FINANCIAL SERVICE PROVIDERS AND STEMMING CRIME

The broad range of services offered by financial services providers can make them vulnerable to beign exploited by criminals involved in money aundering and/or the inancing of terrorist activities.

It is for this reason that financial services providers are included as one of the 16 Schedule 1 accountable institutions in the Financial Intelligence Centre Act, 2001 (Act 38 of 2001).

The Act gives the Financial Intelligence Centre the mandate to identify funds generated from criminal acts, to combat money laundering and terror financing As the South Africa's centre for gathering gathering and analysing financial data, the FIC is able to develop valuable financial intelligence reports for investigative and prosecutorial authorities for their follow up actions and investigations. This information gathering and report development, however, is largely reliant on the of institutions and the submission of reports from them.

Financial service providers, like all accountable institutions, are required to fulfil compliance obligations that is geared to protect the financial system and its institutions, and to strengthen them against abuse.

FIC ACT DEFINITION OF FSP

A financial services provider requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002), to provide advice and intermediary services in respect of the investment of any financial product (but excluding a short term insurance contract or policy referred to in the Short-term Insurance Act, 1998 (Act 53 of 1998) and a health service benefit provided by a medical scheme as defined in section 1(1) of the Medical Schemes Act, 1998 (Act 131 of 1998).

These seven compliance obligations are:

TRANSPARENCY AND GLOBAL STANDARDS FOR SOUTH AFRICA

As money movements within and across borders continue, across the globe, the call for transparency is increasing at a similar pace.

In South Africa, much consideration on transparency in the financial system has gone into the amendments made to the Financial Intelligence Centre Act, 2017 (Act 1 of 2017) which was promulgated 2 May 2017. A more transparent financial system entails application of customer due diligence, proper record keeping, reporting measures to enable detection, investigation and sanctioning of illicit activity.

The built in innovative standards and provisions brought about in the amended FIC Act are designed to bring South Africa's financial system in line with global practices. The major changes to the Act include:

ADOPTION OF A RISK-BASED APPROACH TO KNOWING THE CUSTOMER

This approach gives financial institutions the flexibility to assess and manage risk depending on the category of the customer. Institutions can vary their approach, depending on factors such as type of customer, business relationship, product and location.

IDENTIFYING WHO REALLY OWNS AND BENEFITS FROM COMPANIES

Institutions need to know the people behind companies – those who benefit financially – to bring greater transparency to the financial system. This will help authorities detect, investigate and prosecute instances where corporate structures have been used to hide illicit financial dealings.

IMPROVING THE MANAGEMENT OF RELATIONSHIPS WITH PROMINENT INFLUENTIAL PERSONS

According to global standards, financial institutions need to pay close attention to people in prominent positions in the public sector. The amendments to the FIC Act has adopted this measure and broadened its scope to include people in the private sector who do business with government (those in senior positions responsible for high value procurement contracts).

IMPOSING UNITED NATIONS SECURITY COUNCIL FINANCIAL SANCTIONS

The amended Act establishes a legal framework to applying and administering financial sanctions emanating from United Nations Security Council Resolutions. The FIC will be responsible for administering the measures requiring accountable institutions to freeze property or transactions that are subject to these Resolutions.

The legislative amendments also bring South Africa's anti-money laundering and counter terror financing standards in line with recommendations made by the international standard setting body, the Financial Action Task Force (FATF).

This should augur well South Africa in 2019, when the FATF is scheduled to conduct a mutual evaluation of the country's implementation of measures to combat money laundering and terror financing.

RISK-BASED APPROACH: GREATER FLEXIBILITY AND INCLUSIVITY

Fundamental to the amendments in the Financial Intelligence Centre Act, 2017 (Act 1 of 2017) has been the introduction of a risk-based approach.

The regulatory framework for protecting the integrity of the South African financial system was originally set in place with the promulgation of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001). This has been further strengthened by the introduction of the risk-based approach to customer due diligence by the amendments to the FIC Act in 2017.

The intention of the risk-based approach is to introduce greater efficiencies and to offer a less burdensome and cost-effective alternative to prescriptive methods for institutions to meet compliance measures.

The risk-based approach requires the FIC, financial institutions, other accountable and reporting institutions and supervisory bodies to take steps to identify and assess the risk of doing business with their customers with a view to deciding how best to manage that risk. By rating their clients in terms of risk for money laundering and terrorist financing against specific products, services and other factors, institutions are able to allocate their resources more efficiently using the risk-based approach. Where money laundering or terror financing risks are amplified, stronger controls will be needed. Conversely, where there is low level of risk, fewer or a reduced amounts of controls will be needed.

As part of implementation of their risk-based approach, institutions need to know and practice the following:

• Institutional risk framework needs to be in writing – a risk management compliance programme
• The above programme needs to be regularly updated
• When doing client profiles in regard to money laundering and terror financing risk, consider these scenarios as high risk:

- **Type of client** – politically exposed persons, legal entities, non-face-to-face clients
- **Product type** – Internet accounts, private banking, money remittals, stock brokering, annuities, insurance products, off shore services, correspondent banking etc.
- **Geographical location** – Countries listed on terrorism and sanctions lists of governments and international organisations and non-members of the Financial ActionTask Force (FATF) or of a FATF style regional body.

RISK MANAGEMENT COMPLIANCE PROGRAMME

To meet compliance requirements of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), accountable institutions need to fulfil the following obligations:

• Client identification and verification using a risk-based approach
• Risk management and compliance programme using a risk-based approach
• Record keeping
• Reporting
• Appointment of a compliance officer
• Training of employees
• Registration with the FIC.

One of these obligations, the risk management and compliance programme, was introduced as part of the suite of amendments to the Financial Intelligence Centre Act, 2017 (Act 1 of 2017). Included in section 42 of the amended Act, this amendment obliges accountable institutions to develop, document, maintain and implement a risk management and compliance programme (RMCP).

The letter and spirit of institutions' RMCP need to be fully understood by their boards and senior management who need to actively lead the process to understand money laundering and terror financing risks that they need to take into account.

The RMCP is integral to the application of the amended FIC Act's risk-based approach. For institutions' to know how and to what extent they are vulnerable to money laundering and terrorist financing, they need to conduct a risk assessment, which in turn will help them determine the extent of resources required to mitigate that risk.