IMPACT OF THE FIC ACT ON AUTHORISED USERS OF EXCHANGES

WHO IS THE FIC

The Financial Intelligence Centre (FIC) was established in terms of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001). The FIC together with the South African Reserve Bank and the Financial Sector Conduct Authority is empowered to regulate the financial sector on anti-money laundering and combating of terrorist financing.

The FIC's primary objectives include the identification of funds generated from criminal acts, and combating money laundering and terrorist financing, as well as the implementation of financial sanctions as imposed by the resolutions of the United Nations Security Council. In light of the latter, the FIC publishes a list of persons subject to targeted financial sanctions on its website.

Due to the vulnerability of identified financial and non-financial sectors to money laundering and terrorist financing abuse, the FIC Act imposes certain obligations on them as accountable institutions. This includes authorised users of exchanges.

All accountable institutions, listed as Schedule 1 items in the FIC Act, are required to fulfil obligations including registering with the FIC and submitting regulatory reports. Using the information provided by the accountable institutions, the FIC conducts analysis to develop financial intelligence reports. These reports are disseminated to domestic competent authorities such as the South African Police Service and the South African Revenue Service, as well as international partners and peers. The provision of financial intelligence to law enforcement and other competent authorities, therefore, is largely reliant on the fulfilment of compliance of obligations by institutions.

To update and inform institutions, the FIC provides guidance notes and public compliance communications. Examples of this are: Guidance note 4B which deals with suspicious and unusual transaction reporting; Guidance note 5B which deals with cash threshold reporting and Guidance note 6A deals with terrorist property reporting.

WHAT IS MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering refers to the concealing or disguising of the nature, source, location, disposing or movement of the proceeds of unlawful activities. Broadly, terrorist financing refers to the provision of funds, facilitating the transfer of funds and the sourcing of funds for terrorist and related activity, which funds could be from either illegal or legal sources.

FIC ACT AND AUTHORISED USERS OF AN EXCHANGE

Accountable institutions must comply with the obligations as set out in the FIC Act. The diagram below depicts a high level view of the FIC Act obligations which apply to all accountable institutions.

Penalties for non-compliance can include administrative sanctions and criminal prosecution. This may amount to a maximum of 15 years in prison or a fine not exceeding R100 million. Penalties depend on the contravention and the severity of the offence.

Accountable institutions are required to submit the following regulatory reports to the FIC:

- **Suspicious and unusual transaction reports (section 29 of the FIC Act)**
- **Cash threshold reports (on transactions of R24 999.99 and above) (section 28 of the FIC Act)**
- **Terrorist property reports (section 28A of the FIC Act)**

Accountable institutions must scrutinise their client information including client transactions, against the targeted financial sanctions list in order to identify whether their clients are included as listed persons or entities on the sanctions list.

Accountable institutions may use various factors when monitoring client transactions to identify potentially suspicious and unusual activity across a client's profile. The following are examples of factors that should be considered:

- **The client's source of income does not match with the incoming transaction amounts, the client's occupation and/or the sector they are involved in**
- **The use of nominees in attempts to conceal the identity of individuals involved in the transaction**
- **The client's income and/or turnover in previous financial years is notably lower that the current financial year, and also transaction patterns differ drastically from the client's transaction history.**
- **Transaction patterns indicating possible insider trading**
- **Activity related to tax evasion**
- **Transactions to and from high risk jurisdiction and/or high risk persons.**

HOW TO HELP BREAK THE CYCLE OF MONEY LAUNDERING

Effective reporting and completion of customer due diligence by the accountable institutions, plays a vital part in closing the gap when it comes to identifying money laundering. Suspicious and unusual transaction reports contain valuable information, and form the basis for the analysis and dissemination of intelligence by the FIC. The information contained in regulatory reports submitted by institutions enables the FIC to have an overview of money flows. It allows the FIC to identify how money moves from one person or entity to another, or even to see how different accountable or reporting institutions are being misused as vehicles for laundering money.

The FIC Act requires that anyone who is involved in a business directly or indirectly (i.e. employed by, owns or manages the business) must submit a section 29 report i.e. a suspicious and unusual transaction report. This is required if that person becomes aware of, or suspects that a transaction, and or activity may be related to either money laundering, terrorist financing and/or the financing of a person subject to targeted financial sanctions. Section 29 reports must be submitted within 15 days of forming a suspicion concerning a transaction or activity. The institution or business may proceed with the transaction even after a section 29 report has been submitted to the FIC. The purpose of the suspicious and unusual transaction report or STR, is simply to alert the FIC that it is suspected or known that a client may be abusing the entity for purposes of money laundering.

Information included in STRs assist the FIC in its development of financial intelligence reports. Law enforcement authorities, investigative agencies and prosecutorial authorities use the FIC's financial intelligence reports in their crime detection, investigation and prosecutions. Therefore, submitting STRs and other regulatory reports is how accountable institutions can contribute to fighting crime against the financial system and the country.

TARGETED FINANCIAL SANCTIONS

Financial sanctions imposed by the resolutions of the United Nations Security Council place restrictions on activities that relate to particular countries, goods, services, and/or persons and entities. Targeted financial sanctions measures generally restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property.

To effect these sanctions, the FIC Act requires accountable institutions to freeze property and transactions pursuant to financial sanctions imposed in the United Nations Security Council Resolutions. This obligation is outlined in section 26(A) of the FIC Act and it came into effect on 1 April 2019. The FIC carries a consolidated list of persons and entities included in resolutions of the United Nations Security Council on its website www.fic.gov.za. The list is available to users at no cost and it may be subscribed to for updates and alerts. Accountable institutions are required to screen the information relating to their new and existing clients, including transactions against the targeted financial sanctions list. This process should be clearly indicated in the accountable institutions' risk management compliance programme.

Should an accountable institution find that a client is on the targeted financial sanctions list, transactions must cease with that client. Should the accountable institution further identify that this client has in their possession terrorist property or that the client is in control of such property on behalf of a person or entity, then the accountable institution must submit a terrorist property report (TPR) in terms of section 28A(1)(c).