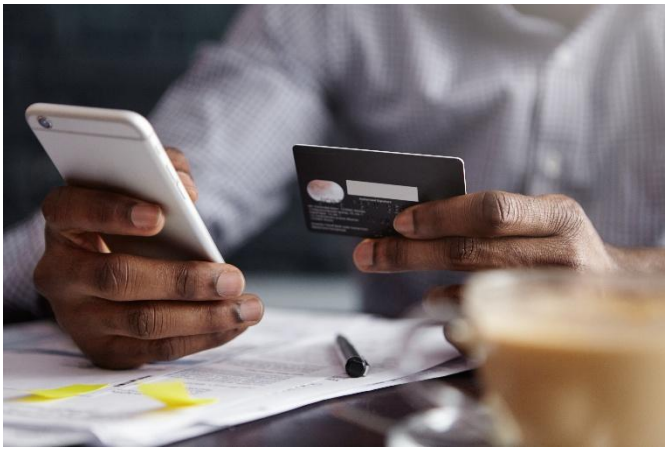
WHAT CREDIT PROVIDERS CAN DO TO AVOID THE MONEY LAUNDERING TRAP



Credit providers must be alert to the methods that criminals can use their exploit their services for money laundering and terrorist financing.

One of the ways is when clients repay their loans early or faster than planned or agreed upon using the proceeds of crime. Using this technique, criminals can introduce 'dirty money' into the financial system, giving it the appearance of legitimacy.

Credit providers can also be exploited to solicit, collect and provide funds and other assets to support terrorist activity, individual terrorists and groups. Unlike money laundering, financing for terrorism is not always generated through criminal activity or predicate crimes. This is because terrorism can be financed from both legal and illegal sources. For example, a home loan could be used to access funds to finance terrorist activities.

Listed as accountable institutions under item 11 of Schedule 1 to the Financial Intelligence Centre Act (FIC Act), credit providers must meet compliance obligations which will assist in identifying the proceeds of crime, combating money laundering, combatting terrorist financing and combatting the proliferation of weapons of mass destruction.

The Financial Intelligence Centre has issued Draft Public Compliance Communication 23A (PCC 23A), to provide additional clarity on the scope and interpretation of credit providers under Item 11 of Schedule 1 once finalised.

Compliance obligations for credit providers

In terms of Schedule 1 of the FIC Act, a credit provider is a person who carries on the business of a credit provider as defined in the National Credit Act (NCA) or someone who carries on the business

of providing credit in terms of any credit agreement that is excluded from the application of the NCA.

As accountable institutions, credit providers are required to comply with FIC Act obligations which include but are not limited to:

- Applying a risk-based approach to customer due diligence
- Record keeping in line with existing FIC Act requirements, which prescribe a minimum five-year retention period.

- Appointing a person responsible for compliance
- Developing and implementing a risk management and compliance programme (RMCP) that aligns with updated requirements set out in Guidance Note 7A, including enhanced entity-wide risk assessment, strengthened monitoring, and board-level accountability.
- Training employees on FIC Act compliance
- Submitting 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.

Regulatory reporting obligations

As part of their FIC Act obligations, accountable institutions must file regulatory reports that assist in combating money laundering, terrorist financing and proliferation financing. The three main regulatory reporting streams for accountable institutions are:

- cash threshold;
- suspicious and unusual transaction; and
- terrorist property reports.

In March 2025, the FIC issued Directive 3A and PCC 50A, which introduced mandatory procedures for accountable institutions that identify reporting failures or defective regulatory reports. Institutions must notify the FIC in writing immediately upon discovering a failure and engage with the FIC regarding remediation steps.

Cash threshold reports

Credit providers are required to report to the FIC cash transactions exceeding R49 999.99, including instances where the entity pays or receives funds from a client in cash in excess of the threshold.

Cash threshold reports should be submitted as soon as possible but no later than three working days after becoming aware of the cash transaction that has exceeded the threshold. For further guidance on cash threshold reporting, refer to Guidance Note 5C.

Suspicious and unusual transaction, and activity reporting

The obligation to report suspicious and unusual activities and transactions applies to all businesses in South Africa. Any person associated with a business and who knows or suspects that the business has received or is about to receive proceeds of unlawful activities must file a suspicious and unusual transaction report (STR).

STRs are submitted in respect of transactions while suspicious activity reports (SARs) are filed where the suspicion is about an activity or transaction which is incomplete, abandoned or cancelled.

Where the suspicion relates to financing of terrorist and related activities, the entity must either submit a terrorist financing transaction report or a terrorist financing activity report.

STRs should be submitted as soon as possible but no later than 15 working days after becoming aware of the facts which raise suspicion. Updated goAML User Guide V5.4 (September 2025) also introduces revised data-capture screens and submission processes that accountable institutions must follow when filing STRs and SARs.

For further information, refer to Guidance Note 4B.

Targeted financial sanctions

South Africa implements the targeted financial sanctions measures which originate from United Nations Security Council resolutions. It is prohibited to transact with a sanctioned person or entity, or to process transactions for such a person or entity.

Credit providers must screen their clients' information against the targeted financial sanctions list. When an accountable institution identifies a designated person or entity as a client or a person or entity who is linked to its client, it must immediately cease any activity in relation to that designated person or entity.

Credit providers must ensure screening is performed not only at onboarding but also when conducting transactions and when the TFS list is updated.

Additionally, the accountable institution must file a terrorist property report in terms of section 28A of the FIC Act, regardless of whether a transaction is concluded. The mere

attempt at making a transaction linked to a designated person or entity, warrants the submission of a terrorist property report.

Terrorist property reports must be submitted as soon as possible but no later than five working days after being aware that the institution has property associated with terrorist or related activities in its possession or under its control. For further guidance, refer to PCC 44A.

For compliance information and guidance, 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/

Possible indicators of money laundering in the provision of credit facilities to businesses and individuals include:

- Reversing transactions before repayments of loans have started, resulting in the borrowed funds being repaid within a short space of time.
- Repayment amounts for loans are higher or within a shorter time frame than originally agreed upon with no reasonable explanation for this or the source of funds used for the loan repayments.
- Multiple cash repayments without plausible explanation on source of funds.
- Clients hesitant to provide personal information, and/or information on their proposed business.
- Loan is serviced by a third party that was not part of the original transaction.

Possible indicators of terrorist financing in the provision of credit facilities may include:

- Mortgage credit facility paid up multiple times before the end of the agreement, and money is withdrawn continuously without a reasonable explanation.
- After several months of small regular payments there is a significant payment that has been deposited into the mortgage account without a reasonable explanation.

- Where the credit card holder makes multiple purchases at institutions that are outside of the country, but their economic activity does not justify doing so.