CREDIT PROVIDERS AND THEIR ROLE IN COMBATING MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

Recognised as being vulnerable to money laundering, terrorist financing and proliferation financing (ML, TF and PF), credit providers must adopt measures to avoid criminal exploitation. Credit providers can mitigate potential abuse by complying with the measures set out in the Financial Intelligence Centre Act (FIC Act).

Listed as accountable institutions in the FIC Act, credit providers must meet certain regulatory requirements. The FIC Act defines a credit provider, in terms of item 11 of Schedule 1, as a person who carries on the business of a credit provider as defined in the National Credit Act (NCA). The second category are persons who carry on the business of 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.

The FIC Act obligations include developing a risk management and compliance programme (RMCP), implementing a risk-based approach, conducting customer due diligence, screening clients against the targeted financial sanctions list, monitoring transactions, and registering with the FIC.

Due to intimate understanding of their operating environment, credit providers are best placed to determine their ML, TF and PF vulnerabilities. Credit providers must assess the risks they face on an entity wide level.

Once a credit provider has a holistic picture of their ML, TF and PF risks, they can implement controls proportionate to the risks.

Registration with the FIC

All accountable institutions, including credit providers, must register with the FIC to be able to meet their regulatory obligations. By registering, credit

providers will have access to the FIC's reporting platform, called goAML.

Should an accountable institution be listed under multiple Schedule 1 items i.e. a credit provider and a high-value goods dealer, they must register separately for each item. This is referred to as dual registration. Refer to public compliance communication (PCC) 5D in this regard.

Reporting to the FIC

As part of their FIC Act obligations, credit providers must report suspicious and unusual activities and/or transactions relating to their business to the FIC in terms of section 29 of the FIC Act.

Section 29 reports should be made in relation to suspicions concerning the proceeds of unlawful activities, money laundering, terrorist financing and financial sanctions offences as opposed to criminal activity in general.

A suspicious and unusual transaction report (STR) is filed where a transaction is completed while a suspicious activity report (SAR) relates to a transaction that is incomplete or abandoned. 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.

How is money typically laundered via credit providers?

Not all credit providers' products, clients or transactions bear the same ML, TF and PF risks and it is up to the accountable institution to determine their level of exposure to potential abuse.

Illicit funds could, for example, be laundered via the sector through early repayment of loans or the use of the loans to commit crime. The FIC's 2022 assessment of ML, TF and PF risks inherent to the sector found that cash was still largely used for loan repayments, whether directly or into the credit provider's bank account. This practice raises the level of risk for potential money laundering, and credit providers should take special care when dealing with cash transactions.

Targeted financial sanctions

The FIC publishes a targeted financial sanctions (TFS) list of all persons and

entities designated on the United Nations Security Council's (UNSC's) consolidated list. TFS measures restrict designated persons and entities from having access to funds, property and from receiving financial services. No person may transact with or process transactions for a designated person or entity.

Where an accountable institution knows that it possesses or controls property of a designated person or entity, the institution should submit a terrorist property report (TPR) to the FIC. The accountable institution is required to freeze the person's funds and services provided, refer to public compliance communication 44A for guidance on TFS.

Beneficial ownership

The FIC Act requires accountable institutions to establish and take reasonable steps to verify the beneficial owners of clients. In doing so, the accountable institution gains an understanding of who ultimately receives the benefits from a client.

Trends show that criminals may exploit legal persons, trusts and partnerships to hide the ownership and control of funds generated from illegal activities or intended to be used for illegal activities.

When determining which natural person is the beneficial owner of a legal person, accountable institutions must follow a process of elimination:

- Identify the natural person who has a controlling interest in the legal person e.g. percentage of shareholding.
- If in doubt, the institution should identify the natural person who exercises control through other means e.g. nominee shareholders, power of attorney, court order.
- If a natural person is not identified, the institution should identify the natural person who exercises control over the management of the legal person e.g. executive officer, non-executive director or manager.

For further guidance in relation to beneficial ownership refer to PCC 59. Credit providers can find more information relating to their sector on the dedicated page on the FIC website.

For more compliance information and guidance offered to accountable institutions, refer to the FIC website (www.fic.gov.za). 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/