



Risk Management & Compliance Program

in terms of Section 42 of the Financial Intelligence Centre Act, No. 38 of 2001 for FSP Solutions (PTY) Ltd (Co. Reg. 2003/000619/07)

The Board of Directors and shareholders are responsible for the RMCP's approval, development, documentation, implementation & maintenance.

Date of Compilation	March 2022
Last Review Date	September 2025



CONTENTS

01: Introduction	03
02: Overview of FSP Solutions (PTY) Ltd	04
03: Definitions	05
04: Introduction to the FSP's RMCP	08
4.1 The FSP's Risk Rating Indicators	08
4.2 The FSP's Risk Criteria Indicators	08
4.3 The FSP's Distribution Model	08
4.4 The FSP's Risk Rating applicable to this Product & Distribution Model	09
4.5 Foreign prominent public officials, domestic prominent influential persons and their family members and their known close associates	09
4.6 Customers Due Diligence Procedures (CDD)	09
4.7 Compliance Risks & Controls	10
4.8 FICA Awareness Training	11
4.9 FICA Reporting Duty	11
4.10 The Implementation of this RMCP	11
4.11 Approval of the RMCP	11
4.12 Appointment of FICA Compliance Officer	12
4.13 Offences and Penalties	12
4.14 Reassessment of Risk	12



01 | INTRODUCTION

The purpose of FICA is to prevent money laundering and the financing of terrorism, which places the economy and constitutional order of any country at risk.

FICA seeks to fulfil this purpose by imposing certain obligations on Accountable Institutions, which are recognised as potential vehicles for money laundering and the financing of terrorism.

These obligations regulate the manner in which Accountable Institutions handle money and property in the course of their Financial Service providers dealings with Clients and Prospective Clients.

Financial service providers (and thus, FSP Solutions (PTY) Ltd), is one of 16 (sixteen) categories of Accountable Institution falling within the ambit of FICA.

The purpose of the RMCP is to formally document the commitment of FSP Solutions (PTY) Ltd to its obligations under the Financial Intelligence Centre Act, 38 of 2001, as amended by the Financial Intelligence Centre Amendment Act, 2017 and associated regulations and guidance notes as well as the Prevention of Organised Crime Act, 24 of 1999.

FSP Solutions (PTY) Ltd will not condone money laundering, and it will not knowingly conduct business with individuals or entities it believes to be engaged in unlawful behaviour related to money laundering.

The following legislation governs anti-money laundering and anti-terrorist financing requirements in South Africa:

- a) The Prevention of Organised Crime Act, 121 of 1998 (POCA);
- b) The Financial Intelligence Centre Act, 38 of 2001 (FICA); and
- c) The Protection of Constitutional Democracy against Terrorist and Related Activities Act, 33 of 2004 (POCDATARA).

This RMCP has been drafted in accordance with this legislation as read, where applicable, with the supplementary Regulations and Guidance Notes. FSP Solutions (PTY) Ltd will apply these rules to all operations to enable the business to comply with its obligations, set out in this document.

This RMCP is legally binding on all Employees, and any non-compliance therewith is to be regarded by the FSP as serious misconduct. Senior Management will approve this RMCP, and it will be subject to periodic reviews thereafter.



02 | OVERVIEW OF FSP SOLUTIONS (PTY) LTD

FSP Solutions (PTY) Ltd is licensed for the following categories of financial services: Category 1 Financial Services Provider, registered to sell Short-Term, Long-Term and Short-Term Commercial Insurance.

CATEGORY DESCRIPTION	Advice Automated	Advice Non-automated	Intermediary Scripted	Intermediary Other
CATEGORY I				
Long-Term Insurance subcategory A		X		X
Short-Term Insurance Personal Lines		X		X
Long-Term Insurance subcategory B1		X		X
Long-term insurance subcategory B2		X		X
Long-term Insurance subcategory B2-A		X		X
Long-term Insurance subcategory B1-A		X		X
Short-term Insurance Personal Lines A1		X		X
Short-Term Insurance Commercial Lines		X		X

goAML Reporting Entity ID: 42648

Predominant services include:

- Binder services for some of our insurer partners (20% activity);
- Outsource services for some of our partners (80% activity);
- Supply IT technology, Infrastructure, staffing & management to support the services listed above.

The FSP is licensed as a non-mandated intermediary with binding authority. The FSP does not deal with the public directly, and no consumer advice is given at any stage. The FSP only interacts with clients directly when acting for the insurer through its binding authority services.

The financial services on offer through The FSP are:

- Short-Term Insurance
- Funeral Insurance

The FSP only deals through authorised intermediaries as accountable institutions in terms of the services and products provided.



The likelihood of The FSP being used for money laundering, and or terrorist financing activities is low.

Money Laundering Compliance & Reporting Officer for FSP Solutions (Pty) Ltd:
Retha Botha, Operational Director of the Company.

FSP Solutions (Pty) Ltd has an office based in Tshwane, Gauteng.

03 | DEFINITIONS

In this RMCP, the following words and expressions bear the meanings ascribed to them:

The FSP

FSP Solutions (PTY) Ltd an accountable institution under the Act, referred to as 'The FSP' in this document.

The Act / FICA

The Financial Intelligence Centre Act, No. 38 of 2001 (also known as "FICA"), as amended by the Financial Intelligence Centre Amendment Act, 2017.

Accountable Institution

An accountable institution is any person or entity, as described in Schedule 1 of the Financial Intelligence Centre Act, No. 38 of 2001 that must ensure adherence to the legal requirements and responsibilities as set out therein. The FSP is an Accountable Institution as defined in the Act.

Business Relationship

A bilateral agreement / contractual arrangement between the client and The FSP. This together with the acceptance by The FSP to receive fees for services rendered, after customer due diligence processes has been passed. It typically contemplates a transaction, or a series of transactions over time.

Client

A 'client' in relation to an accountable institution, means a person who has entered into a business relationship or a single transaction with an accountable institution. In this case FSP Solutions (PTY) Ltd based on the nature of the business conducted and business rules in place. Limited to Funeral or Short-Term Insurance as per license category.



Client Risk Rating (Client Underwriting)

The process to identify, assess, understand, the Money Laundering and Terrorist Financing risks. To take Anti-Money Laundering and Counter-Terrorist Financing measures to mitigate those risks.

Controlling Person

A person who –

- exercises general executive control over and management of the whole, or a significant portion, of the business and activities of the entity; or
- regularly participates to a material degree in management as a whole.

Customer Due Diligence (CDD)

The steps and procedures taken to identify and verify clients, as referred to in Section 21 of the Act. For the purposes of abbreviation, it is also referred to as 'CDD'.

Enhanced Due Diligence (EDD)

The application of obtaining additional information and verification when a client is not classified as a low risk Client. For the purposes of abbreviation, it is also referred to as 'EDD'.

MLFT

Money Laundering and the Financing of Terrorism, where 'money laundering' refers to any practice through which the proceeds of crime are dealt with in order to obscure their illegal origins.

MLRO

The Money Laundering Reporting Officer.

PIP

A Prominent Influential Person refers to any individuals who are or have in the past been entrusted with prominent functions in a country and encompasses the immediate family members and known close associates of any client.

PIPs can be split into two distinct categories:

- **Foreign Prominent Public Officials (FPPO):** Individuals who hold or have held prominent positions at any time during the preceding 12 months in a foreign country.
- **Domestic Prominent Influential Persons (DPIP):** Individuals who hold or have held (including acting positions exceeding 6 months) prominent positions within the Republic of South Africa.

**POCDATARA**

The Protection of Constitutional Democracy Against Terrorism and Related Activities Act, No 33 of 2004, as amended from time to time.

Intermediary

For purposes of the questionnaire, the person who is authorised to complete the questionnaire and deal with the FSP on behalf of the Client.

Risk Officer

- a) Mrs. M.A Botha who has been charged with overseeing compliance with FICA and this RMCP; or
- b) if no specific person has been so charged or in Mrs. M.A Botha's absence, then the FSP's highest decision-making organ, all of the members of which shall be jointly responsible for the FSP's FICA and RMCP compliance.

Risk Rating

This is a term used to determine treatments / restrictions on new or existing client accounts based on the results of client profiling.

RMCP

Risk Management and Compliance Program, as envisaged by the Act.

Terrorist Activities

Any of the offences specified in POCDATARA, all of which relate to terrorism.

Transaction

A Transaction between The FSP and the Client under which The FSP will contract to render financial services to the Client.

Verification

The method to confirm information obtained in the identification process, is done by the intermediary as accountable institution.



04 | INTRODUCTION TO THE FSP'S RMPC

4.1 THE FSP'S RISK RATING INDICATORS ARE AS FOLLOWS:

- Product Type
- Geography
- Domestic or International
- Nature of Clients
- Transaction Type Premium

4.2 THE FSP'S RISK CRITERIA INDICATORS ARE:

- Low risk = 1
- Medium risk = 2
- High risk = 3

4.3 THE FSP'S DISTRIBUTION MODEL

There are 3 parties to the distribution model. The intermediary, The FSP & the Insurer.

4.3.1) The Intermediary's role:

- Gather and verify and store information
- Do CDD, (if applicable do EDD)
- Give advice, issue instructions to issue policy via THE FSP

The intermediary is the Accountable party who gathers info and advises the client. MLFT verification processes all done by the intermediary.

4.3.2) The FSP's role:

- Capture or record the verified information as received from the intermediary on the system
- Do automated CDD via the system through comprehensive forced data requirements in order to issue policies
- Collect premiums & pay insurer and share policy data
- Assist registering a claim on behalf of the insurer

The FSP will not enter a business relationship with anonymous clients, or clients lacking data fields including ID, physical address, bank detail, occupation and many other (Automated CDD).

The FSP will also not issue a policy when:

- A client's shows unreasonable resistance, or unwillingness to confirm CDD information.
- There are inconsistencies between CDD information provided, or suspicious account activity and / or transactions occurs.



4.3.3) The Insurers role:

- Determine policy wordings, benefits, premiums and conditions
- Process & settle all claims

4.4 THE FSP'S RISK RATING APPLICABLE TO THIS PRODUCT AND DISTRIBUTION MODEL

4.4.1) Product Type:

By product type = low risk = 1 (Funeral policy with low cover options (maximum R10 000) & very low premiums less than R25 000).

4.4.2) Geography:

By Geography = low risk = 1 (limited to borders of RSA)

4.4.3) Domestic / International:

By Domestic or International = low risk = 1 (limited to RSA ID or passport holders only).

4.4.4) Nature of clients:

By nature of clients = Low risk = 1 (limited to private individuals only).

4.4.5) Transaction Type:

By transaction type = Low risk = 1 (limited to debit order deductions).

Legacy clients will be done via the same distribution model and subjected to same risk rating done by the intermediary, and The FSP's automated processes in place.

4.5 FOREIGN PROMINENT PUBLIC OFFICIALS, DOMESTIC PROMINENT INFLUENTIAL PERSONS AND THEIR FAMILY MEMBERS AND THEIR KNOWN CLOSE ASSOCIATES

The risk of The FSP being used for money laundering or terrorist financing by prominent public officials or domestic prominent influential persons, their family members or close associates is insignificant. Therefore, this section is not applicable.

4.6 CUSTOMERS DUE DILIGENCE PROCEDURES (CDD)

4.6.1) The FSP has adopted a risk-based approach with regards to performing a secondary Client Due Diligence, after receiving instructions from the intermediary:

- Via its automated processes
- Reviewing detail as received and measuring client's responses for accuracy
- and vagueness, when voice recorded underwritings are being done.

4.6.2) All employees responsible for interacting with clients and / or maintaining client and transaction records, will at all times observe the organisation's implemented control measures, and conduct the appropriate CDD procedures as outlined in the list on the next page.



RISK	LIKELIHOOD & RATING	CONTROLS
A customer makes inquiries that would indicate a desire to avoid reporting	<i>Possible with a medium rating</i>	FICA Training and Employee Reporting
Unusual business identified	<i>Possible with a medium rating</i>	FICA Training and Employee Reporting
A customer attempts to convince employee not to complete any documentation required for the transaction	<i>Possible with a high rating</i>	FICA Training and Employee Reporting
A customer has unusual knowledge of the law in relation to suspicious transaction reporting	<i>Possible with a low rating</i>	FICA Training and Employee Reporting
A customer seems very conversant with money laundering or terrorist activity financing issues	<i>Unlikely with a low rating</i>	FICA Training and Employee Reporting

4.6.3) Once an employee becomes aware of a suspicious or unusual transaction, it must be reported immediately. Every employee has a duty to approach Money Laundering Reporting Officer and to make a full disclosure of the facts and circumstances giving rise to such belief that a report to the FIC is required. Any documentation related to these facts and circumstances must also be brought to the attention Money Laundering Reporting Officer.

4.6.4) No employee is allowed to disclose any details about the suspicious, or unusual transaction to anyone else, unless this is required in terms of the FICA, or for the purposes of legal proceedings or in terms of an order of court. Employees are specifically not entitled to disclose any details about the report to the person who is the subject of the report. If by some coincidence, an employee becomes aware that another employee has made a report about a suspicious or unusual transaction, the duty of confidentiality is the same as if that employee had made the report.

4.6.5) Where employees responsible for interacting with clients and/or maintaining client and transaction records are unable to conduct a Client Due Diligence procedure for any reason, the employee will cancel the transaction and inform the Compliance Officer.

4.7 COMPLIANCE RISKS & CONTROLS:

4.7.1) The FSP has identified compliance risks given its compliance objectives and obligations.



4.7.2) The compliance risks have assessed and evaluated based on the likelihood of it occurring, and the impact should the event occur. Risks are rated from a high to low, pending the level of impact.

4.7.3) The controls put in place to mitigate and minimise these risks.

COMPLIANCE RISK	LIKELIHOOD	RATING	CONTROLS
Failure to report suspicious or unusual transactions	<i>Possible</i>	<i>High</i>	FICA Training and Employee Reporting
FICA CDD not completed	<i>Possible</i>	<i>High</i>	FICA Training
FICA requirements not implemented and reviewed	<i>Unlikely</i>	<i>High</i>	Annual review or updates when required
Brand damage if FICA awareness training not done with staff	<i>Unlikely</i>	<i>High</i>	FICA Training

4.8 FICA AWARENESS TRAINING

4.8.1) FSP Solutions (Pty) Ltd provide training to its employees to enable them to comply with the provisions of FICA and the RMCP.

4.8.2) The Training Portal allows FSP Solutions (PTY) to monitor staff's compliance on training related matters.

4.9 FICA REPORTING DUTY

4.9.1) Every employee of The FSP has a duty to report any suspicious transaction to the Company's Money Laundering Officer.

4.9.2) The duty to report is triggered when an employee becomes aware of a suspicious transaction.

4.10 THE IMPLEMENTATION OF THIS RMCP

All staff members are to be made aware of the existence of this RMCP which will be posted on the company's Training Portal & website. New versions of the RMCP will be posted on the same page and staff will be made aware of such changes for training and acceptance of the new version.

4.11 APPROVAL OF THE RMCP

This RMCP, and all amendments hereto, is approved by the Director and compliance team.



4.12 APPOINTMENT OF FICA COMPLIANCE OFFICER

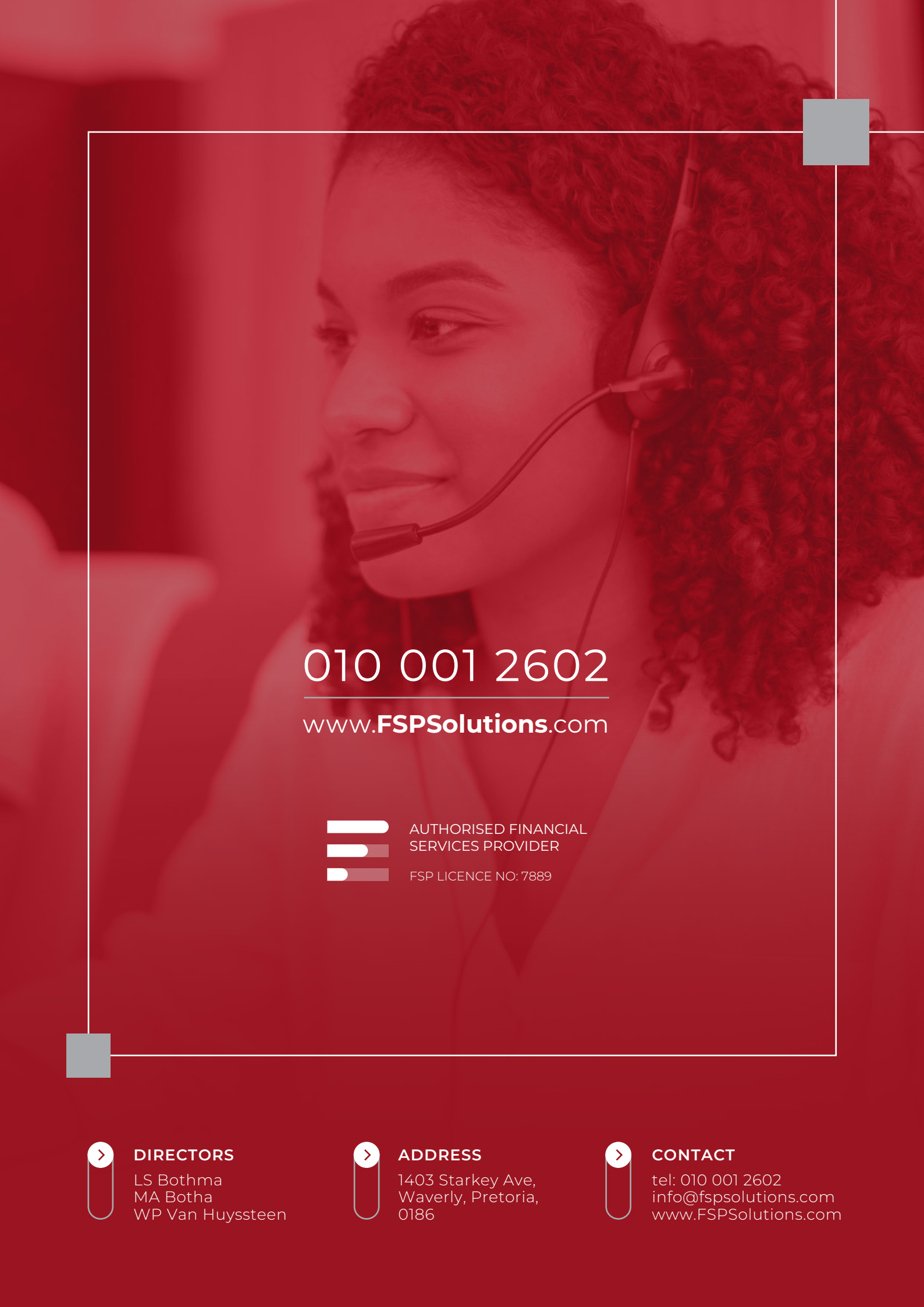
- a) FSP Solutions (Pty) Ltd MLRO: *Retha Botha*
- b) FSP Solutions (Pty) Ltd external compliance officer: *Askari Compliance Services*

4.13 OFFENCES AND PENALTIES

Failure to comply with this RMCP and / or the Financial Intelligence Centre Act, is an offence punishable by an internal sanction of this company and by harsh fines and prison sentences in terms of the Act.

4.14 REASSESSMENT OF RISK

This RMCP shall be updated and reviewed annually. This shall however not detract from the duty of management to update and amend this RMCP as and when additional risks occur, or when risk management is required.



010 001 2602

www.FSPSolutions.com



AUTHORISED FINANCIAL
SERVICES PROVIDER

FSP LICENCE NO: 7889



DIRECTORS

LS Bothma
MA Botha
WP Van Huyssteen



ADDRESS

1403 Starkey Ave,
Waverly, Pretoria,
0186



CONTACT

tel: 010 001 2602
info@fsp solutions.com
www.FSPSolutions.com