

TRUST AND COMPANY SERVICE PROVIDERS REMINDED OF THEIR COMPLIANCE OBLIGATIONS

Criminals may see companies – often trusts and similar legal arrangements – as vehicles to control criminally derived assets or conceal the origin of funds from illicit activity.

Trust service providers and company service providers (TCSPs) are listed as accountable institutions in schedule 1 to the Financial Intelligence Centre Act (FIC Act) due to the sector's potential exposure to money laundering and terrorist financing (ML and TF).

As accountable institutions, TCSPs must fulfil certain obligations in terms of the FIC Act. These include registering with and filing regulatory reports to the FIC.

ATCSP is a person who carries on the business of –

- Assisting their client in the creation, operation and management of a company, or of an external company, a foreign company or a close corporation
- Acting or arranging for an individual to act as nominee for their client, and
- Creating a trust arrangement for the client

The determining factors are activities where 'creation' can include registration of the client with the relevant authority; 'operation' entails assisting with the day-to-day operations of the client; and 'management' includes performing any active role, including decision-making.

REGISTRATION

Registration with the FIC is the first step for an accountable institution to play its part in the fight against financial crime. Once registered, the institutions can file the necessary regulatory reports with the FIC.

A person could provide multiple services listed in the definition of a TCSP. If so, the person must register as either a 'company service provider', a 'trust service provider' or both, depending on the services offered.

If the person falls under one of the other items listed under schedule 1 of the FIC Act, that person is required to register per schedule item. For example, if a legal practitioner provides any of the services under the TCSP definition, the legal practitioner is required to register as both a legal practitioner and a TCSP. (Refer to the goAML accountable institutions registration guide and PCC 5D for guidance on how to register.)

RISK INDICATORS

Each sector has inherent ML and TF vulnerabilities. TCSP services may be exploited, for example, by obscuring beneficial ownership or clients disguising the source of funds using complex structures. Understanding these sector-specific risks will assist TCSPs to adopt an effective risk-based approach:

SERVICES

- Unnecessary layers of complexity are added to the ownership structure e.g. trusts where the beneficiary of a trust is another trust
- Companies are purchased for no obvious commercial purpose
- It is apparent that there is no need for a TCSP in the transaction.

CLIENT LEVEL

- Profits generated by the company are inconsistent with their business activities.
- Searches of media coverage yield reporting or convictions of corruption on the client or their close associates.
- A company is registered with no links or activities in the jurisdiction where the company is established.

Refer to the FIC website for the sector risk assessments of company service providers and trust service providers and public compliance communication 6A for further risk indicators.

RISK AND COMPLIANCE RETURNS

In terms of directive 6 of 2023, TCSPs are urged to file their risk and compliance returns (RCRs) with the FIC without further delay.

The FIC designed the RCR questionnaire to enable accountable institutions to assess and understand their ML and TF vulnerabilities. Using its purpose-built risk and compliance analysis assessment tool, the FIC is able to use the information in the RCRs to understand TCSPs' risk and tailor its risk-



based supervision. As of the end of July 2024, approximately 76% of TCSPs registered with the FIC had submitted their RCRs.

Failure to submit RCRs may result in administrative sanctions. RCR questionnaires can be accessed on the FIC website: File your 2023 risk and compliance return today.

Accountable institutions can obtain confirmation of submissions by logging a compliance query. There is no requirement to resubmit the RCR for the 2024 cycle, however, if incomplete or inaccurate information was included in the submission then the TCSP is urged to resubmit.

REPORTING TO THE FIC

As accountable institutions, TCSPs must monitor client transactions to identify and report to the FIC, where necessary using the following regulatory reporting streams:

- Cash threshold reports (CTR) (see Guidance Note 5C)
- Terrorist property reports (TPR) (see Guidance Note 6A)
- Suspicious and unusual transaction reports (STR) (see Guidance Note 4B)

SUSPICIOUS AND UNUSUAL TRANSACTION/ACTIVITY REPORTS

Suspicious and unusual transaction reports (STRs) relate to the suspicion or knowledge regarding risks of ML and TF risk, for example if a transaction has no apparent lawful purpose. STRs must be filed without delay but no later than 15 days from becoming aware of the suspicious and unusual transaction or activity. There is no threshold amount which triggers the reporting obligation.

The reporter should holistically evaluate the transactions and the client's history when determining whether a transaction or activity is suspicious or unusual.

TCSPs may continue with the transaction unless directed otherwise (in writing) by the FIC. However, they may not disclose that a report has been submitted, nor the content of the report as this would amount to 'tipping off'. (Refer to Guidance Note 4B for further information on STRs.)

TARGETED FINANCIAL SANCTIONS

Strengthening South Africa's counter-terrorist financing framework is a major step towards the country exiting the Financial Action Task Force's grey list. Identifying terrorist financing risks and activities is a critical part of the exit plan, and accountable institutions play a crucial role in identifying these risks.

In terms of section 26 of the FIC Act, an accountable institution's targeted financial sanctions (TFS) obligations include a scrutinise–freeze–report approach:

- Scrutinising client information against TFS lists
- Freezing property of designated persons
- Filing terrorist property reports (TPR) and/or STRs where applicable

ATPR must be filed without delay, no later than five days from becoming aware, where it is found that property is linked to a designated person or entity on the United Nations Security Council's TFS list. The consolidated list can be accessed on the FIC website [here](#).

Where the TCSP only suspects, without actual knowledge, that a transaction or activity may be linked to a designated person or entity, then the TCSP must file an STR or suspicious activity report.

ATCSP cannot continue with the transaction when a TPR has been submitted. If no hit has been found on the client against the TFS list, the accountable institution may continue with the transaction. PCC 44A provides guidance on the TFS obligations and combating TF and PF. Webinars on how to scrutinise clients can be found on the FIC's YouTube channel.

Refer to the FIC website for further guidance notes and public compliance communications. Alternatively, contact the FIC's compliance contact centre on +27 12 641 6000 or log a compliance query on the FIC website.

AUTHOR

Walter Bhengu, Project Director: Legislation and Governance, Audit and Assurance at SAICA