

CREDIT PROVIDERS ARE REMINDED OF THEIR FINANCIAL INTELLIGENCE CENTRE ACT OBLIGATIONS

The products and services offered by credit providers, such as loans and finance, make them vulnerable targets for money laundering and terrorist financing.

Illicit funds could, for example, be laundered via the sector through early repayment of loans or the use of the loans for illicit purposes. The sector has therefore been brought into South Africa's anti-money laundering and counter financing of terrorism (AML and CFT) regulatory fold to help mitigate the risk of criminal exploitation.

Credit providers are listed as accountable institutions under item 11 of Schedule 1 to the Financial Intelligence Centre Act (FIC Act) which obliges the sector to meet compliance obligations which will help assist in identifying the proceeds of crime and combating money laundering and terrorist financing (ML and TF).

Among these obligations are

- ✓ Establishing and verifying customer information, through customer due diligence,
- ✓ record keeping,
- ✓ appointing a person responsible for compliance,
- ✓ developing and implementing a risk management and compliance programme (RMCP),
- ✓ training employees on FIC Act compliance and the institution's RMCP, and
- ✓ submitting various regulatory reports to the FIC.
- ✓ The first step accountable institutions must take, however, before they can file a regulatory report, is to register with the FIC.

Compliance with these obligations strengthens the sector against ML and TF vulnerabilities while further enhancing and protecting the economy at large. The following risk indicators have been identified for the sector and includes (amongst others):

- The use of credit funds for illicit activities
- Borrowed funds being repaid within a shorter space of time, than the loan term

- Repayment amounts for loans are higher than originally agreed upon
- No reasonable explanation for this or the source of funds used
- Multiple cash repayments without plausible explanation for source of funds
- Clients hesitant to provide personal information and information on their proposed business
- The business being established does not make economic sense and does not fit into the profile of the borrower
- A change in the business or the business strategy of the borrower that does not make economic sense
- The client is part of a complex structure or group or is a trust established in a foreign jurisdiction
- The loan is serviced by a third party that was not part of the original transaction.
- Multiple loans are taken out which do not make sense or do not fit the economic profile of the client

Credit providers are urged to read the latest sector risk assessment of [credit providers](#) and the FIC's [draft public compliance communication 23A](#) which provides sector specific guidance to credit providers.

Registration with the FIC

Credit providers, falling within the ambit of item 11 of Schedule 1, must register as soon as possible on the FIC's [registration and reporting platform](#). Registration with the FIC is free and must be completed electronically using the online registration system, which is accessible via www.fic.gov.za.

Credit providers should read the [goAML accountable institutions registration guide](#) as well as the FIC's [PCC 5D](#) for guidance on how to register with the FIC.

Submitting a risk and compliance return

Credit providers must assess, identify, understand and then risk rate the inherent money laundering risks associated with their products, services, clients and geographical areas as some may pose higher risk for ML and TF.

The FIC designed a questionnaire (called a [risk and compliance return](#)) which enables the regulator to measure an individual credit providers' understanding of the ML and TF risks they face. In addition, the FIC can use the information to assess the inherent ML and TF risks in the sector and supervise them using a risk-based approach.

All credit providers are urged to submit, without further delay, their risk and compliance returns (RCRs) in respect of Directive 7. Credit providers that fail to submit their RCRs are [non-compliant](#) and may face administrative sanctions.

The RCR questionnaires can be accessed via the FIC website home page by scrolling down and clicking on the link: "Accountable Institutions: [File your 2023 risk and compliance return today](#)".

Reporting to the FIC

Accountable institutions, such as credit providers, must monitor client transactions to identify suspicious and unusual transactions and activities. There are three primary regulatory reporting streams for credit providers:

- Cash threshold reports (CTRs) (see [Guidance Note 5C](#) for further reading on CTRs)
- Terrorist property reports (TPR) (see [Guidance Note 6A](#) for further reading on TPRs)
- Suspicious and unusual transaction reports (see [Guidance Note 4B](#) for further reading on STRs).

Suspicious and unusual transaction or activity reports

Reports must be filed with the FIC without delay but no later than 15 days from a person becoming aware of the suspicious and unusual transaction or activity. Suspicious and unusual transaction reports (STRs) and suspicious activity reports (SARs) must be filed

regardless of the amount of money involved. There is no threshold amount which triggers the STR and SAR reporting requirement.

A suspicion may involve several factors that could seem insignificant but taken together may arouse suspicion concerning that situation. The reporter should evaluate the transactions and the client's history, background and behaviour when determining whether a transaction or activity is suspicious or unusual.

An accountable institution can continue with the transaction when an STR has been submitted to the FIC. However, they may not disclose that a report was submitted, nor the content of the report. Doing so would amount to "tipping off."

Targeted financial sanctions

Section 26 of the FIC Act requires that accountable institutions scrutinise client information, file terrorist property reports (TPRs) and freeze property where it is found that property is linked to a designated person or entity on the United Nations Security Council targeted financial sanctions list. The targeted financial sanctions (TFS) list, can be found on the [FIC website](#).

[PCC 44A](#) and the [TFS manual](#) provide guidance on the TFS obligations and the risk-based approach to combating terrorist financing and proliferation financing.

Freezing of property

In terms of section 26B of the FIC Act, no one may provide financial or other services to persons or entities designated on a TFS list. Credit providers are prohibited from establishing a business relationship or conducting a single transaction with designated persons or entities. This may include not releasing any property to the designated person or entity. This is referred to as an "asset freeze". The accountable institution must have processes in place to ensure that 'freezing' occurs immediately where it is in the possession or control of a designated person's property.

Terrorist property reports

Section 28A of the FIC Act requires accountable institutions to file a TPR with the FIC if the business knows that it possesses, or controls property linked to terrorism or designated persons and entities. It is an offence for an accountable institution to continue with the transaction when a TPR has been submitted to the FIC. TPRs must be filed without delay and no later than five days from the accountable institution becoming aware.

For more information and guidance, refer to the FIC website for various guidance notes and public compliance communications. Alternatively, contact the FIC's compliance contact centre on +27 12 641 6000 or log an online compliance query on the FIC website.