process as soon as possible.

*The application of the Directive 3 process applies to various scenarios. Example 1 is an illustration of one such scenario.

- 2.7 As prescribed in Directive 3, the reporter must notify the Centre, in writing, of the reporter's reporting failures relating to the non-submission of a report as soon as the reporter becomes aware thereof. This notification must contain the details regarding the nature and extent of the loss of data and the proposed remediation actions as follows:
- 2.7.1 The time period over which the non-submitted report(s) range;
 - 2.7.2 The extent of the non-submitted report(s), including but not limited to the volume and value of the impacted transactions;
 - 2.7.3 The root cause(s) of the reporting failure;
 - 2.7.4 Any factors that may impact the remediation process, including mitigating or aggravating factors;
 - 2.7.5 Steps that the entity may have already taken to mitigate the current, and re-occurrence of the reporting failures; and
 - 2.7.6 Proposed remediation plan, indicating proposed time period for successful completion.
- 2.8 All Directive 3 notifications must be sent to the Executive Manager: Compliance and Prevention at Directive3@fic.gov.za.
- 2.9 Where the reporter does not have all the information as required in paragraph 2.7 at the time of notifying the Centre, the reporter is to provide the preliminary information available, and

state the reasons why all the information is not available. Additionally, the reporter must indicate a reasonable date within which the further required information will be provided to the Centre.

- 2.10 The Centre may request a meeting with the reporter regarding the reporting failure and may include the relevant supervisory body in the meeting. The purpose of the meeting is to discuss the non-submission of reports as detailed in the written notification, indicated in paragraph 2.7. The conclusion of this meeting would be to reach an agreement with the Centre regarding the remediation process, including the submission of reports.
- 2.11 The reporter must submit formal, written progress reports on the submission of non-submitted reports including information on systems development and process enhancements in mitigation of reporting failures as agreed with the Centre.
- 2.12 The reporter must obtain consent from the Centre prior to filing a remediated report on the Centre's reporting platform. This would enable the Centre to manage the data flow on the reporting platform and to ensure that there are no backlogs created.
- 2.13 The Centre will track the submission of the report(s) by the reporter as per the agreed remediation actions.
- 2.14 Upon completion of the Directive 3 process, the reporter must provide the Centre with a formal, written close out report detailing the steps taken to remediate the non-submitted reports and prevent a re-occurrence of the reporting failure. The close out report must include reconciliation reports submitted as part of the corrective action and confirm that all non-submitted reports have been successfully filed.
- 2.15 The Centre may require the reporter to carry out system testing on the Centre's reporting platform testing environment before submitting the reports on the production environment as part of the submission of the non-submitted reports.

2.16 While a reporter is undergoing a Directive 3 remediation process, the reporter must continue with the reporters reporting obligations for new reports. The Directive 3 process does not suspend other reporting obligations that the reporter has under the FIC Act. The Directive 3 process must be managed simultaneously with the reporter's existing reporting obligations.

Non-compliance

2.17 Where a reporter fails to notify the Centre of a non-submitted report(s), or where a reporter fails to remediate a report according to the remediation plan, the reporter has not complied with its duty in terms of Directive 3 and may be subject to administrative sanctions in terms of the FIC Act.

PART B

3 DEFECTIVE REPORT

Process of the submission of a report

- 3.1 A report must contain all the required information as prescribed in the MLTFC Regulations and reporting platform rules.
- 3.2 A report submitted on the Centre's reporting platform goes through a series of automated validation checks to ensure that the report has met the prescribed requirements of all mandatory and readily available information being captured.
- 3.3 Failure to file a report with the correct or complete prescribed particulars, may result in either a report failing the validation process and being rejected, or a report being received by the Centre with incomplete or false data. In both these cases the defective report must be remediated.
- 3.4 The reporter is required to remediate a defective report either as soon as the reporter is notified that the report is rejected or becomes aware that the report contains inaccurate or incorrect data. This process is set out in goAML notice 4A.
- 3.5 Directive 3 does not apply in instances where a report has been submitted, but it is defective.

Status of the confirmation notification following submission of a report

- 3.6 After submission of a report, a reporter will automatically receive an e-mail notification from the Centre's reporting platform, to confirm that the Centre has received the report.
- 3.7 The e-mail notification does not constitute a confirmation that the reporter has discharged the reporters reporting obligation. Rather, it serves as confirmation that the Centre's reporting platform has received a report for consideration and further processing. The receipt of the e-mail notification would not absolve the reporter from the consequences of defective reports being submitted or enforcement action which could arise as a result of the defective report.
- 3.8 When the report is received and processed by the Centre's reporting platform, it is reviewed against the prescribed validation criteria. Where a report fails the validation process the

report will be rejected and a notification will be sent to the reporter's message board functionality on the reporting platform. It is therefore essential that the reporter accesses and reviews the message board after a report is submitted and until such time that the status of the report reflects as either received or rejected.

- 3.9 Should the report meet the validation criteria, confirmation of this will be displayed on the message board functionality on the reporting platform.
- 3.10 This confirmation in the message board does not constitute a confirmation that the reporter has fully discharged the reporters reporting obligation. Should the Centre or the reporter identify that the information contained in the submitted report is incorrect, even though it has passed the validation requirements, the reporter has not discharged the reporters reporting obligation.
- 3.11 Both the email message and confirmation on the message board merely indicates that a report has either been rejected or received by the reporting platform.

4 DEFECTIVE REPORTS– SYSTEMS RULE FAILURE AND REJECTED REPORT

- 4.1 A report that is submitted and then **rejected** by the reporting system because it fails the validation requirements that apply to the specific report, is not considered to be submitted to the Centre, and the reporter has not discharged the reporters reporting obligation.
- 4.2 A rejected report must be remediated and re-submitted to ensure adequate submission.
- 4.3 Reasons for report systems rule failure may include where the submitted report does **not**:
 - 4.3.1 Contain the mandatory information as set out in the MLTFC regulations; and/or
 - 4.3.2 Have the mandatory information captured in the correct format.

Example 4

Incorrectly filed report owing to system rule failure

Accountable institution C submits a suspicious and unusual transaction report (FIC Act section 29) on Mr X, a South African citizen. Mr X's identification number is not captured in the report submission.

The report would not meet the validation requirements and will be rejected. Accountable institution C would be required to remediate the incorrect information and submit the corrected report to the Centre.

- 4.4 The reporter is obliged to take measures to correct and remediate the rejected report in terms of the FIC Act. These measures include:
- 4.4.1 Correcting the information;
 - 4.4.2 Using the correct format as prescribed; and
 - 4.4.3 Submitting the remediated report on the reporting platform.
- 4.5 The reporting entity must resubmit the corrected report within the initial prescribed period as set out in the MLTFC regulations, that apply to that report type. There is no additional time provided to a reporter in the reporters final submission of a report.
- 4.6 The reporter must formally, in writing, confirm to the Centre when the remediation process has been completed.

5 DEFECTIVE REPORTS – REPORT CONTENT FAILURE

- 5.1 A reporter that submits a report that is **accepted** by the reporting system, where the reporter has captured inaccurate or false information in this report to bypass the reporting system validation rules, has not discharged the reporters reporting obligation. The reporter must remediate this report.

- 5.2 A report is defective when a report contains incorrect data captured either in good faith or intentionally inserted in an attempt to bypass the system rules for the report to be processed on the reporting platform.
- 5.3 Upon becoming aware of a defective report being filed, the reporter is obligated to take measures to correct and remediate the report. These measures include to:
- 5.3.1 Correct the information;
 - 5.3.2 Use the correct prescribed format; and
 - 5.3.3 Submit the remediated report on the reporting platform.
- 5.4 The Centre does not tolerate the behavior of reporters intentionally inserting incorrect data when filing a report. This behavior is against the spirit and the intention of the FIC Act and is not conducive to the fight against financial crime. Where it is evident that a report with incorrect data is submitted intentionally, the reporter has not met the reporting obligation to the Centre as required in terms of the FIC Act. The capturing of false information to the Centre is considered as an act of fraud.

6 RECOMMENDATIONS TO LIMIT REPORTING ERRORS

Information required in terms of the MLTFC regulations

- 6.1 Reporting entities must adhere to the FIC Act together with the MLTFC Regulations when submitting reports to the Centre, as well as the applicable prescribed reporting platform.
- 6.2 Chapter 4 of the MLTFC Regulations sets out the requirements that apply to reporting. Reporters must obtain the mandatory information as required in data fields necessary to comply with the MLTFC Regulations as adopted in the reporting system's reporting forms. Reporters are to further consider additional information that could be captured should the information be readily available.
- 6.3 The Centre recommends that reporters obtain sufficient information from the reporter's clients that could be obtained through customer due diligence processes or any other information obtained in order to facilitate a transaction to make it commercially viable.

- 6.4 The Centre recommends that reporters develop client file system validation rules, to ensure that only quality data is captured at client onboarding and ongoing due diligence stages.
- 6.5 The Centre recommends that reporters develop transaction information validation rules to ensure that only quality data is captured when processing transactions.
- 6.6 A reporter should consider the following system rules that could be built into the reporter's systems:
 - 6.6.1 The entity must ensure that a valid name, surname, and an identification number is captured for all its natural clients.
 - 6.6.2 For clients who are South African citizens, the entity must ensure that a valid ID number is captured i.e. the number must contain 13 digits and must adhere to all the requirements defined by the Department of Home Affairs.
 - 6.6.3 For clients who are foreigners, the entity must ensure that a valid identification number is captured e.g. a passport number or a permit number.
 - 6.6.4 The entity must ensure that a valid and accurate date of birth is captured for all the entity's clients that are natural persons.
 - 6.6.5 The entity must ensure that a valid name and registration number is captured for all its clients that are legal persons.
 - 6.6.6 The entity must file cash threshold reports to the Centre, for cash transactions above the threshold.

Pre-validation of report information

- 6.7 The Centre recommends that reporters conduct pre-validation of all reports before filing reports with the Centre. This is to help prevent report failures or rejections. This will also ensure that prescribed and accurate information is reported to the Centre within the prescribed format and time period.
- 6.8 Pre-validation includes the reporter checking whether the report includes all mandatory information and that which is readily available as prescribed for the report type in terms of the MLTFC Regulations.

6.9 Pre-validation may be an automated and/or manual process.

6.10 The obligation is on the reporter to ensure that the prescribed accurate information is submitted as required in terms of the MLTFC Regulations as well as the reporting platform rules. The onus is on the reporter to ensure the reporters reports are compliant.

Quality reviews and assurance processes

6.11 Reporting entities should follow a multi-disciplinary approach that will enable them to apply adequate quality control measures and implement assurance processes in order to identify potential issues relating to the submission of a report to the Centre.

6.12 Prior to the reporter being able to submit batch regulatory reports, the Centre will require that the reporter test this functionality in the user acceptance testing environment. This is to ensure that the reports submitted meet the minimum standards. Reporters who want to submit batch reports must contact the Centre to facilitate such arrangements.

7 COMMUNICATION WITH THE CENTRE

7.1 General compliance queries can be directed to the compliance contact centre on 012 641 6000 and select option 1. Queries can also be submitted online by clicking on <http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx> or by visiting the Centre's website and submitting an online compliance query.

Issued By:

The Director Financial Intelligence Centre

Date 31 March 2021