MEASURES TO HELP CREDIT PROVIDERS MITIGATE THE RISK OF FINANCIAL CRIME

Products and services offered by credit providers, such as loans and finance, make them vulnerable targets for money laundering and terrorist financing abuse. Illicit funds could, for example, be laundered via the sector through early repayment of loans or the use of the loans for illicit purposes.

To help mitigate the risk of criminal exploitation, credit providers have therefore been brought into South Africa's anti-money laundering, combating the financing of terrorism and combating proliferation financing (AML, CFT and CFP) regulatory fold. Credit providers are listed as accountable institutions under item 11 of Schedule 1 to the Financial Intelligence Centre Act (FIC Act). As accountable institutions, credit providers must meet certain compliance obligations which are geared to assist them in identifying the proceeds of crime and combating money laundering and terrorist financing.

The FIC Act describes a credit provider as a person who carries on the business of:

(a) a credit provider as defined in the National Credit Act 34 of 2005 (NCA); and

(b) providing credit in terms of any credit agreement that is excluded from the application of the NCA by virtue of section 4(1)(a) or (b) of that Act.

HOW CREDIT PROVIDERS CAN BE VULNERABLE TO MONEY LAUNDERING

Not all credit providers' products, clients or transactions bear the same risks of being misused for money laundering, terrorist financing, and proliferation financing. The onus is on individual credit providers to determine their level of exposure to potential abuse.

As part of the measures to help mitigate these risks, credit providers are required to develop, document, maintain and implement a risk management and compliance programme (RMCP) for AML, CTF and CPF.

The RMCP document must record all the elements of the programme as set out in section 42 of the FIC Act. This includes how the institution complies with obligations such as implementing a risk-based approach, customer due diligence, targeted financial sanctions, account monitoring, reporting to the FIC, and record keeping.

ELEMENTS OF AN EFFECTIVE RMCP

To develop an effective RMCP, the credit provider must first conduct an entity wide risk assessment to identify the money laundering, terrorist financing, and proliferation financing risks the institution faces. In turn, the credit provider can then determine the controls required to mitigate the risk.

The risk assessment should be sufficiently comprehensive to enable the credit provider to clearly identify, assess, mitigate and manage the inherent and residual money laundering, terrorist financing, and proliferation financing risks and threats. This includes considering the nature, size, products, service offerings, industry, client base, geographic location(s), complexity of business, delivery mechanisms, third-party service providers and any other relevant factors of the credit provider.

Refer to the FIC Revised guidance note 7A for more indicators and further guidance on the implementation of various aspects of the FIC Act.

Revised Guidance Note 7A provides the following examples for risk indicators:

Indicators relating to products and services – Does the product allow for third party payments?

Indicators relating to delivery channels – Is the product offered to prospective clients directly or through intermediaries?

Indicators relating to geographic locations – Is the client domiciled in South Africa or in another country or does the client operate in another country?

Indicators relating to clients – Is the client a natural person or corporate vehicle? What information does the client provide concerning their source(s) of income?

RISK MITIGATION AND MANAGEMENT

Credit providers must mitigate and manage the assessed risks by applying appropriate controls, this includes but is not limited to customer due diligence, reporting, and record keeping. These controls must be designed to detect and respond appropriately when money laundering and terrorist financing risks materialise.

Customer due diligence provides the credit provider with the knowledge about their client's identity, nature of the business relationship, intended purpose of the business relationship and source of funds.

Where there are higher money laundering, terrorist financing, and proliferation financing risks, enhanced customer due diligence measures must be taken to mitigate those risks.

The institution must monitor whether the controls implemented are adequate and effective to mitigate the identified risks. Customer due diligence can form part of ongoing risk monitoring.

THE ROLE OF MANAGEMENT IN THE ACCOUNTABLE INSTITUTION

The accountable institution's board of directors, senior management, or the person(s) with the highest authority must approve the RMCP and ensure compliance by the accountable institution and its employees, with the provisions of the FIC Act and its RMCP. The duty to approve the RMCP document cannot be delegated to any other person.

The board of directors, senior management, or the person(s) with the highest authority must consider whether the RMCP adequately mitigates the money laundering, terrorist financing, and proliferation financing risk and that all relevant risk factors have been considered.

SUBMISSION OF AN RMCP TO THE FIC

Credit providers as accountable institutions must make available a copy of the RMCP document to the FIC when requested. On 4 March 2025, all accountable institutions were advised to submit a copy of their RMCP document to the FIC by 12 March 2025 via the goAML platform. Credit providers should refer to the RMCP request letter for the manner in which the RMCP document must be submitted.

SUSPICIOUS AND UNUSUAL TRANSACTION REPORTING

All businesses are required to report suspicious and unusual transactions and activity in terms of section 29 of the FIC Act. Section 29 reports can either be a transaction or an activity report. These reports should be submitted to the FIC without delay as soon as possible but no later than 15 days from when a person becomes aware of facts which give rise to the suspicion. For guidance in terms of suspicious and unusual reporting, please refer to Guidance Note 4B.

For sector specific compliance information and guidance, kindly refer to the FIC web page for credit providers. The FIC's compliance contact centre can be reached on +27 12 641 6000 or log an online compliance query by clicking on: https://www.fic.gov.za/compliance-queries/