Financial
Intelligence Centre

DRAFT DIRECTIVE 5/2019

THE USAGE OF AN AUTOMATED TRANSACTION MONITORING SYSTEM FOR THE DETECTION AND SUBMISSION OF REGULATORY REPORTS TO THE FINANCIAL INTELLIGENCE CENTRE IN TERMS OF SECTION 29 OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT NO. 38 OF 2001)

PREFACE

This Directive is issued by the Financial Intelligence Centre (the Centre) in terms of section 43A(1) of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) (the FIC Act).

This Directive applies to all accountable and reporting institutions and to other persons (collectively referred to as reporters for purposes of this directive) who use an automated transaction monitoring system (ATMS) to enable them to discharge their obligation of submitting regulatory reports to the Centre in terms of section 29 of the FIC Act read with Regulation 24(3) of the Money Laundering and Terrorist Financing Control Regulations (the MLTFC Regulations).

This Draft Directive consists of four parts:

1. **Purpose of the Directive**
2. **Directive**
3. **Conditions for using an ATMS**
4. **Effective Date and Non-Compliance**

1. Purpose of the Directive

1.1 The purpose of this Directive is to set conditions for the use of an automated transaction monitoring system (ATMS) implemented by reporters to identify potentially suspicious and unusual activities or transactions or a series of transactions, and to ensure that a proper governance arrangement is in place for reporters to fully comply with all reporting obligations.

2 Directive

2.1 Reporters who have implemented an ATMS are directed to attend to all alerts generated by the ATMS within 48 hours of an alert being generated with a view to determine whether a report should be submitted to the Centre.

2.2 The reporter is deemed to have knowledge of the possible suspicious and unusual activity when an alert is generated by the ATMS.

2.3 Suspicious and unusual transaction or activity reports must be submitted to the Centre in accordance with regulation 24(3) as soon as possible but no later than 15 days after the alert has been generated by the ATMS.

2.4 Reporters are directed to comply with the conditions for using an ATMS as stipulated in paragraph 3 below.

3. Conditions for using an ATMS

3.1 Reporters must, as a condition to using an ATMS, ensure compliance with the following requirements to ensure effective money laundering and terrorist financing risk management:

3.1.1 The board of directors, senior management or other person or group of persons exercising the highest level of authority in an accountable institution responsible to ensure the effectiveness of the compliance function of an accountable institution must have adequate oversight over the process of implementing the ATMS, alert management, adequacy of rules and or scenarios implemented including testing thereof, and reporting to the Centre arising from alerts generated by the ATMS.

3.1.2 Reporters must ensure that all alerts are timeously investigated to ensure that reports are submitted to the Centre within the prescribed period.

3.1.3 Reporters must clearly allocate responsibilities for reviewing, investigating and reporting of alerts generated by the ATMS within their respective organisations.

3.1.4 The persons so responsible in paragraph 3.1.3 must have the appropriate level of skill required to perform this function, and must be regularly trained to identify unusual and suspicious activities.

3.1.5 All investigations and decisions taken relating to alerts generated by the ATMS must be adequately documented, and kept in a manner readily accessible to the respective reporters' relevant supervisory body and or the Centre where applicable.

3.1.6 Adequately skilled staff must be appointed by reporters to deal with the volumes of alerts generated by the ATMS.

3.1.7 Reporters utilising an ATMS must ensure that there are adequate resources to report timeously and not create a backlog of unattended alerts.

3.1.8 Where a suspicious or unusual transaction or activity is detected by a reporter in an instance other than through the ATMS, the reporter must ensure that the ATMS detection rules are developed and implemented to enable future detection of similar scenarios via the ATMS.

3.1.9 The fact that an accountable institution uses an ATMS must not prevent the accountable institution from receiving manual reports from internal stakeholders regarding suspicious and unusual activity or transactions.

3.1.10 Reporters must ensure that the detection methodology and effectiveness of an ATMS are validated and tested to ensure that the system is detecting potentially suspicious and unusual transactions or series of transactions, resulting in the generation of high quality alerts, and is being effectively utilised by the reporter.

3.1.11 Reporters that are accountable institutions must include the process for reporting information to the Centre and the investigation of automated alerts in the accountable institution's Risk Management and Compliance Programme (RMCP).

3.1.12 The effectiveness of the ATMS must be periodically reviewed and approved, at least annually by the board of directors, senior management or other person or group of persons exercising the highest level of authority in the accountable institution and in accordance with the reporters RMCP.

3.1.13 The ATMS must be subject to ongoing risk assessment and parameter calibration (tuning), and such risk assesment and tuning methodology should be included in the RMCP of that reporter.

3.1.14 All configuration changes to the ATMS must follow a documented governance procedure, must be adequately tested and significant changes must be authorised by the board of directors, senior management or other person or group of persons exercising the highest level of authority prior to implementation.

3.1.15 At all times a clear audit trail should exist to demonstrate what changes, configurations, additions or withdrawal of rules and scenarios have occured, as well as when the changes took place and the responsible person/s that effected these changes.

3.1.16 Reporters must ensure that the detail relating to the detection methodology including algorithms, scenarios, threshold settings or rules used by the ATMS are set out accurately and clearly, and is documented, and in the case of an accountable institutions is included in its RMCP.

3.1.17 Reporters must ensure that the detection methodology including, algorithms, scenarios, threshold settings or rules used by the ATMS are sufficient to address the associated money laundering and terrorist financing risks applicable to the reporter.

3.1.18 Where a reporter is a subsidiary or a branch of a foreign-based organisation which also utilises an ATMS, the reporter must have procedures in place to ensure its usage of the ATMS is adequately customised for its domestic money laundering and terrorist financing risks within the domestic reporting regime.

3.1.19 For reporters that have branches, departments and partnering agents (such as mobile service providers), the ATMS must monitor the clients and transactions across all products and services, including transactions effected by agents.

3.1.20 Where a reporter, who is an accountable institution, is utilising more than one ATMS which operates independently of each other, must ensure that the systems utilised do not prevent a reporter from having a holistic view of both the alerts generated and the total number of suspicious and unusual transaction or activity reports submitted in respect of a specific client of a reporter.

3.1.21 Reporters must make available to the Centre or to the reporters' relevant supervisory body, on request, reports relating to the results of an evaluation of the ATMS.

4 Effective Date and Non-Compliance

4.1 This Directive is effective from date of publication in the Government Gazette.

4.2 Failure to comply with this Directive may result in the imposition of an administrative sanction, in accordance with section 45C of the FIC Act.

Draft Issued by:
The Financial Intelligence Centre
March 2019