FSCA

Financial Sector
Conduct Authority

FSCA Press Release **19 September 2025**

FSCA imposes administrative sanctions on DSL Solutions (Pty) Ltd (FSP 50891) and Opes Trust (FSP 45423)

The Financial Sector Conduct Authority (FSCA) has imposed administrative sanctions on the following financial services providers (FSPs) for failing to comply with certain provisions of the Financial Intelligence Centre Act, No. 38 of 2001 (FIC Act):

- DSL Solutions (Pty) Ltd (DSL); and
- Opes Trust (Opes).

Both entities are licensed FSPs under the Financial Advisory and Intermediary Services Act, No. 37 of 2002 (FAIS Act) and accountable institutions under the FIC Act.

The FSCA is responsible for supervising and enforcing compliance of FSPs with the FIC Act. The FIC Act aims, among other things, to help combat money laundering, the financing of terrorism and other related criminal activities. All accountable institutions designated under the FIC Act must comply fully with its requirements.

The FSCA conducted inspections on both DSL and Opes as part of its ongoing supervisory activities in terms of section 45B of the FIC Act. The inspections revealed the institutions to be in breach of the following provisions of the FIC Act:

- **Sections 42(1) and (2) - Risk Management and Compliance Programme (RMCP):** Accountable institutions must develop, document, maintain and implement an RMCP for anti-money laundering (ML), counter-terrorist financing (TF) and proliferation financing (PF). The RMCP must outline how an accountable institution will mitigate its ML/TF/PF risks and ensure compliance with the FIC Act.

  Although both institutions had developed RMCPs, they were found to be deficient in that the RMCPs failed to outline how the respective institutions would comply with

various FIC Act requirements. Additionally, neither institution could demonstrate that its RMCP was implemented effectively.

- **Sections 20A - 21H - Customer Due Diligence (CDD):** Accountable institutions are required to conduct ongoing customer due diligence which includes, among other things, the identification and verification of clients, obtaining beneficial ownership information and establishing if the clients or beneficial owners of clients are politically exposed persons.

  Both institutions failed to conduct the requisite customer due diligence as follows:
  - DSL failed to identify and verify the identity of clients, establish the source of funds and otherwise conduct ongoing due diligence.
  - Opes failed to verify the identity of clients, obtain information describing the nature of the business relationship and the source of funds, determine whether or not certain clients are politically exposed persons and otherwise conduct ongoing due diligence.

- **Section 28A read with section 26B - Targeted Financial Sanctions (TFS) screening:** Accountable institutions are required to scrutinise their client information to determine if any of their clients are listed on TFS lists.

  Both DSL and Opes failed to scrutinise client information against the United Nations Security Council TFS Lists published under the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, No. 33 of 2004 (POCDATARA Act), as required.

- **Section 29(1) - Reporting of Suspicious and Unusual Transactions:** Accountable institutions are required to file suspicious and/or unusual transaction reports with the Financial Intelligence Centre (FIC) and to ensure that the reports contain all relevant details as outlined in regulation 23A of the Money Laundering and Terrorist Financing Control Regulations (the Regulations).

  Moreover, accountable institutions are required to ensure that suspicious and unusual transaction reports (STRs) are successfully processed and that any failures/rejections are remediated accordingly.

Opes failed to complete all the details in the report as required by regulation 23A of the Regulations and did not remediate the rejected report.

- **Section 42A(2) - Governance:** An accountable institution which is a legal person must have a compliance function to assist the Board or senior management in discharging their obligations in terms of the FIC Act. Furthermore, a person with sufficient competence and seniority must be assigned to ensure the effectiveness of the compliance function.

  Both DSL and Opes did not have effective compliance functions to ensure that the respective institutions complied with the requirements of the FIC Act and their RMCPs.

In light of the above contraventions and based on an assessment of various factors applicable to each institution respectively, the FSCA issued directives to the institutions to remediate the identified deficiencies and imposed the following administrative sanctions:

- DSL was fined **R200 000.00** and cautioned not to repeat the conduct which led to the contraventions.
- Opes was fined **R500 000.00**, of which **R250 000** is conditionally suspended for two years.

The FSCA considers the identified compliance deficiencies to be serious breaches of the FIC Act. The requirement to understand and mitigate money laundering and terrorist financing risks through effective implementation of an RMCP is vital not only because it assists accountable institutions to protect and maintain the integrity of their own businesses but also because it helps contribute to the integrity of the South African financial system as a whole.

Proper due diligence of clients and screening against the TFS lists is crucial to help identify and mitigate against suspicious and criminal elements from infiltrating the financial system.

Filing STRs with the FIC is important for protecting and maintaining the integrity of the South African financial system and early detection of potential money laundering and

terrorist financing risks. The reporting of suspicious transactions and activities helps with the effective identification, investigation and prosecution of financial crimes.

The above sanctions serve as reminders that the FSCA will not tolerate non-compliance with the FIC Act. All accountable institutions are urged to continually review and enhance their anti-money laundering and terrorist financing controls at the highest levels and to conduct thorough risk assessments on a regular basis. Failure to do so will result in firm regulatory action.

ENDS

Enquiries: Financial Sector Conduct Authority
Email address: Communications@fsca.co.za
Telephone: 012 422 2842