FINANCIAL SERVICE PROVIDERS HAVE AN IMPORTANT ROLE TO PLAY IN THE FIGHT AGAINST MONEY LAUNDERING

Criminals are becoming increasingly adept at finding ways to hide, conceal, or disguise their proceeds of unlawful activities using corporate vehicles, such as listed companies, to evade detection by law enforcement.

Listed companies are often used as conduits for criminals to hide their ill-gotten gains where they seek to purchase shares of large national and international entities to create layers of opaqueness and hide behind the proverbial corporate veil or remain anonymous.

Certain obligations have been placed on the accountable institutions, such as financial service providers, in terms of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act).

The compliance obligations are geared to protect the financial system and its institutions, and to strengthen them against abuse. Certain of these obligations are highlighted below.

Accountable institutions are required to follow a risk-based approach to combatting money laundering (ML), terrorist financing (TF) and proliferation financing (PF). This entails assessing and identifying the level of inherent ML/TF/PF risk including the nature and complexity of their products and services, delivery channels, customer profiles, geographic location and countries of operation. The higher the ML/TF/PF risk the more stringent the compliance controls.

The accountable institution must develop, document, maintain and implement a risk management and compliance programme (RMCP) based on the unique risks they face. The RMCP can contain policy documents, and must detail all the processes, systems and controls used for risk management. This includes customer due diligence, record keeping, reporting and how a risk-based approach will be applied. Section 42 of the FIC Act sets out the requirements that must be covered in the accountable institution's RMCP. When dealing with a client, the accountable institution must identify and verify the client, understand the nature and intended purpose of the business relationship, as well as the source of funds. They must further establish the nature of the client's business as well as the ownership and control structure which assists in the identification of the beneficial owners.

Sanctions considerations

South Africa has adopted measures to combat the financing of the proliferation of weapons of mass destruction and related acts which includes regularly publishing the list containing particulars of persons and entities identified for targeted financial sanctions.

The targeted financial sanctions measures contained in the FIC Act relate to combating the financing of the proliferation of weapons of mass destruction as well as other instances of targeted financial sanctions-related to threats to the peace, breaches of peace and acts of aggression. Persons are listed on sanctions lists due to terrorist or related activities, threats to international peace and security, which includes the proliferation of weapons of mass destruction, oppressive regimes and/or human rights abuses. The FIC makes available one of the targeted financial sanctions lists on its website, while a consolidated sanctions list can be found on the website of the United Nations Security Council.

Accountable institutions are prohibited from acquiring, collecting or using property of persons or entities whose names appear in the targeted financial sanctions list. This includes providing financial services and/or products to those persons or entities. No person may transact with a sanctioned person or entity, or process transactions for such a person or entity.

Before an accountable institution establishes a business relationship or conducts a single transaction for a client, it must scrutinise the client information (this includes the client identity as well as beneficial owners and other authorised representatives' information) against the TFS lists.

Refer to sections 26A, 26B, 26C and 28A of the FIC Act and sections 4 and 25 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) (POCDATARA Act), as well as public compliance communication 44 and Guidance note 6A which are published on the FIC's website. The public compliance communication and guidance note provide further information on the sanctions regimes that apply in South Africa.

Guidance note 6A provides guidance on the reporting obligations as imposed by section 28A of the FIC Act and in terms of section 12 of POCDATARA Act.

Throughout the course of the business relationship, accountable institutions must monitor transactions including all complex, exceptionally large, and unusual patterns of transactions, that have no apparent business or lawful purpose.

Where the accountable institution identifies suspicious and unusual activity, it must file a report to the FIC in terms of section 29 of the FIC Act.

For more information refer to the FIC website (www.fic.gov.za) for the various FIC public compliance communications, guidance notes, reporting and registration user guides. You can contact the FIC's compliance contact centre on +27 12 641 6000 or log an online compliance query by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx.