



**Financial Sector Conduct Authority  
Anti-Money Laundering/  
Counter Financing of Terrorism**

Body of Knowledge

Date: April 2022

## CONTENTS

1. INTRODUCTION .....	5
2. GLOSSARY .....	6
3. ACCOUNTABLE INSTITUTIONS .....	9
3.1. Explanation/legal definition.....	9
3.2. Examples of accountable institutions .....	10
3.3. Duties of accountable institutions.....	11
3.4. Frequently asked questions.....	12
4. BENEFICIAL OWNERS.....	13
4.1. Explanation/ legal definition.....	13
4.2. Examples of beneficial owners .....	15
4.3. How to identify and verify the identity of a beneficial owner .....	15
4.4. Frequently asked questions.....	15
5. CLIENTS .....	16
5.1. Explanation/ legal definition.....	16
5.2. Examples of clients .....	16
5.3. Single transactions and business relationships with clients .....	16
5.4. Frequently asked questions.....	17
6. COMPLIANCE OFFICER .....	18
6.1. Explanation/ legal definition.....	18
6.2. Examples of compliance officers .....	18
6.3. Duties of compliance officers.....	19
6.4. Frequently asked questions.....	19
7. DIRECTIVES.....	20
7.1. Explanation/ legal definition.....	20
7.2. Examples of directives .....	20
7.3. Purpose of directives .....	21
7.4. Frequently asked questions.....	21
8. ENFORCEMENT.....	21
8.1. Explanation/ legal definition.....	21
8.2. Examples of enforcement .....	22
8.3. Purpose of enforcement.....	22
8.4. Frequently asked questions.....	22
9. FIC/THE CENTRE .....	23

9.1.	Explanation/legal definition.....	23
9.2.	Duties of the FIC.....	23
9.3.	Frequently asked questions.....	24
10.	<b>FSCA.....</b>	<b>25</b>
10.1.	Explanation/ legal definition.....	25
10.2.	Functions of the FSCA.....	25
10.3.	Frequently asked questions.....	26
11.	<b>JURISTIC REPRESENTATIVES .....</b>	<b>27</b>
11.1.	Explanation/ legal definition.....	27
11.2.	Examples of juristic representatives .....	27
11.3.	Duties of juristic representatives.....	27
11.4.	Frequently asked questions.....	28
12.	<b>MONEY LAUNDERING .....</b>	<b>29</b>
12.1.	Explanation/ legal definition.....	29
12.2.	Examples of money laundering.....	29
12.3.	How to identify money laundering.....	30
12.4.	Frequently asked questions.....	30
13.	<b>POPIA.....</b>	<b>31</b>
13.1.	Explanation/ legal definition.....	31
13.2.	Examples of the application of POPIA in the AML / CFT environment.....	32
13.3.	POPIA v FICA .....	32
13.4.	Frequently asked questions.....	33
14.	<b>PROLIFERATION FINANCING (TFS) .....</b>	<b>34</b>
14.1.	Explanation/ legal definition.....	34
14.2.	Examples of proliferation financing.....	35
14.3.	How to identify proliferation financing.....	35
14.4.	Frequently asked questions.....	35
15.	<b>RECORD KEEPING .....</b>	<b>36</b>
15.1.	Explanation/ legal definition.....	36
15.2.	Examples of record-keeping .....	37
15.3.	Submitting details of third-party record keeper to FIC and FSCA.....	37
15.4.	Frequently asked questions.....	38
16.	<b>REGISTRATION .....</b>	<b>41</b>
16.1.	Explanation/ legal definition.....	41
16.2.	Examples of registration.....	41
16.3.	Registration platform .....	42

.....	43
16.4. Frequently asked questions.....	43
<b>17. RELIANCE ON THIRD PARTIES .....</b>	<b>45</b>
17.1. Explanation/ legal definition.....	45
17.2. Examples of reliance.....	45
17.3. Activities where assistance cannot be requested from another accountable institution:.....	46
17.4. Frequently asked questions.....	46
<b>18. SCREENING (TERRORIST PROPERTY AND TARGETED FINANCIAL SANCTIONS).....</b>	<b>47</b>
18.1. Explanation/ legal definition.....	47
18.2. Examples of screening.....	48
18.3. Screening results related to reporting obligations.....	48
18.4. Frequently asked questions.....	49
<b>19. SECTOR RISK ASSESSMENT.....</b>	<b>50</b>
19.1. Explanation/ legal definition.....	50
19.2. Examples of sector risk assessments.....	50
19.3. Purpose of sector risk assessments.....	50
19.4. Frequently asked questions.....	50
<b>20. TERRORIST FINANCING .....</b>	<b>52</b>
20.1. Explanation/ legal definition.....	52
20.2. Examples of terrorist financing.....	52
20.3. How to identify terrorist financing.....	52
20.4. Frequently asked questions.....	53
<b>21. UNALLOCATED FUNDS .....</b>	<b>53</b>
21.1. Explanation/ legal definition.....	53
21.2. Examples of unallocated funds.....	53
21.3. Processes and reporting duties.....	54
21.4. Frequently asked questions.....	54
<b>22. USEFUL LINKS .....</b>	<b>55</b>

## 1. INTRODUCTION

Section 45(1) of the Financial Intelligence Centre Act (the FIC Act) provides that every supervisory body is responsible for supervising and enforcing compliance with the FIC Act by all accountable institutions regulated or supervised by it. The Financial Sector Conduct Authority (the Authority) is a supervisory body tasked with this responsibility in relation to the financial services industry. In particular, accountable institutions listed under items 4, 5 and 12 of Schedule 1 to the FIC Act. The Authority delegated its power in relation to the supervision of authorised users (listed in item 4 of Schedule 1 to the FIC Act), to Exchanges licensed under the Financial Markets Act, No 19 of 2012.

The purpose of the Authority's AML/ CFT Body of Knowledge is to provide a practical tool for accountable institutions supervised by the Authority, assisting with creating a consistent understanding of AML/ CFT concepts dealt with on a day-to-day basis. The AML/ CFT Body of Knowledge will be reviewed and updated at least annually to ensure that it stays relevant in line with local and international AML/ CFT best practice.

This document contains simplified explanations of terms, policies and procedures in the AML/ CFT environment. As a result, the document is not a copy and paste of the FIC Act, regulations or guidance issued by the Financial Intelligence Centre (the FIC). The reader still needs to read the FIC Act, regulations or guidance issued by the FIC to understand the exact requirements of the FIC Act and obligations it places on accountable institutions. The Authority accepts no liability for any non-compliance or loss suffered as a result of reliance on this document. By clicking on the link below, you will be directed to the FIC's website where you will be able to find contact particulars of the FIC, the FIC Act, regulations and guidance issued by the FIC: <https://www.fic.gov.za/Pages/Home.aspx>

## 2. GLOSSARY

TERMINOLOGY	EXPLANATION
Accountable Institution <b>(AI)</b>	An FSP, MANCO or AU described in schedule 1 to the FIC Act. An AI has specific duties in terms of the FIC Act.
Anti-Money Laundering <b>(AML)</b>	Efforts to combat or mitigate money laundering.
Authorised User <b>(AU)</b>	An authorised user of an Exchange also referred to as stockbrokers
Cash Threshold Transaction Report <b>(CTR)</b>	Reports that must be submitted to the FIC in relation to receiving or paying out cash above R24 999,99
Collective Investment Scheme <b>(CIS)</b>	A unitized investment scheme
Collective Investment Schemes Control Act, 2002 <b>(CISCA)</b>	The Act that legislates unitized investment schemes and managers
Constitution of South Africa, 1996 <b>(Constitution)</b>	The supreme law of the Republic of South Africa
Customer Due Diligence <b>(CDD)</b>	The process of obtaining information from a client and verification thereof in line with the RMCP
Director <b>(Director)</b>	The Director of the Financial Intelligence Centre
Enhanced Customer Due Diligence <b>(ECDD)</b>	The process of obtaining additional information from a client and verification thereof in line with the RMCP

FICA Compliance Officer ( <b>CO</b> )	The person responsible to ensure that the FIC Act is complied with, in support of senior management
Financial Advisory and Intermediary Services Act, 2003 ( <b>FAIS</b> )	The Act that legislates the rendering of financial services
Financial Intelligence Centre ( <b>FIC/THE CENTRE</b> )	The entity that has been established in terms of the FIC Act to identify proceeds of crime, combat ML and TF and administer in South Africa the implementation of targeted financial sanctions by the United Nations
Financial Intelligence Centre Act, 2001 ( <b>FICA/the FIC Act</b> )	The Act implemented to mitigate and combat ML, TF and administer in South Africa implementation of targeted financial sanctions by the United Nations
Financial Markets Act, 2012 ( <b>FMA</b> )	The Act implemented to govern financial markets
Financial Sector Conduct Authority ( <b>FSCA/THE AUTHORITY</b> )	The Authority delegated the powers of a supervisory body in terms of the FIC Act
Financial Services Provider ( <b>FSP</b> )	A person or entity who renders financial services in respect of financial products
Financial Sector Regulation Act, 9 of 2017 ( <b>FSRA</b> )	The Act which establishes the Twin Peaks model, and provides for coordination and cooperation with the FIC
Johannesburg Stock Exchange ( <b>JSE</b> )	The largest stock exchange in Africa
Manager approved in terms of Cisca ( <b>MANCO</b> )	The manager of a CIS
Minister ( <b>Minister</b> )	The Minister of Finance

Money Laundering ( <b>ML</b> )	The activity of hiding, 'cleaning' or moving proceeds of illegal activities
Ongoing Customer Due Diligence ( <b>OCDD</b> )	The process of ensuring that CDD information and risk rating of the client is up to date on an ongoing basis
Protection of Personal Information Act, 4 of 2013 ( <b>POPIA</b> )	The Act which provides conditions for the processing of personal information
Proliferation financing ( <b>PF</b> )	The provision of funds or financial services used for the manufacture, acquisition, possession, or dealing with nuclear, chemical or biological weapons in contravention of national laws or, where applicable, international obligations
Risk Management and Compliance Program ( <b>RMCP</b> )	The plan developed by an AI which sets out the ML/TF risks identified and the controls to mitigate these risks and the measures introduced to comply with all other requirements of the FIC Act
Suspicious and Unusual Activity Report ( <b>SAR</b> )	A report that must be submitted to the FIC when an activity, which does not result in a transaction being completed but that is suspicious or unusual, is identified
Suspicious and Unusual Transaction Report ( <b>STR</b> )	A report that must be submitted to the FIC when a transaction that is suspicious or unusual is identified and is completed
Terrorist Financing ( <b>TF</b> )	The activity of financing terrorism and related activities



Terrorist Property Report ( <b>TPR</b> )	A report that must be submitted to the FIC when property related to terrorist activity is identified
--	--

### 3. ACCOUNTABLE INSTITUTIONS

#### 3.1. Explanation/legal definition

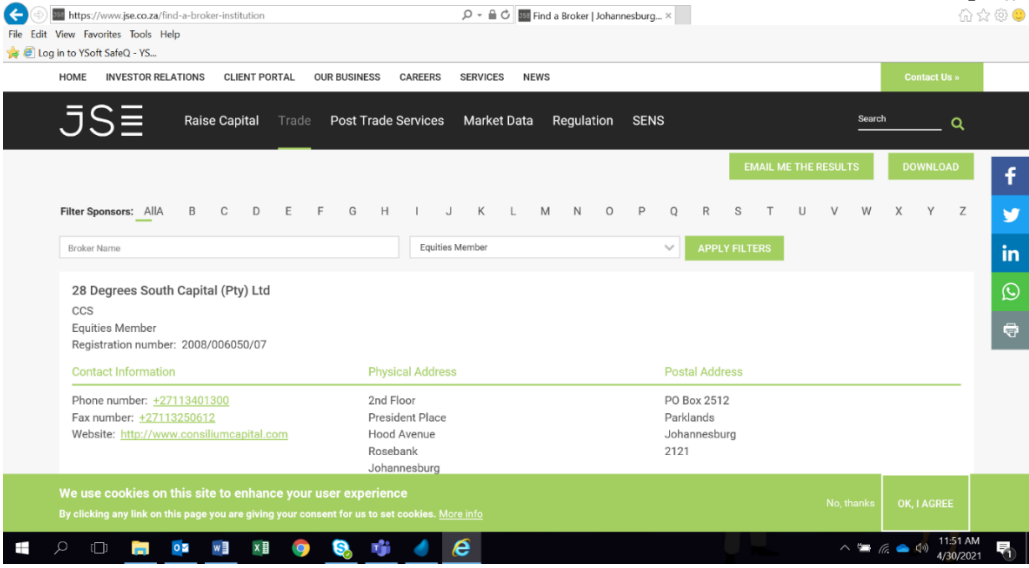
**“Accountable institution”** means a person referred to in Schedule 1 to the FIC Act.

An accountable institution includes but is not limited to:

- An authorised user of an Exchange as defined in the Financial Markets Act, 2012 (Act 19 of 2012) (item 4 of Schedule 1).
- A manager registered in terms of the Collective Investment Schemes Control Act, 2002, but excludes managers who only conduct business in part VI of the Collective Investment Schemes Control Act, 2002 (item 5 of Schedule 1).
- A person who carries on the business of a financial services provider requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, 2002, to provide advice and intermediary services in respect of the investment of any financial product (but excluding a short-term insurance contract or policy referred to in the Short-term Insurance Act, 1998 and a health service benefit provided by a medical scheme as defined in section 1(1) of the Medical Schemes Act, 1998).

### 3.2. Examples of accountable institutions

Example of an AU as per the official website of the JSE on 30 April 2021:



The screenshot shows the JSE website interface. The main content area displays details for '28 Degrees South Capital (Pty) Ltd'. The information is organized as follows:

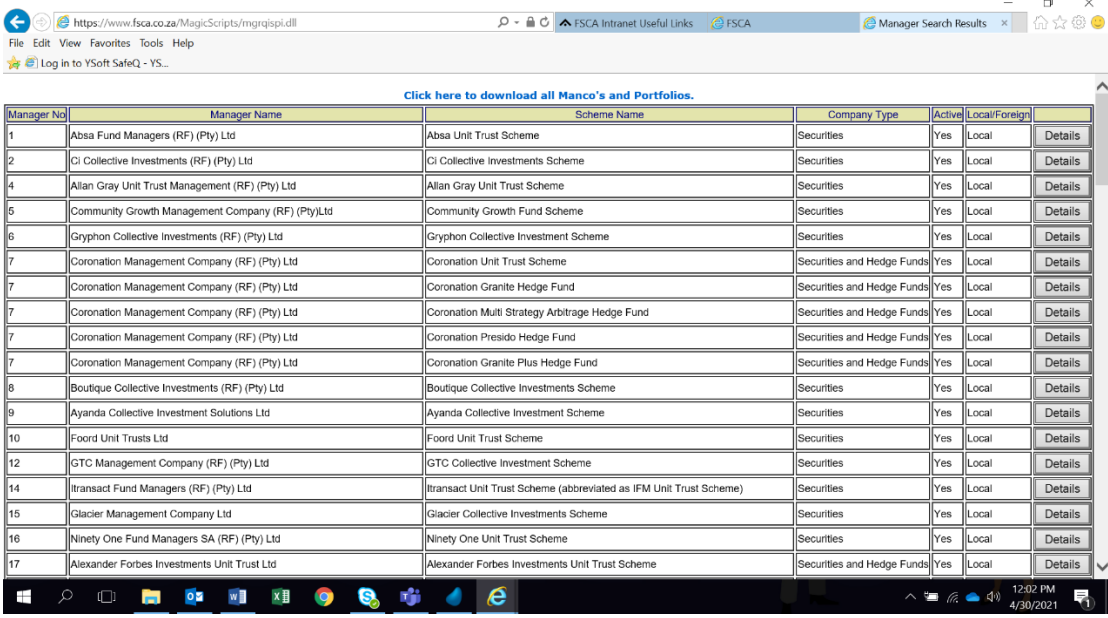
- Company Name:** 28 Degrees South Capital (Pty) Ltd
- CCS:** CCS
- Equities Member:** Equities Member
- Registration number:** 2008/006050/07

Below this, there are three columns of contact and address information:

Contact Information	Physical Address	Postal Address
Phone number: <a href="tel:+27113401300">+27113401300</a>	2nd Floor	PO Box 2512
Fax number: <a href="tel:+27113250612">+27113250612</a>	President Place	Parklands
Website: <a href="http://www.consiliumcapital.com">http://www.consiliumcapital.com</a>	Hood Avenue	Johannesburg
	Rosebank	2121
	Johannesburg	

At the bottom of the page, there is a cookie consent banner with the text: 'We use cookies on this site to enhance your user experience. By clicking any link on this page you are giving your consent for us to set cookies. More info'. Buttons for 'No, thanks' and 'OK, I AGREE' are visible.

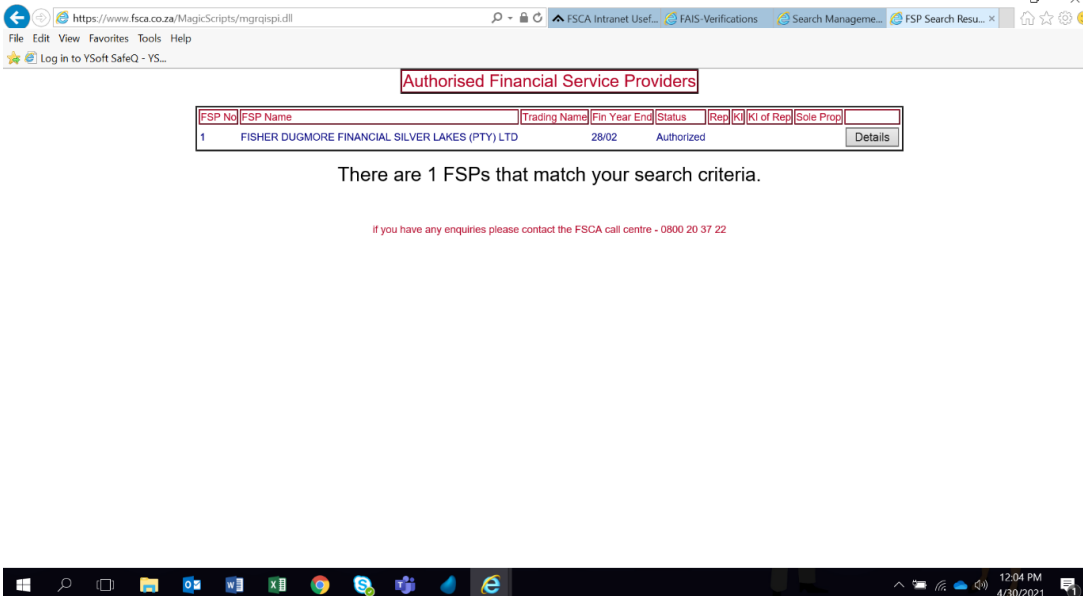
Example of CIS Manco as per the official website of the FSCA on 30 April 2021:



The screenshot shows a table titled 'Click here to download all Manco's and Portfolios.' on the FSCA website. The table lists various Manco entities and their associated schemes. The columns are: Manager No, Manager Name, Scheme Name, Company Type, Active, Local/Foreign, and Details.

Manager No	Manager Name	Scheme Name	Company Type	Active	Local/Foreign	Details
1	Absa Fund Managers (RF) (Pty) Ltd	Absa Unit Trust Scheme	Securities	Yes	Local	Details
2	CI Collective Investments (RF) (Pty) Ltd	CI Collective Investments Scheme	Securities	Yes	Local	Details
4	Allan Gray Unit Trust Management (RF) (Pty) Ltd	Allan Gray Unit Trust Scheme	Securities	Yes	Local	Details
5	Community Growth Management Company (RF) (Pty)Ltd	Community Growth Fund Scheme	Securities	Yes	Local	Details
6	Gryphon Collective Investments (RF) (Pty) Ltd	Gryphon Collective Investment Scheme	Securities	Yes	Local	Details
7	Coronation Management Company (RF) (Pty) Ltd	Coronation Unit Trust Scheme	Securities and Hedge Funds	Yes	Local	Details
7	Coronation Management Company (RF) (Pty) Ltd	Coronation Granite Hedge Fund	Securities and Hedge Funds	Yes	Local	Details
7	Coronation Management Company (RF) (Pty) Ltd	Coronation Multi Strategy Arbitrage Hedge Fund	Securities and Hedge Funds	Yes	Local	Details
7	Coronation Management Company (RF) (Pty) Ltd	Coronation Presidio Hedge Fund	Securities and Hedge Funds	Yes	Local	Details
7	Coronation Management Company (RF) (Pty) Ltd	Coronation Granite Plus Hedge Fund	Securities and Hedge Funds	Yes	Local	Details
8	Boutique Collective Investments (RF) (Pty) Ltd	Boutique Collective Investments Scheme	Securities	Yes	Local	Details
9	Ayanda Collective Investment Solutions Ltd	Ayanda Collective Investment Scheme	Securities	Yes	Local	Details
10	Foord Unit Trusts Ltd	Foord Unit Trust Scheme	Securities	Yes	Local	Details
12	GTC Management Company (RF) (Pty) Ltd	GTC Collective Investment Scheme	Securities	Yes	Local	Details
14	Itransact Fund Managers (RF) (Pty) Ltd	Itransact Unit Trust Scheme (abbreviated as IFM Unit Trust Scheme)	Securities	Yes	Local	Details
15	Glacier Management Company Ltd	Glacier Collective Investments Scheme	Securities	Yes	Local	Details
16	Ninety One Fund Managers SA (RF) (Pty) Ltd	Ninety One Unit Trust Scheme	Securities	Yes	Local	Details
17	Alexander Forbes Investments Unit Trust Ltd	Alexander Forbes Investments Unit Trust Scheme	Securities and Hedge Funds	Yes	Local	Details

## Example of authorised FSP as per the official website of the FSCA on 30 April 2021:



The screenshot shows a web browser window with the URL <https://www.fsc.co.za/MagicScripts/mgrqispi.dll>. The page title is "Authorised Financial Service Providers". Below the title is a table with the following data:

FSP No	FSP Name	Trading Name	Fin Year End	Status	Rep	KI	KI of Rep	Sole Prop	
1	FISHER DUGMORE FINANCIAL SILVER LAKES (PTY) LTD		28/02	Authorized					Details

There are 1 FSPs that match your search criteria.

If you have any enquiries please contact the FSCA call centre - 0800 20 37 22

### 3.3. Duties of accountable institutions

An accountable institution is required to:

- Not establish business relationships or conclude single transactions with anonymous persons or persons with apparent false or fictitious names (section 20A of the FIC Act).
- Identify and verify the identity of clients according to their ML/TF risks (section 21 of the FIC Act).
- Understand the nature and purpose of the business relationship as well as the source of funds of the client (section 21A of the FIC Act).
- Conduct additional due diligence on legal persons, trusts and partnerships (this is also referred to as beneficial ownership) (section 21B of the FIC Act).
- Conduct ongoing due diligence on clients (section 21C of the FIC Act.)
- Establish and conduct CDD of foreign prominent public officials, domestic prominent influential persons, their families and their known close associates (sections 21F-21G of the FIC Act).

- Maintain records of CDD and transactions (section 22 and 22A of the FIC Act).
- Perform screening in relation to targeted financial sanctions and freeze the property of clients that have been identified as appearing on the targeted financial sanction list (section 26B of the FIC Act).
- Perform screening in relation to clients associated with terrorist and related activities and cease the conducting of business with clients that own, or control property associated with such terrorist and related activities (section 28A of the FIC Act).
- Provide the FIC with information related to clients (section 27 of the FIC Act).
- Submit reports to the FIC (sections 28, 28A and 29 of the FIC Act).
- Provide additional information on reports submitted to the FIC on request of the FIC (section 32 of the FIC Act).
- Develop and implement an RMCP (section 42 of the FIC Act).
- Establish a compliance framework within the institution (section 42A of the FIC Act).
- Ensure training is performed and attended (section 43 of the FIC Act).
- Register with the FIC (section 43B of the FIC Act).

### **3.4. Frequently asked questions**

#### **3.4.1. I am a sole proprietor that does not accept client money. Am I still an accountable institution and should I comply with all these requirements?**

Unless you are exclusively authorised to render financial services in respect of short-term insurance and/or health service benefits, you are an accountable institution, regardless of the size of your business or whether you receive client money.

#### **3.4.2. I only sell funeral policies in terms of Long-term insurance category A. Am I still an accountable institution?**

Yes, you are an accountable institution.

### **3.4.3. My business is dormant. Must I still comply with the requirements related to an accountable institution?**

Yes, you are required to comply with all the requirements related to an accountable institution, at least as far as it relates to registration, understanding your ML/ TF risks and developing an RMCP and controls to combat ML/ TF risks.

### **3.4.4. My business has been suspended. Must I still comply with the requirements related to an accountable institution?**

When an FSP is suspended, the FSP is not allowed to render financial services until the status of suspension is reversed to “authorised” again upon the FSP’s remediation of whatever contravention that led to the suspension. The Authority must be satisfied that the FSP has become compliant. Provisional suspension is usually issued where the contravention/s are so serious that the suspension is prioritised. Suspension (provisional or not) can however be reversed to the status of “authorised” again. You would have to maintain compliance with your duties as an AI in the event that you (i) become authorised again or (ii) your clients are transferred to another AI due to withdrawal of your licence, in which case the clients must, for FIC Act purposes, be treated as new clients by the AI to which they are being transferred.

## **4. BENEFICIAL OWNERS**

### **4.1. Explanation/ legal definition**

**“Beneficial owner**, in respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly –

- (a) Owns the legal person; or
- (b) Exercises effective control of the legal person”

(See section 1 of the FIC Act)

A beneficial owner is only applicable where the client is a legal person i.e., a company, close corporation, foreign company or any other form of corporate arrangement or association.

A beneficial owner can only be a natural person.

The FATF definition of beneficial owner in the context of legal persons must be distinguished from the concepts of legal ownership and control. On the one hand, legal ownership means the natural or legal persons who, according to the respective jurisdiction's legal provisions, own the legal person. On the other hand, control refers to the ability to take relevant decisions within the legal person and impose those resolutions, which can be acquired by several means (for example, by owning a controlling interest in a block of shares).

However, an essential element of the FATF definition of the beneficial owner is that it extends beyond legal ownership and control to consider the notion of ultimate (actual) ownership and control. In other words, the FATF definition focuses on the natural (not legal) persons who owns and take advantage of capital or assets of the legal person; as well as on those who exerts effective control over it (whether or not they occupy formal positions within that legal person), rather than just the (natural or legal) persons who are legally (on paper) entitled to do so.

For example, if a company is legally owned by a second company (according to its corporate registration information), the beneficial owners are the natural persons who are behind that second company or ultimate holding company in the chain of ownership and who are controlling it. Likewise, persons listed in the corporate registration information as holding controlling positions within the company, but who are acting on behalf of someone else, cannot be considered beneficial owners because they are ultimately being used by someone else to exercise effective control over the company.

Another essential element to the FATF definition of the beneficial owner is that it includes natural persons on whose behalf a transaction is being conducted, even where that person does not have actual or legal ownership or control over the customer. This element of the FATF definition of beneficial owner focuses on individuals that are central to a transaction being conducted even where the

transaction has been deliberately structured to avoid control or ownership of the customer but to retain the benefit of the transaction.

#### **4.2. Examples of beneficial owners**

- Person A holds 100% ownership in a company. The company as a legal person becomes the client of an FSP. Person A is a beneficial owner.
- Person B holds the majority voting rights in a company. The company as a legal person becomes the client of an FSP. Person B is a beneficial owner.
- Person C is a trustee of a trust. The trust owns 60% shares in a company. The company as a legal person becomes the client of an FSP. Person C is a beneficial owner. It must however be noted that the nature of the trust and the position of the trustee and beneficiary must in each individual case be determined as the beneficiary may in some instances have vested rights in the property of the trust.

#### **4.3. How to identify and verify the identity of a beneficial owner**

- This applies to clients that are legal persons, trusts and partnerships.
- You can ask the client to tell you who the beneficial owner is.
- You can verify the information provided to you by the client by looking at the share register of a company/trust deed of trust to establish the veracity of the information provided by the client.
- You could look at corporate documents such as an organogram/board resolutions/minutes/directorships/memorandum of incorporation/annual shareholder meetings/Annual General Meeting etc. to establish which person exercises control over the client.

#### **4.4. Frequently asked questions**

##### **4.4.1. Is there a prescribed limit to shareholding constituting beneficial ownership?**

No, there is no prescribed limit. Using a risk-based approach, you can decide this for yourself. It has however been established that the lower the threshold, the more conclusive the results.

#### **4.4.2. Whose identity should be established when beneficial ownership is apparent?**

The identity of each natural person who, independently or together with other person/s, has controlling ownership interest/exercises control over the management of the client.

#### **4.4.3. To what extent should I go to establish the identity of a beneficial owner?**

You should comply with the requirements of section 21B of the FIC Act and must provide for the steps to comply with this section in your RMCP. This applies to both local and foreign beneficial ownership.

## **5. CLIENTS**

### **5.1. Explanation/ legal definition**

“**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”.

(See section 1 of the FIC Act)

### **5.2. Examples of clients**

- A natural person i.e. Joe Soap
- A legal person i.e. Joe Soap CC, Joe Soap (Pty) Ltd
- A trust i.e. the Joe Soap Trust
- A partnership i.e. Joe Soap Partnership

### **5.3. Single transactions and business relationships with clients**

- Business relationship means an arrangement between a client and an accountable institution for concluding transactions on a regular basis. This implies regular and ongoing contact between the accountable institution and



the client for purposes of performing transactions on behalf of a client during the life cycle of a financial product. An example would be where the accountable institution performs recurring transactions on behalf of a client in relation to an investment.

- Single transaction means a transaction, other than a transaction concluded during a business relationship; and where the value of the transaction is not less than R5 000.00. The accountable institution may not conduct a single transaction on behalf of a client who is anonymous or uses a fictitious name.

## **5.4. Frequently asked questions**

### **5.4.1. To what extent must I conduct CDD on a client when I perform a single transaction?**

You are not required to conduct the full scope of CDD measures if the value of the single transaction is below R5 000.00. You are however required to obtain some information from the client, although you would not need to verify such information. Examples would be the full name and identity number of the client as well as contact details. This is also to ensure that you are not dealing with an anonymous client, as no business may conclude a transaction with an anonymous client (refer to section 20A of the FIC Act).

### **5.4.2. I only conduct single transactions. Am I still an accountable institution?**

Yes, you are still an accountable institution, and you are required to comply with all the duties of an accountable institution. Your RMCP should provide detail of the nature of your business and the scope of CDD that you will perform on clients, albeit that the CDD requirements are limited in relation to single transactions below R5 000.00.

### **5.4.3. How do I know the difference between a business relationship and a single transaction?**

You are required to determine this in line with the context of your specific business and provide for this adequately in your RMCP so that your staff who are involved in rendering financial services to clients, will understand what the distinction is.

## **6. COMPLIANCE OFFICER**

### **6.1. Explanation/ legal definition**

A person with sufficient competence and seniority assigned to ensure the effectiveness of the compliance function of the accountable institution. The compliance function must assist the board/senior management in discharging their obligations in respect of the FIC Act and the RMCP. It must be noted that the responsibility for compliance with the FIC Act always remains the responsibility of the board of directors (in the case of a company)/senior management in the case of other (legal) entities (See section 42A of the FIC Act).

### **6.2. Examples of compliance officers**

A compliance officer can be any person, as long as the following two requirements are met:

- The person must be sufficiently competent:  
“Competence” is not defined in the FIC Act. However, on a practical level, competence relates to the person’s knowledge and experience in relation to AML/ CFT-related matters, as well as a comprehensive understanding of the size, nature and complexity of the AI’s business.
- The person must have seniority:  
Similarly, “seniority” is not defined in the FIC Act. However, on a practical level, seniority relates to the person’s position in the business of the AI, as well as the fact that the person can exert authority when providing guidance to the AI in relation to AML/ CFT-related matters and having an adequate level of independence. This implies that the person could be an employee in a senior position in the business of AI.

### 6.3. Duties of compliance officers

- Provide guidance to with the AI in relation to the development of AML/ CFT-related policies and procedures that meet the compliance obligations of the accountable institution in relation to the nature, size and complexity of its business. Compliance officers play a crucial role in the development and implementation of the RMCP as well as training of staff members.
- Monitor the effective implementation of the AML/ CFT-related policies and procedures by the AI.
- Escalate any deficiencies observed as a result of performing monitoring functions to the board/senior management.
- Ensure that deficiencies are timeously remedied and that the remedial action is effective to ensure that reportable transactions are identified and reported.
- Assist the AI to respond to requests for information by the Authority.
- Possess character qualities of honesty and integrity and perform its functions without fear or favour in the interest of combatting money laundering and the financing of terrorism and related activities.
- Ensure that all employees are trained in terms of the FIC Act and the RMCP so that employees are aware of and understand their legal and regulatory responsibilities including their role in combatting money laundering and financial crime.

### 6.4. Frequently asked questions

#### 6.4.1. If I am a sole proprietor, what constitutes “senior management”?

The person who is managing the business constitutes the senior management.

#### 6.4.2. Can I appoint an external compliance officer?

There is no prohibition on who can be appointed by the AI, except for the two requirements related to competence and seniority. If you contract with your compliance officer appointed for purposes of compliance with

the FAIS Act, you would be required to demonstrate how this person meets both these requirements. The requirement related to seniority in the business may then become difficult to comply with. An external compliance officer would not be able to assist with the identification and reporting of transactions to the FIC because of the confidentiality provisions. It is therefore suggested that an internal person is officially registered as the contact person and reporting on the FIC's registration platform. If necessary, such internal person may be assisted by an externally appointed person on condition that information relating to suspicious and unusual transactions is not shared with the externally appointed person. The FIC does not allow an external third party to register on the goAML profile of an institution.

## **7. DIRECTIVES**

### **7.1. Explanation/ legal definition**

A directive is an instruction issued by the FIC and/or the Authority (as a supervisory body) to do something such as to provide it with information in relation to the provisions of the FIC Act or to stop doing something that may be in contravention of the FIC Act. (See section 43A of the FIC Act).

### **7.2. Examples of directives**

- A directive to provide information/reports/statistical returns specified in the notice
- A directive to cease or refrain from engaging in an act/ omission/ conduct which could be interpreted as being in contravention of the FIC Act
- A directive to perform acts necessary to remedy an alleged non-compliance with the FIC Act
- A directive to perform any act necessary to meet any obligation imposed by the FIC Act

The Authority issued a Directive to Provide Information in 2021 which required accountable institutions to provide information in respect of their understanding of ML/ TF risk and compliance with the FIC Act.

### **7.3. Purpose of directives**

The purpose of directives is to obtain information from accountable institutions to assist the FIC and/or supervisory body to execute its functions and responsibilities in terms of the FIC Act. Such information could be required to assist with the analysis of financial intelligence or to assess the accountable institution's level of compliance with the FIC Act.

A directive is also used to instruct accountable institutions to remediate non-compliance detected or to prohibit continuing with actions that may lead to non-compliance with the FIC Act.

### **7.4. Frequently asked questions**

#### **7.4.1. I received a directive from the FIC. Is it compulsory for me to provide a response?**

Yes, responding to a directive within the period specified in the notice is compulsory.

#### **7.4.2. What are the consequences of failing to comply with a directive issued by the FIC or the Authority?**

An accountable institution that fails to comply with a directive is non-compliant and is subject to an administrative sanction. See "Enforcement" under para 3.6 below.

## **8. ENFORCEMENT**

### **8.1. Explanation/ legal definition**

**"Administrative sanction** means an administrative sanction contemplated in section 45C" (of the FIC Act). (See section 1 of the FIC Act). Enforcement is

the action taken against an accountable institution by the FIC and/or the Authority for failing to comply with the requirements of the FIC Act.

## **8.2. Examples of enforcement**

- 8.2.1.** A caution not to repeat the conduct which leads to non-compliance.
- 8.2.2.** A reprimand
- 8.2.3.** A directive to take remedial action or to make specific arrangements.
- 8.2.4.** The restriction or suspension of certain specified business activities.
- 8.2.5.** A financial penalty not exceeding R10 million in respect of any natural person and R50 million in respect of any legal person.

## **8.3. Purpose of enforcement**

The main purpose of enforcement is deterrence. Enforcement action must be appropriate, proportionate and dissuasive. Enforcement action is the consequence for non-compliance with the FIC Act and must be:

- appropriate in relation to the type and extent of non-compliance,
- proportionate to the nature, size and complexity of the business and
- dissuasive in that it discourages other accountable institutions from being similarly non-compliant and
- ultimately improves the industry's level of compliance with the FIC Act.

## **8.4. Frequently asked questions**

### **8.4.1. Are all sanctions issued against accountable institutions published?**

Yes, all sanctions that are issued against accountable institutions are published, unless if there are exceptional circumstances present that would justify the preservation of the confidentiality of the sanction. The mere fact that the publication of the sanction will damage the reputation of the institution is not exceptional circumstance. The publication of sanctions also serves as a dissuasive action to enhance the overall level of compliance by the industry.

#### **8.4.2. How does the Authority decide which sanction should be issued?**

The Authority relies on internal policies which provide for a matrix to commence the consideration for appropriate enforcement action. The Authority's enforcement process was developed in line with the enforcement methodology of the FIC and the Prudential Authority (PA). It is very important to note that this guidance provides touchpoints to commence the consideration but aggravating and mitigating factors related to each individual case impacts the final decision which is communicated with an accountable institution.

#### **8.4.3. I received a notice of sanction from the Authority. Can I appeal the decision?**

Yes, the FIC Act makes explicit provision for lodging an appeal against a decision of the FIC or a supervisory body (like the Authority). An appeal must be lodged in writing within 30 days from receiving the notice of sanction. Submission of an appeal must be accompanied by an affidavit containing, amongst others, full particulars of the appellant and proof of payment of the prescribed appeal fee (R10 000.00). (Refer to section 45D of the FIC Act and Regulation 27C of the Money Laundering and Terrorist Financial Control Regulations).

## **9. FIC/THE CENTRE**

### **9.1. Explanation/legal definition**

**"The Centre** means the Financial Intelligence Centre established as an institution outside the public service but within the public service administration as envisaged in section 195 of the Constitution". (See section 1 of the FIC Act).

### **9.2. Duties of the FIC**

#### **9.2.1. The objectives of the FIC include:**

- assist in the identification of the proceeds of unlawful activities
- assist in the combating of ML/ TF and related activities

- assist in the implementation of financial sanctions pursuant to some resolutions adopted by the Security Council of the United Nations
- to make information it collects available to specific institutions including supervisory bodies and law enforcement agencies
- to administer measures requiring AIs to freeze property and transactions pursuant to financial sanctions
- to facilitate effective supervision and enforcement by supervisory bodies

#### **9.2.2. The functions of the FIC include:**

- To process, analyse and interpret information disclosed to it and to inform, advise and co-operate with specifically mentioned institutions that include law enforcement agencies;
- to give guidance to AIs regarding their compliance with the FIC Act as it relates to registration and reporting obligations;
- provide guidance to AIs in relation to freezing property and transactions pursuant to financial sanctions;
- implement and maintain a registration system where AIs can submit intelligence reports to the FIC.

### **9.3. Frequently asked questions**

#### **9.3.1. Is the FIC and the Authority the same organisation?**

No. The FIC was established in terms of the FIC Act and operates as a financial intelligence unit. The Authority was established in terms of the FSR Act and operates as a market conduct regulator. The relationship between the FIC and the Authority lies in the designation of the Authority as a supervisory body in terms of item 1 of Schedule 2 to the FIC Act. The FIC, PA and the Authority have a close working relationship in order to combat ML/ TF and to ensure a consistent approach in supervision and enforcement of the FIC Act.



### **9.3.2. If I am supervised by the Authority as an accountable institution, should I engage with the FIC directly on any matter?**

Yes, you are required to engage with the FIC directly in respect of submitting reports on the FIC's GoAML system in relation to any reportable activity and transaction. For this purpose, you are required to register with the FIC and will, upon registration, be issued with an ORG ID number. You are further required to engage the FIC directly when responding to a directive issued by the FIC to provide them with information about your clients/transactions which may assist the FIC in executing its responsibilities. Queries on registration and reporting should be addressed to the FIC. The FIC may also contact accountable institutions relating to registration, reporting, awareness or guidance issued by the FIC.

### **9.3.3. How can I contact the FIC?**

- By visiting their official website at [www.fic.gov.za](http://www.fic.gov.za) and submitting a written enquiry
- By contacting them telephonically at 012 641 6000

## **10. FSCA**

### **10.1. Explanation/ legal definition**

“**Financial Sector Conduct Authority** means the authority established in terms of section 56 of the FSR Act”. It was established as a juristic person. It is a national public entity for the purposes of the Public Finance Management Act and the Commissioner is the accounting authority of the FSCA for purposes of that Act. (See section 1 of the FSR Act).

### **10.2. Functions of the FSCA**

In terms of the functions of the FSCA, it must, amongst other things:

- regulate and supervise financial institutions in accordance with financial sector laws;
- co-operate with other entities such as the PA and the FIC;

- promote sustainable competition in the provision of financial products and services;
- promote financial inclusion
- take steps to mitigate risks identified to the achievement of its objectives;
- focus on fairness and appropriateness of financial products and services;
- formulate and implement strategies for financial education for the general public.

### **10.3. Frequently asked questions**

#### **10.3.1. Why does the Authority supervise me as an accountable institution in terms of the FIC Act when it is a market conduct regulator?**

The Authority is a market conduct regulator in terms of the FSR Act. It is also a supervisory body in terms of item 1 of Schedule 2 to the FIC Act. By virtue of this designation, it is responsible for supervising accountable institutions listed in items 4, 5 and 12 of Schedule 1 to the FIC Act for FIC Act compliance (see “Accountable Institutions” above in the BOK).

#### **10.3.2. What is the FICA-related supervisory activities that the Authority performs on accountable institutions?**

The Authority performs both onsite and offsite inspections and supervisory activities on accountable institutions to test compliance by accountable institutions with the obligations of the FIC Act. The Authority is also responsible for creating awareness of the AML/ CFT requirements applicable to accountable institutions and to promote compliance with the FIC Act. Finally, we take enforcement action against accountable institutions that fail to comply with the FIC Act.

#### **10.3.3. How do I contact the Authority?**

- By visiting our official website at [www.fsca.co.za](http://www.fsca.co.za)
- By contacting us telephonically at 012 428 8000

## 11. JURISTIC REPRESENTATIVES

### 11.1. Explanation/ legal definition

“**Representative** means any person, including a person employed or mandated by such first-mentioned person, who renders a financial service to a client for or on behalf of a financial services provider, in terms of conditions of employment or any other mandate, but excludes a person rendering clerical, technical, administrative, legal, accounting or any other service in a subsidiary or subordinate capacity, which service does not require judgement on the part of the latter person, or does not lead a client to any specific transaction in respect of a financial product in response to general enquiries”.

“**Person** means any natural person, partnership or trust and includes any organ of State as defined in section 239 of the Constitution; any company incorporated or registered as such under any law; anybody of persons corporate or unincorporated”

(See section 1 of the FAIS Act)

A juristic representative is a legal person, appointed by an FSP, to render financial services to clients on behalf of the FSP.

### 11.2. Examples of juristic representatives

- XXX (Pty) Ltd appointed by FSP Y to render financial services to clients
- XXX CC appointed by FSP Y to render financial services to clients
- XXX Trust appointed by FSP Y to render financial services to clients
- XXX Partnership appointed by FSP Y to render financial services to clients

### 11.3. Duties of juristic representatives

The duty of a juristic representative is to render financial services in respect of financial products, to clients, as a regular feature of a

business, on behalf of the FSP who appointed the juristic representative. The appointment of a juristic representative forms part of the distribution

channel selected by the FSP to render financial services to clients. Juristic representatives are legal entities, and the rendering of financial services may not be its core function as the latter may even be unrelated to the rendering of financial services.

## **11.4. Frequently asked questions**

### **11.4.1. Is a juristic representative an accountable institution?**

No, a juristic representative is not an accountable institution in terms of item 12 of Schedule 1 to the FIC Act. It may well be an accountable institution or reporting institution in its own right in respect of other items in Schedule 1 or schedule 3 to the FIC Act, depending on its own core business activities. For example, Company A is a registered estate agent. For this reason, it is an accountable institution in terms of item 3 of Schedule 1 to the FIC Act. But Company A is also registered as a juristic representative of FSP B to sell life insurance products to new homeowners. Company A is not an accountable institution due to its registration as a juristic representative of FSP B.

### **11.4.2. Should a juristic representative register with the FIC?**

No. Since it is not an accountable institution by virtue of the fact that it is a juristic representative, it should not register with the FIC as an accountable institution from this perspective. See para 3.9.4.1 above in this regard as well.

### **11.4.3. Will the appointment of a juristic representative affect my exposure as an accountable institution to ML/ TF risk?**

As is the case with any distribution channel, you should consider the nature, size and complexity of the business of the juristic representative that you want to appoint. Any clients to which the juristic representative will render financial services to, are your clients and you remain fully responsible for all FIC Act obligations in respect of those clients. It is your responsibility to ensure that your juristic representative is trained on your RMCP as well as the FIC Act. It is also necessary to consider

the core business of the juristic representative that you appoint if it is not solely related to the rendering of financial services. It is possible that its core business activities are more vulnerable to ML/TF and related activities which may by extension impact you. The nature and business of juristic representations play an important role in the ML/TF risks of an institution. It is important that such risks are understood and, where necessary, mitigated and managed.

## 12. MONEY LAUNDERING

### 12.1. Explanation/ legal definition

**“Money laundering** means an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of the FIC Act or section 4, 5 and 6 of POCA”. (See section 1 of the FIC Act).

Investopedia describes money laundering as the illegal process of making large amounts of money generated by criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process launders it to make it look clean.

### 12.2. Examples of money laundering

- Duplicate payments/ “finger errors” requesting a refund
- Using illegally obtained credit card details/online banking passwords to purchase goods i.e., financial products and receiving the subsequent benefit thereof when funds or goods are moved to another account or sold
- Insisting on placing investments in jurisdictions known as tax havens
- Opening of bank accounts and transferring funds through such accounts
- Investing in financial products using illicit funds

- See the sector risk assessment for more examples.

### **12.3. How to identify money laundering**

The following are red flags:

- Evasive responses when asked about the source of the funds
- Investment actions make no business sense
- Inexplicable transactions
- Shell companies
- Unnecessarily complex corporate structures to hide the true source of the funds
- Early withdrawals
- See the sector risk assessment for more red flags.

### **12.4. Frequently asked questions**

#### **12.4.1. I do not accept cash from clients. Can my business still be used for money laundering?**

The reality is that the concept of “no-risk” does not exist. It is possible that the risk is lower when cash is not received from a client. However, there are several other risk factors that should be considered when identifying and assessing your ML risk. Important to understand is that risks are ever-changing, and criminals become more inventive and sophisticated by the day. It is also important to understand the nature, purpose and intention of the business relationship entered into with clients. De-risking as a concept should be avoided. It is discouraged to avoid risk as the focus should rather be on risk mitigation.

#### **12.4.2. I have known my clients for many years, and they are all good people. Why should I be concerned with money laundering?**

The only constant is change. This includes changes to economic circumstances of people and the advancement of technology. The

circumstances of clients, as well as their intentions and behaviour change over time. If you are not vigilant with regards to such changes taking place and how this could possibly impact your ML risks, you may become vulnerable to a client abusing your business for money laundering purposes.

#### **12.4.3. I have a small business. How can I make a difference in the effort to combat money laundering and terrorism financing?**

Combating ML and TF is the responsibility of every accountable institution and extends to a person who carries on a business, is employed by a business, is in charge of or manages a business (for purposes of submitting reports in terms of section 29 of the FIC Act). Once you deliberately identified and assessed your ML risk, you should be able to identify transactions and activities reportable to the FIC. Timeous and quality reporting to the FIC strengthens their ability to analyse the financial intelligence and package it for distribution to the relevant agencies for investigation and, where necessary, prosecution.

## **13. POPIA**

### **13.1. Explanation/ legal definition**

The Protection of Personal Information Act, 4 of 2013, aims to:

- Promote the protection of personal information processed by public and private bodies;
- Introduce certain conditions to establish minimum requirements for the processing of personal information;
- Provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- Provide for the issuing of codes of conduct;
- Provide for the rights of persons regarding unsolicited electronic communications and automated decision making;

- Regulate the flow of personal information across the borders of the Republic;
- Provide for matters connected therewith.

### **13.2. Examples of the application of POPIA in the AML / CFT environment**

- An AI obtains consent from a client for purposes of performing CDD and the client is made aware of the purpose for which the information will be processed.
- An AI submits a report to the FIC in relation to a suspicious and unusual activity/transaction which includes personal information of a client.
- The FIC makes a referral to the Authority in terms of section 44 of the FIC Act to further investigate allegations included in the referral based on the analysis of financial intelligence.

### **13.3. POPIA v FICA**

In terms of section 37 of the FIC Act, no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law agreement, affects compliance by an AI or supervisory body as it relates to:

- (i) Reporting duties and access to information
- (ii) Measures to promote compliance by AIs
- (iii) Compliance and enforcement

In terms of section 41A of the FIC Act, the FIC must ensure appropriate measures are taken in respect of personal information in its possession. It must take reasonable measures to:

- Identify all reasonable and foreseeable risks to personal information in its possession/ under its control.
- Establish and maintain appropriate safeguards against risks identified.
- Regularly verify that the safeguards are effectively implemented.
- Ensure that the safeguards are continually updated in response to new risks.



Section 38 of POPIA provides for an exemption in respect of certain conditions. In particular, any function:

- Conferred on any person in terms of the law, which is performed with the view to protect members of the public against:
  - (i) Financial loss due to dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or
  - (ii) Dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity.

The protection of personal information as provided for in POPIA is applicable to the FIC and the Authority, to the extent and limitation described above.

#### **13.4. Frequently asked questions**

##### **13.4.1. I am an AI and I am required in terms of the FIC Act to perform CDD on my clients. As a result, I must obtain personal information from my clients. Does POPIA prohibit me from obtaining this personal information from my client?**

No, you are required to obtain sufficient personal information from your client to ensure that you do not conduct business with an anonymous person or a person with a fictitious name. You are further obligated to perform CDD in line with your RMCP which has to provide for establishing the identity of beneficial owners and the source of funds used by the client when establishing a business relationship. You are however required to obtain your client's consent and make sure your client understands the purpose for which you intend to process their personal information. This includes the processes you will undertake as part of performing CDD in relation to verification of the information you

obtain from your clients which may or may not include verification of such information by an independent third party.

**13.4.2. I am an AI and I received a notice of inspection from the Authority. In the notice, they request copies of my client files for sampling as part of their inspection activities. Am I allowed to provide them access to my client files which includes personal information about my clients?**

The Authority has developed, in line with the requirements of POPIA, policies and procedures to ensure that it deals with personal information of people in their possession and under their control, in the manner provided for in POPIA.

The Authority is also delegated as a supervisory body in terms of the FIC Act and is required to execute such supervisory functions necessary to ensure compliance with the FIC Act by AIs. Personal information obtained as a result of performing such supervisory activities, including the sampling of client files which contains personal information, is permissible as provided for in POPIA.

## **14. PROLIFERATION FINANCING (TFS)**

### **14.1. Explanation/ legal definition**

Proliferation financing is the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

FATF Recommendation 1 states that countries should also identify, assess and understand the proliferation financing risks for the country. In the context of Recommendation 1, “proliferation financing risk” refers strictly and only to the potential breach, non-implementation or evasion

of the targeted financial sanctions obligations referred to in Recommendation 7.

#### **14.2. Examples of proliferation financing**

- Trade-in and financing of proliferation-sensitive goods i.e. dual-use goods
- Revenue-raising activities i.e. cybercrime and abuse of cryptocurrencies
- Financial and corporate networks i.e. North Korean diplomats facilitating North Korean sanctions evasion activities

#### **14.3. How to identify proliferation financing**

The following are red flags:

- Geographic and environmental elements such as porous borders
- Economic vulnerabilities such as constrained economies with limited resources
- Technological vulnerabilities such as weak cyber-security practices
- Social and political vulnerabilities such as maintaining cultural and diplomatic relations with North Korea or Iran

#### **14.4. Frequently asked questions**

##### **14.4.1. I am a small brokerage and am not involved in any activities related to financing of weapons of mass destruction. Why should I be concerned about proliferation financing?**

As an AI, you are required to identify and assess PF risk, ensure that your clients are screened against the targeted financial sanction lists, that assets are frozen where necessary and that reports are submitted to the FIC in this regard. PF is a risk that every country is exposed to in various degrees. Unawareness of PF risk and failure to report to the FIC in this regard, could result in a range of harmful consequences for the country, including but not limited to:

- Economic losses from illicit activity

- Reputational damage
- It is an indication of gaps in tackling other forms of financial and organised crime

#### **14.4.2. Which risk indicators should I consider when assessing PF risk?**

You should take into consideration all the risk indicators explained in Guidance Note 7 with a specific focus on geographic locations as well as PCC 49 which deals with ML/ TF/ PF risk relating to geographic areas. The features and activities related to a specific geographic area could serve as an indication of potential abuse for PF within a specific geographic area.

#### **14.4.3. What are dual-use goods?**

Dual-use items are goods, software and technology that can be used for both civilian and military applications which contribute to the proliferation of weapons of mass destruction. Examples include electronics, computers and navigation devices.

#### **14.4.4. Is there a specific body to control and manage matters related to the proliferation of weapons of mass destruction in South Africa?**

Yes, the South African Council for the Non-Proliferation of Weapons of Mass Destruction is a statutory body appointed by the Minister of Trade, Industry and Competition and was created for this purpose.

## **15. RECORD KEEPING**

### **15.1. Explanation/ legal definition**

Record keeping is an intrinsic activity in relation to CDD, transactions and an accountable institution's reporting obligations. The FIC Act does not prescribe how records should be kept, other than which records must be kept, the period for which such records must be kept and that records of prescribed information must be kept safe. Third parties may also be appointed by an accountable institution to keep its records. However, the

responsibility for ensuring that the records are kept safe and that free and easy access will be available at all times remains the responsibility of the accountable institution. (See sections 22, 22A, 23 and 24 of the FIC Act read with Regulation 20).

## **15.2. Examples of record-keeping**

Mechanisms that could be used for keeping records include:

- Internal networks
- Physical storage devices i.e. hard drives or files
- Cloud storage
- Electronic document repositories

## **15.3. Submitting details of third-party record keeper to FIC and FSCA**

If an accountable institution appoints a third party to store its records, it must provide the following details of such third party to both the FIC and the Authority:

- The third party's full name, if the third party is a natural person
- The third party's registered name, if the third party is a close corporation/ company
- The name under which the third party conducts business
- The full name and contact particulars of the individual who exercises control over access to those records
- The address where the records are kept
- The address from where the third-party exercises control over the records
- The full name and contact particulars of the individual who liaises with the third party on behalf of the accountable institution concerning the retention of the records

Should the details of the third-party record keeper change, the accountable institution should inform the FIC and the Authority of the relevant changes. The FIC can be informed of a third-party record

keeper by addressing correspondence to The Manager: Compliance Monitoring – Compliance and Monitoring Unit of the FIC.

## **15.4. Frequently asked questions**

### **15.4.1. Must I only keep records of CDD and transaction information?**

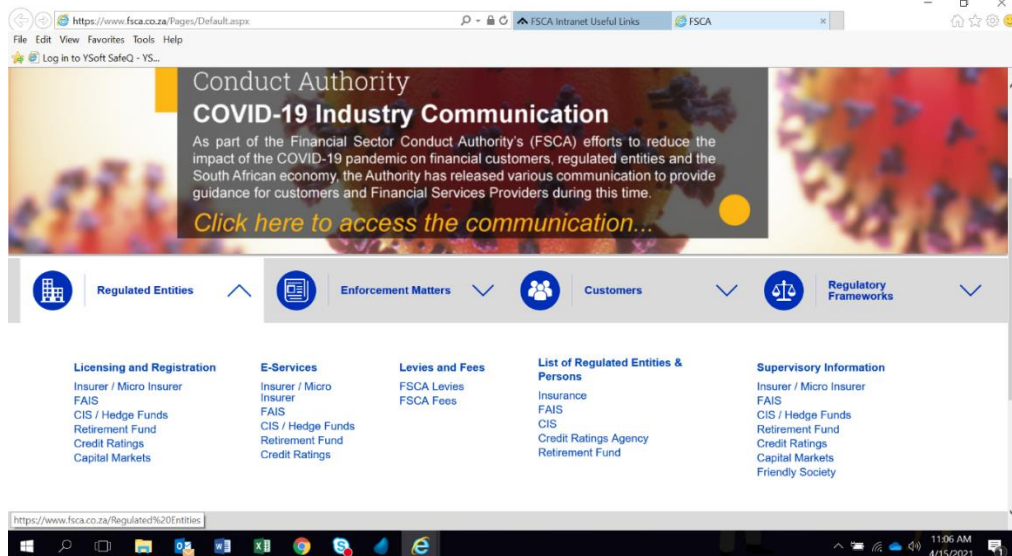
Record-keeping requirements are not dependent on risk levels and the accountable institution is required to keep records of all CDD and transaction information obtained from clients. In addition, an accountable institution should maintain records of all other information obtained in relation to a single transaction or business relationship as far as such records relate to all of the accountable institution's obligations under the FIC Act. Accountable institutions should also keep record of transactions and activity that gave rise to a report in terms of section 29 of the FIC Act. Proof of submission of STRs and CTRs should also be kept as evidence that transactions or activities have been reported to the FIC. Records should be kept for five years after date of termination of the business relationship/ conclusion of a single transaction.

### **15.4.2. How must I inform the Authority of the details of the third-party record keeper that I appointed?**

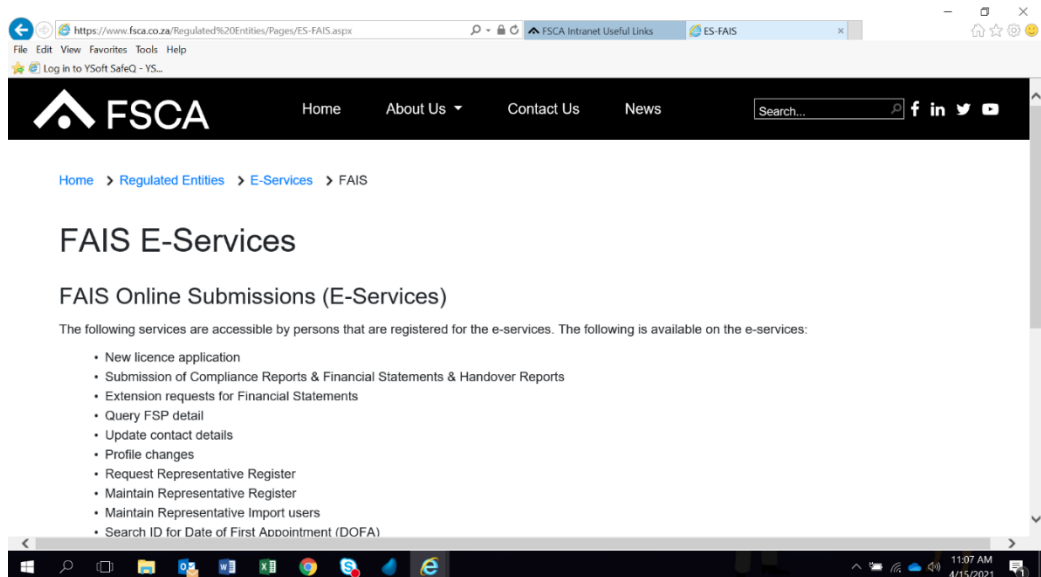
The Authority developed an online facility where you must capture the details referred to above under para 3.13.3 on the e-portal:

#### **Practical steps:**

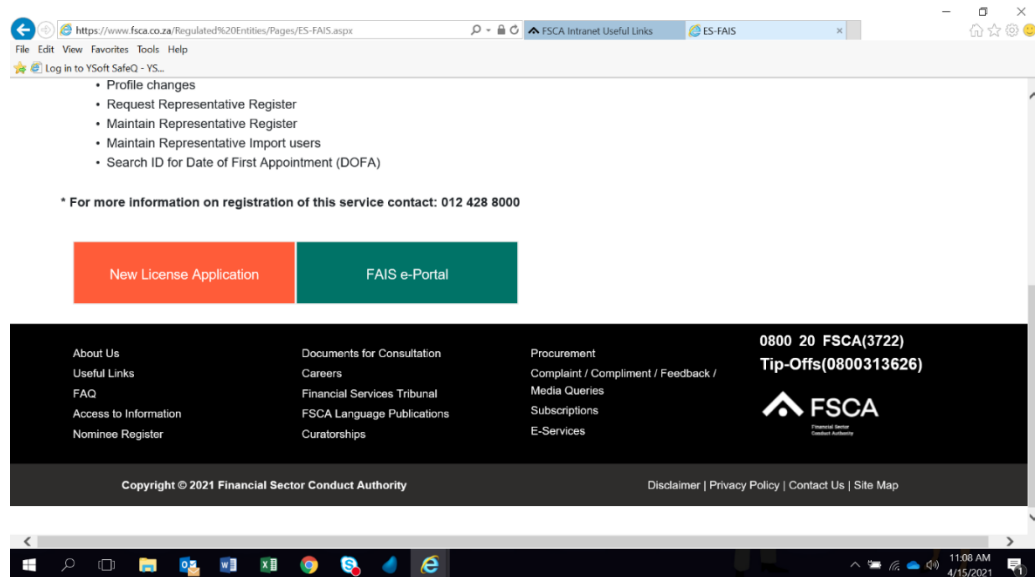
- **Search for the website of the Authority on the internet using the following address: [www.fsca.co.za](http://www.fsca.co.za)**
- **Scroll down to the bottom of the landing page to “Regulated Entities”:**



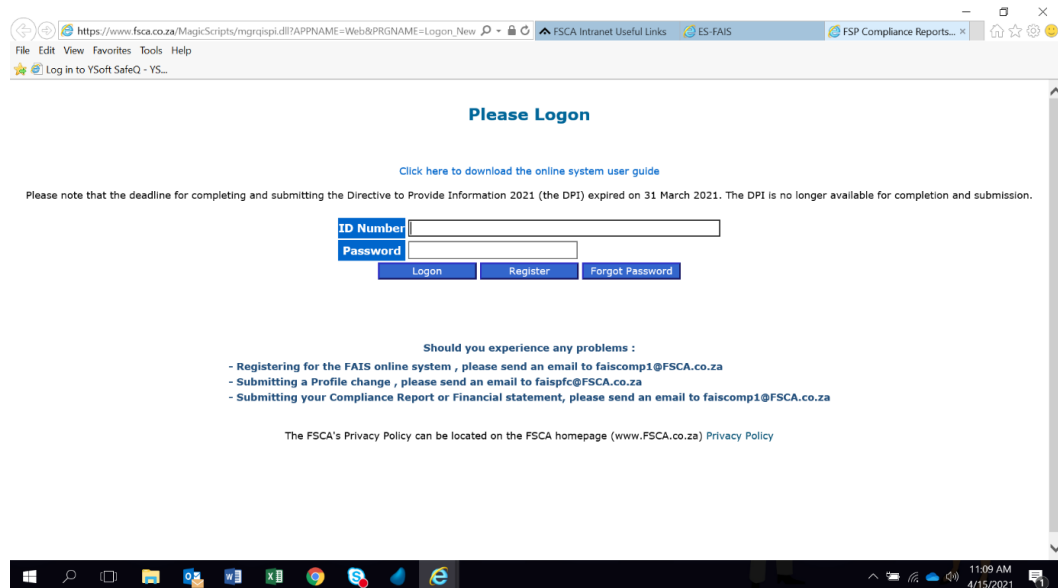
- **Second, from the left, there is a tab for E-Services. Click on “FAIS” (third from the top)**



- **Scroll down to the green block titled “FAIS e-portal” and click on the button:**



- **The logon/registration page is now visible:**



- **If you experience issues with registration on the FAIS e-portal**

Note that a dedicated e-mail address is provided: [faiscomp1@fsca.co.za](mailto:faiscomp1@fsca.co.za). If there are any issues with your registration, the system will automatically generate a notification to you explaining what the issue is i.e. your identity or passport number on record is invalid/ the e-mail address is incorrect etc. **Send an enquiry to**



[faiscomp1@fsca.co.za](mailto:faiscomp1@fsca.co.za) immediately and provide the following information to ensure we can focus our response to assist you:

- Your FSP number
- The name, surname and identity or passport number of the person registering (it MUST be a key individual)
- The correct e-mail address which should be used to send you the password required to log on
- A description of the issue that you experience i.e. your e-mail address must be updated

**Once registered, you will be able to access all the facilities on the FAIS e-portal including the facility to capture the details of your third-party record keeper.**

#### **15.4.3. Why should I provide this information to the FIC and the Authority?**

The details are required in the event that a warrant needs to be issued to obtain the records of an AI kept by a third party.

## **16. REGISTRATION**

### **16.1. Explanation/ legal definition**

Registration with the FIC is a legal obligation in terms of the FIC Act. See section 43B of the FIC Act. Registration enables an institution to fulfil its reporting obligations in terms of the FIC Act by submitting the transactions or activity to the FIC in electronic format.

(See <https://www.fic.gov.za/Compliance/Pages/Registration.aspx>).

### **16.2. Examples of registration**

Both accountable and reporting institutions are required to register on the FIC's GoAML system. Upon registration, you will be issued with what is referred to as an ORG ID number. This ORG ID number will then give you access to submit your reports to the FIC.

It is important to note that the ORG ID number is NOT the same as your own identity number/ the registration number of your business (where your business is a legal person). It should also NOT be confused with the Org ID number issued by the Council for Medical Schemes upon accreditation with them.

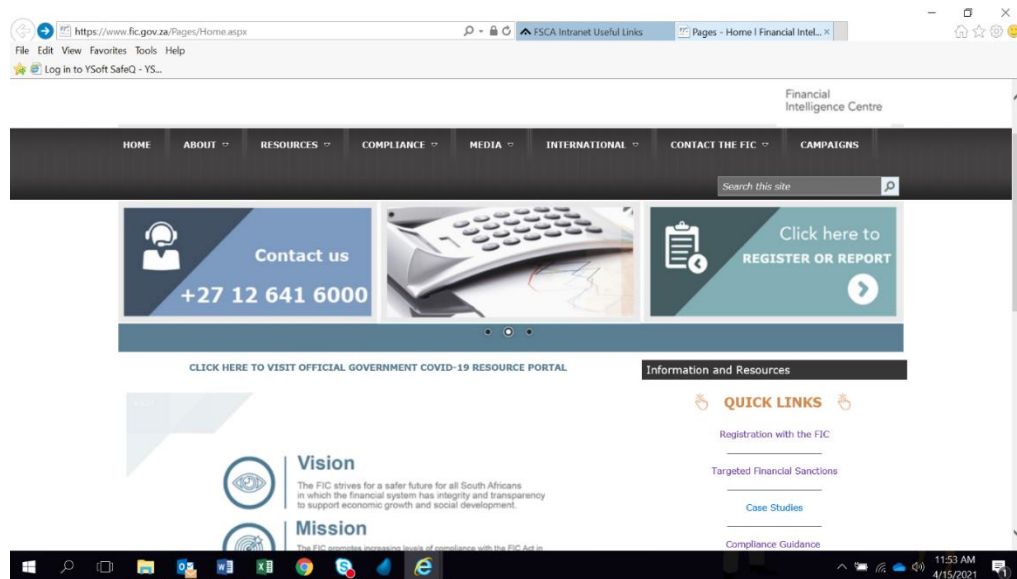
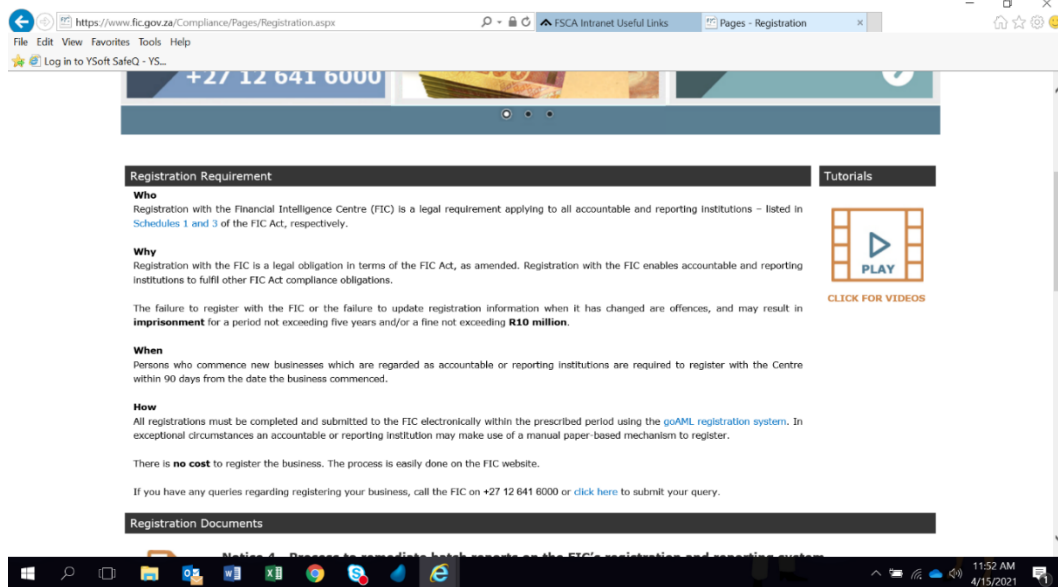
Finally, it is very important not to confuse the FIC's GoAML system with the e-portal of the Authority. The FIC and the Authority are not the same entity. You are not able to submit reports (as prescribed by the FIC Act) to the Authority. For example, you can only submit a cash threshold report/ a suspicious and unusual transaction report to the FIC.

### **16.3. Registration platform**

If you have not yet registered with the FIC on the GoAML system, you should immediately contact the FIC at 012 641 6000 or visit their website at [www.fic.gov.za](http://www.fic.gov.za).

On the landing page of the FIC's website, you will find a heading on the right-hand side in orange: **"Quick Links"**. Just below this heading, you must click on **"Registration with the FIC"**. On the next page, you will find all the information relevant to explain the registration process, including a tutorial video as well as a link at the bottom where you can click on **"click here"** to submit an enquiry to the FIC in relation to registration issues.

A screenshot is provided below to demonstrate the details provided on the FIC's website as explained above:



## 16.4. Frequently asked questions

**16.4.1. I am a newly authorised FSP and an accountable institution in terms of item 12 of Schedule 1 to the FIC Act. When must I register with the FIC on their GoAML system?**

As soon as possible but not later than 90 days of becoming an accountable institution by virtue of having obtained a new FSP licence.

**16.4.2. I have previously registered with the FIC on their GoAML system, but the name of my business has since changed. Must I inform the FIC of such change?**

You are required to ensure that all your details initially provided to the FIC upon registration on their GoAML system remains up to date at all times. Please inform the FIC of any changes without any delay. You will be able to update your institution's details on goAML: log into your profile and complete the update under the "Admin" heading.

**16.4.3. I am an accountable institution, but I am not technologically capable of registering on the GoAML system. What must I do now?**

Please contact the FIC without delay at (telephone): 012 641 6000 or visit their website at [www.fic.gov.za](http://www.fic.gov.za). On the website, you will be able to send a public query by leaving your details so that the FIC can contact you. See the prompts provided under para 14.3 above.

**16.4.4. I am an accountable institution in terms of item 12 of Schedule 1 to the FIC Act. However, I am also an accountable institution/ reporting institution in terms of another item in schedule 1 and/ or 3 of the FIC Act. Must I register with the FIC in accordance with each item?**

Yes, you are required to register with the FIC in respect of each individual item under the relevant schedules to the FIC Act.

**16.4.5. I have not registered with the FIC as an accountable institution. What are the consequences?**

Failure to register with the FIC in terms of section 43B of the FIC Act, read with the regulations, is non-compliance and subject to a sanction. See para 3.6 above in relation to enforcement.

**16.4.6. Can I share my login details with my management team/ my personal assistant to help me log in to the GoAML system/ log in on my behalf?**

No, sharing of login details is strictly prohibited. See Directive 2 published by the FIC in this regard.

**16.4.7. Should juristic representatives of an FSP register separately with the FIC?**

No, only the FSP has to register.

## **17. RELIANCE ON THIRD PARTIES**

**17.1. Explanation/ legal definition**

An accountable institution cannot delegate its compliance accountability to anybody else, including another accountable institution. However, it may rely on CDD information obtained by another accountable institution in respect of a shared client. Such information can be requested in addition to the CDD performed by an accountable institution in respect of its own risk-based approach. The principle of reliance on another institution must be documented in the accountable institution's RMCP and must take into account the risks associated with the client as well as the accountable institution on which reliance is placed.

**17.2. Examples of reliance**

- Request assistance from another accountable institution in respect of identification of a client;
- Verification of identification information in respect of a client; and
- Information such as the source of funds, source of wealth and geographic location.

### **17.3. Activities where assistance cannot be requested from another accountable institution:**

- The ML/ TF risk, and associated rating assigned to a client, by another accountable institution;
- The screening performed on a client by another accountable institution;
- Ongoing due diligence; and
- Any reporting obligation in terms of the FIC Act.

It should be noted that reliance is not the same as outsourcing. Reliance can be placed on another accountable institution in relation to CDD (to a limited extent) as well as in relation to record-keeping. Note however that the following activities cannot be outsourced:

- To fulfil and discharge CDD, reporting and registration obligations;
- An AI's duties in terms of sections 27 and 32 of the FIC Act as it relates to additional information about an AI's client/s;
- Obtaining senior management's approval in relation to sections 21F, 21G and 21H of the FIC Act (as it relates to Foreign Prominent Public Officials, Domestic Prominent Influential Persons and their respective known close associates and family members); and
- Any reporting obligation of an AI.

### **17.4. Frequently asked questions**

#### **17.4.1. I am an accountable institution and operate as an FSP. I perform CDD in line with the requirements of the product provider where I place new business. Is this sufficient?**

You are required to perform CDD in line with your own RMCP. Your RMCP is based on your own identification and assessment of ML/ TF risk. Person A may well be your client and the client of the product provider. However, both accountable institutions (you and the product provider) must fulfil all your obligations in terms of the FIC Act, and neither can delegate this responsibility to the other.

**17.4.2. My core business requires a large dependency on banks as product providers. The banks are already performing screening on my clients. Is this sufficient?**

No. If screening is required in relation to the clients that you onboarded, you should conduct such screening yourself.

**17.4.3. I request CDD information from my clients, but the product providers are responsible for assessing the information I obtained in relation to the ML/ TF risks. Is this sufficient?**

No product provider can assess the type and extent of information that you obtained from your clients, in line with your RMCP. You obtain this information to ensure that you do not deal with anonymous clients/ clients with fictitious names. You further obtain this information to help you to understand the purpose, nature and intent of the business relationship that you enter into with a client. Without this understanding, you will also find it impossible to comply with your reporting obligations in terms of section 29 of the FIC Act.

## **18. SCREENING (TERRORIST PROPERTY AND TARGETED FINANCIAL SANCTIONS)**

### **18.1. Explanation/ legal definition**

An AI must upon:

Publication of a proclamation by the President under section 25 of

POCDATARA; or

Notice being given by the Director under section 26A(3),

**Scrutinise** its information concerning clients with whom it has business relationships in order to determine if it has a client listed in the proclamation. (See section 28A(3) of the FIC Act).

## 18.2. Examples of screening

- The President has issued Government Gazette 40981 under section 25 of POCDATARA on 14 July 2017
- The Government Gazette refers to UN resolution 1267
- The 1267 list contains names of members of Al-Qaida, Taliban and ISIL
- The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation.
- Targeted Financial Sanctions (TFS) provide for financial sanctions only and include a list of all persons and entities who are subject to targeted financial sanctions under the FIC Act.

There are 14 ongoing United Nations Security Council Sanctions Regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation and counter - terrorism.

Current sanctions regimes include:

- Central African Republic
- Democratic People's Republic of Korea (North Korea)
- Democratic Republic of the Congo
- Guinea-Bissau
- Iran
- Iraq
- Lebanon
- Libya
- Mali
- Somalia and Eritrea
- South Sudan
- Sudan
- Yemen

## 18.3. Screening results related to reporting obligations

An accountable institution must submit a report in terms of section 28A of the FIC Act if it has **property owned** or control by or on behalf of, or at the direction of:



- Any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in POCDATARA; or
- A specific entity identified in a notice issued by the President under section 25 of POCDATARA; or
- A person or entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1).

The Director may direct an AI who made a report in terms of section 28A to make additional reports.

## **18.4. Frequently asked questions**

### **18.4.1. I am an AI and heard about the screening of clients. What does this mean?**

You are required to screen your clients against the UNSCR1267 list (for purposes of identifying property associated with terrorists and related activities) as well as the targeted financial sanction lists (for purposes of identifying clients that have been subject to such a sanction). The targeted financial sanctions list is available on the FIC website. The UNSCR1267 list is available on the UN Security Council Resolutions website. You are further required to make reports to the FIC and freeze assets of a client when necessary.

For these types of transactions, you cannot proceed if the client's name appears on one of the lists and freezing of assets must take place without delay. You must provide for how, where and the frequency of your screening obligations in your RMCP. Your RMCP should also provide for the freezing of property as well as reporting obligations to the FIC. You may want to opt for using an automated tool for screening purposes, but if that is not possible, you can also perform the screening activity manually against the published lists.

#### **18.4.2. Where can I find the lists to screen against?**

UN1267 list can be found on the link below:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

To screen against targeted financial sanction lists, go the FIC's website or just click on the link below:

<https://www.fic.gov.za/International/sanctions/Pages/search.aspx>

#### **18.4.3. Can I ask somebody to do screening on my behalf?**

No, you are required to perform the screening activity yourself. You may however utilise software or an automated tool that provides for this particular screening facility. Alternatively, you can screen manually against the published lists.

### **19. SECTOR RISK ASSESSMENT**

#### **19.1. Explanation/ legal definition**

A sector risk assessment can be described as a review of the characteristics of certain sectors of the financial system. It assesses the level of risk of money laundering and terrorism financing occurring in that sector and outlines any particular risks in that area.

#### **19.2. Examples of sector risk assessments**

- The sector risk assessment published by the Authority
- The sector risk assessment published by the Prudential Authority

#### **19.3. Purpose of sector risk assessments**

A sector risk assessment is conducted to assess the level of threats, vulnerabilities and consequences in respect of ML/ TF in the financial services industry. This provides insights into applying a risk-based approach of supervision and filters into the national risk assessment, which is ultimately an overall understanding of ML/ TF risk in the country.

#### **19.4. Frequently asked questions**

#### **19.4.1. Did the Authority conduct a sector risk assessment?**

Yes, the Authority published a summarised version of the results of its first sector risk assessment in May 2019 on the Authority's website. The sector risk assessment is currently being reviewed and the updated version will be published in due course. See the list of useful links under paragraph 4 of the BoK.

#### **19.4.2. What are the results of the Authority's sector risk assessment?**

The overall **threat** and **vulnerability** of the financial sector regulated by the FSCA has been assessed in 2019 as follows:

- Authorised users: medium risk
- CIS managers: low risk
- Category I FSPs: low risk
- Category II FSPs: medium risk
- Category IIA FSPs: medium risk
- Category III FSPs: medium risk

Please ensure that you follow the sector risk assessment reviews as and when published on the Authority's official website as this may impact on the most recently concluded ratings.

#### **19.4.3. I am an accountable institution and focused on assessing my institutional ML/ TF risk. Why should I bother to read the sector risk assessment?**

Considering the results from the sector risk assessment will assist you as an accountable institution to identify, assess and take effective action to mitigate ML/ TF risk. It will alert you to the nature of the ML/ TF risks in the specific industry and the extent thereof.

It is recommended that every accountable institution conduct an institutional risk assessment, with the sector risk assessment informing them of the inherent risks to start the process. This is similar to the national risk assessment, which is of importance as well. Both the

national risk assessment and the sector risk assessment should inform the institutions of their institutional risk.

The risks identified in the national and sectoral risk assessments can be used to “plug into” the institutional risk assessment. An easier method to consider the above is to think of the three levels: the national risk assessment being the broadest, measuring risk throughout the country; the sector risk assessment, which measures the risk applicable to the specific sector; the institutional risk, which is applicable to the specific accountable institution.

## **20. TERRORIST FINANCING**

### **20.1. Explanation/ legal definition**

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.

### **20.2. Examples of terrorist financing**

- Drug trafficking
- Identity theft
- Credit card theft
- Legitimate business
- Crypto currency
- Cybercrime

### **20.3. How to identify terrorist financing**

Terrorist financing has several layers so watch out for the following:

- **Collection:** direct donations/ use of charities and NPOs
- **Storing:** accounts / pre-paid cards/ cryptocurrencies
- **Moving:** mechanisms i.e. financial sector/ high value commodities
- **Using:** terrorist organisations/ foreign fighters/ lone actors

## **20.4. Frequently asked questions**

### **20.4.1. What is the difference between money laundering and terrorist financing?**

Money laundering always stems from illegal proceeds whereas terrorist financing receives funds from both legal and illegal sources. Terrorist financing tends to receive funds from multiple sources for small amounts, where money laundering tends to be larger amounts from a small number of sources.

### **20.4.2. Why is it difficult to identify terrorist financing?**

Money used can come from legal sources and could be low in value which is often not raising suspicion.

### **20.4.3. How should I provide for combatting of terrorist financing as an accountable institution?**

You should conduct a risk assessment and provide for this comprehensively in your RMCP. In addition, you should also comply with the screening and reporting obligations as envisaged in section 28A of the FIC Act.

## **21. UNALLOCATED FUNDS**

### **21.1. Explanation/ legal definition**

Funds that cannot be apportioned or allocated for the purpose of investment/ issuing a financial product because the owner of the funds is unknown.

### **21.2. Examples of unallocated funds**

- Money received by an accountable institution without details of the owner of the funds.
- A benefit is due to be paid out to a client, but the client cannot be located.

### **21.3. Processes and reporting duties**

As an accountable institution you are required to address the issue of handling unallocated funds, and to avoid receiving such funds, in your RMCP. It is important to emphasise that:

- An accountable institution incurs increased money laundering (ML) and terrorist financing (TF) risk when it receives funds from an unidentified person, who may or may not become a prospective client (PCC 31A par 4.1);
- An accountable institution's RMCP should contain measures to mitigate ML/ TF risk (PCC31A, par 4.4); and
- That an accountable institution has a reporting obligation in terms of section 29 of the FIC Act to report suspicious and unusual transactions and activities to the FIC (the Centre).

### **21.4. Frequently asked questions**

#### **21.4.1. If the money was received via a bank, can I request the bank to reverse the transaction?**

Please take note of the requirements set out in section 33 of the FIC Act: "An accountable institution, reporting institution or person required to make a report to the Centre in terms of section 28 or 29, may continue with and carry out the transaction in respect of which the report is required to be made unless the Centre directs the accountable institution, reporting institution or person in terms of section 34 not to proceed with the transaction." This requirement is subject to compliance with the reporting obligations set out in section 29 of the FIC Act in relation to suspicious and unusual transactions and activities as it applies under these circumstances, clearly referenced in PCC31A (see par 5.4).

#### **21.4.2. How can I avoid receiving funds from persons that I do not know?**

Include practical steps in your RMCP and implement these accordingly i.e. do not make your banking details publicly available on your website

or in your marketing material. The timing of the transaction is quite important. Always complete the identification and verification of the client before the funds are paid into your account (refer to PCC31A). If you receive funds which are not based on a transaction or business relationship, then follow the steps set out in your RMCP.

## 22. USEFUL LINKS

### 22.1. ACCOUNTABLE INSTITUTIONS:

**FIC Amendment Act section 1**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**FAIS Newsletter Volume 25**

<https://www.fsca.co.za/Regulated%20Entities/Regulated%20Entities%20Documents/Newsletter%20Volume%2025.pdf>

**FICA Webinars**

[https://www.fsca.co.za/MagicScripts/mgrqispi.dll?APPNAME=Web&PRGNAME=FAIS\\_Conf1&Arguments=-N45](https://www.fsca.co.za/MagicScripts/mgrqispi.dll?APPNAME=Web&PRGNAME=FAIS_Conf1&Arguments=-N45)

### 22.2. BENEFICIAL OWNERSHIP:

**FIC Amendment Act section 21B**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**Guidance Note 7 Chapter 2**

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

**Guidance Note 8 of 2020 para 95 to 122**

<https://www.fsca.co.za/Regulatory%20Frameworks/Pages/Notices.aspx>

**FATF Recommendation 24**

<https://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

**FATF Best Practices for Beneficial Owners of Legal Persons**

<https://www.dlapiper.com/en/us/insights/publications/2020/02/aml-bulletin-winter-2020/fatf-report-best-practices-on-beneficial-ownership-for-legal-persons/>

**FATF Guidance on Transparency and Beneficial Ownership**

<https://www.fatfgafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf>

**22.3. CLIENTS:**

**FIC Amendment Act Section 1**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**22.4. COMPLIANCE OFFICER:**

**FIC Amendment Act Section 42A**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**22.5. DIRECTIVES:**

**FIC Amendment Act Section 43A and Section 45C**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>



**22.6. ENFORCEMENT:****FIC Amendment Act Section 45C**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**FAIS Newsletter Volume 25**

<https://www.fsca.co.za/Regulated%20Entities/Regulated%20Entities%20Documents/Newsletter%20Volume%2025.pdf>

**FICA Webinars**

[https://www.fsca.co.za/MagicScripts/mgrqispi.dll?APPNAME=Web&PRGNAME=FAIS\\_Conf1&Arguments=-N45](https://www.fsca.co.za/MagicScripts/mgrqispi.dll?APPNAME=Web&PRGNAME=FAIS_Conf1&Arguments=-N45)

**FSCA Website**

<https://www.fsca.co.za/Regulatory%20Frameworks/Pages/AMLCFT.aspx>

**22.7. FIC:****FIC Amendment Act Section 2**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**FAIS Newsletter Volume 24**

<https://www.fsca.co.za/Regulated%20Entities/Regulated%20Entities%20Documents/Newsletter%20volume%2024.pdf>

**FAIS Newsletter Volume 25**

<https://www.fsca.co.za/Regulated%20Entities/Regulated%20Entities%20Documents/Newsletter%20Volume%2025.pdf>

**FIC Website**

<https://www.fic.gov.za/Pages/Home.aspx>

**22.8. FSCA:**

**Financial Sector Regulation Act Section 56**

<http://www.treasury.gov.za/legislation/acts/2017/Act%209%20of%202017%20FinanSectorRegulation.pdf>

**FSCA Website**

<https://www.fsca.co.za/Pages/Default.aspx>

**22.9. JURISTIC REPRESENTATIVES:**

**Financial Advisory and Intermediary Services Act Section 1 and Section 13**

<https://www.gov.za/documents/financial-advisory-and-intermediary-services-act>

**Guidance Note 7 para 38**

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

**22.10. MONEY LAUNDERING:**

**FIC Amendment Act Section 1**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**Guidance Note 7: para 5 and 6**

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

**FATF Update: Covid-19-related Money Laundering and Terrorist Financing**

<https://www.fatf-gafi.org/media/fatf/documents/Update-COVID-19-Related-Money-Laundering-and-Terrorist-Financing-Risks.pdf>

**22.11. POPIA:**

**Protection of Personal Information Act**

<https://www.gov.za/documents/protection-personal-information-act>

**Guidance Note 7: para 119**

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

**22.12. PROLIFERATION FINANCING:**

**FIC Amendment Act Sections 26A, 26B, S26C AND 28A**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**Public Compliance Communication (PCC) 44**

<https://www.fic.gov.za/Documents/200320%20PCC%2044.pdf>

**Guidance Note 6A**

<https://www.fic.gov.za/Documents/190327%20FIC%20Guidance%20Note%206A.pdf>

**FATF Guidance on counter-proliferation financing**

<https://www.fatfgafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf>

**22.13. RECORD KEEPING:**

**FIC Amendment Act Sections 22, 22A, 23, 24, 25**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

**Money Laundering and Terrorist Financing Control Regulations,  
Reg 20**

<https://www.gov.za/documents/financial-intelligence-centre-act-regulations-money-laundering-and-terrorist-financing>

Guidance Note 7 para 161 to 179

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

#### 22.14. REGISTRATION:

FIC Act section 43B

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>

Directive 1: update of details

<https://www.fic.gov.za/Documents/140318%20Directive%20media%20statement.pdf>

Directive 2: Use of Login Credentials

<https://www.fic.gov.za/Documents/Use%20of%20login%20credentials%20following%20registration%20with%20the%20FIC.pdf>

Directive 4: Updating registration information

[https://www.fic.gov.za/Documents/ss160304%20Directive%204%20media%20brief%20\(website\).pdf](https://www.fic.gov.za/Documents/ss160304%20Directive%204%20media%20brief%20(website).pdf)

FIC website

<https://www.fic.gov.za/Compliance/Pages/Registration.aspx>

#### 22.15. RELIANCE:

Public Compliance Communication (PCC) 43

<https://www.fic.gov.za/Documents/200227%20PCC%2043%20final.pdf>

**Public Compliance Communication (PCC) 12A**

<https://www.fic.gov.za/Documents/210324%20PCC%2012A%20Outsourcing%20FINAL.pdf>

**22.16. SCREENING:**

**FIC website**

<https://www.fic.gov.za/International/sanctions/Pages/search.aspx>

**UN 1267 list**

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

**22.17. SECTOR RISK ASSESSMENT**

**FSCA Sector Risk Assessment: Securities Sector**

[https://www.fsca.co.za/Regulatory%20Frameworks/Temp/Securities%20Sector%20Risk%20Assessment%20Report%20April%202018%20to%20December%202020%20\(February%202022\).pdf](https://www.fsca.co.za/Regulatory%20Frameworks/Temp/Securities%20Sector%20Risk%20Assessment%20Report%20April%202018%20to%20December%202020%20(February%202022).pdf)

**FSCA Sector Risk Assessment: CIS Managers and FSPs**

[https://www.fsca.co.za/Regulatory%20Frameworks/Temp/FSCA%20Sector%20Risk%20Assessment%20CIS%20%20Financial%20Advisory%20and%20Intermediary%20Services%20Sectors%20-%20April%202018%20to%20December%202020%20\(April%202022\)%20final.pdf](https://www.fsca.co.za/Regulatory%20Frameworks/Temp/FSCA%20Sector%20Risk%20Assessment%20CIS%20%20Financial%20Advisory%20and%20Intermediary%20Services%20Sectors%20-%20April%202018%20to%20December%202020%20(April%202022)%20final.pdf)

**22.18. TERRORIST FINANCING:**

**FATF Recommendations**

<https://www.fatfqafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>

**Money laundering and terrorist financing Awareness Handbook  
for tax examiners and tax auditors**

<https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf>

**FATF Terrorist Financing Risk Assessment Guidance**

<https://docs.mymembership.co.za/docmanager/52c7b7c8-d6fc-4150-8d1a-7b85c1f7012e/00145140.pdf>

**Guidance Note 7 para 7**

[https://www.fic.gov.za/Documents/171002\\_FIC%20Guidance%20Note%2007.pdf](https://www.fic.gov.za/Documents/171002_FIC%20Guidance%20Note%2007.pdf)

**22.19. UNALLOCATED FUNDS:**

**Public Compliance Communication 31A**

[https://www.fic.gov.za/Documents/190211%20PCC31A%20%20\(financial\).pdf](https://www.fic.gov.za/Documents/190211%20PCC31A%20%20(financial).pdf)

**The FIC Act section 29**

<https://www.fic.gov.za/Resources/Pages/FIC-Amendment-Act.aspx>