



Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

The Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) has been amended by Commencement of Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017), Notice No. 563, Government Gazette 40916, dated 13 June 2017.

www.acts.co.za

Table of Contents

Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)	10
Notice No. 1262 of 2001	10
Act	10
1. Definitions	11
1A. Application of Act when in conflict with other laws	16
Chapter 1 : Financial Intelligence Centre	16
2. Establishment	17
3. Objectives	17
4. Functions	18
5. General powers	19
6. Appointment of Director	19
7. Removal from office	20
8. Acting Director	20
9. Proof of appointment	20
10. Responsibilities of Director	20
11. Staff	21
12. Security screening of staff of Centre other than Director	22
13. Security screening of Director of Centre	22
14. Funds and financial year of Centre	23
15. Audit	23
16. Delegation	23
[Repealed] Chapter 2 : Counter-Money laundering advisory Council	24
17. [Repealed] Establishment	24
18. [Repealed] Functions	24
19. [Repealed] Composition	24
20. [Repealed] Meetings and procedure	24
Chapter 3 : Money Laundering, Financing of Terrorist and Related Activities and Financial Sanctions Control Measures	
Part 1 : Customer due diligence	25
20A. Anonymous clients and clients acting under false or fictitious names	25
21. Identification of clients and other persons	25
21A. Understanding and obtaining information on business relationship	26
21B. Additional due diligence measures relating to legal persons, trusts and partnerships	27
21C. Ongoing due diligence	28
21D. Doubts about veracity of previously obtained information	29
21E. Inability to conduct customer due diligence	29
21F. Foreign prominent public official	29
21G. Domestic prominent influential person	30
21H. Family members and known close associates	30
Part 2 : Duty to keep record	30
22. Obligation to keep customer due diligence records	31
22A. Obligation to keep transaction records	31
23. Period for which records must be kept	31
24. Records may be kept in electronic form and by third parties	32
25. Admissibility of records	32
26. [Repealed] Centre's access to records	33
Part 2A : Financial sanctions	33
26A. Notification of persons and entities identified by Security Council of the United Nations	33
26B. Prohibitions relating to persons and entities identified by Security Council of the United Nations	34

26C. Permitted financial services and dealing with property.....	35
Part 3 : Reporting duties and access to information	36
27. Accountable institutions to advise Centre of clients.....	36
27A. Powers of access by authorised representative to records in respect of reports required to be submitted to Centre.....	37
28. Cash transactions above prescribed limit.....	37
28A. Property associated with terrorist and related activities	38
29. Suspicious and unusual transactions.....	39
30. Conveyance of cash to or from Republic.....	40
31. Electronic transfers of money to or from Republic.....	40
32. Reporting procedures and furnishing of additional information.....	40
33. Continuation of transactions.....	41
34. Intervention by Centre.....	41
35. Monitoring orders.....	42
36. Information held by supervisory bodies and South African Revenue Service	43
37. Reporting duty and obligations to provide information not affected by confidentiality rules.....	43
38. Protection.....	44
39. Admissibility as evidence of reports made to Centre	44
40. Access to information held by Centre.....	44
41. Protection of confidential information.....	46
41A. Protection of personal information.....	47
Part 4 : Measures to promote compliance by accountable institutions	47
42. Risk Management and Compliance Programme.....	47
42A. Governance of anti-money laundering and counter terrorist financing compliance	50
42B. Consultation process for issuing guidance.....	50
43. Training relating to anti-money laundering and counter terrorist financing compliance	50
43A. Directives.....	51
43B. Registration by accountable institution and reporting institution	52
Part 5 : Referral and supervision	52
44. Referral of suspected offences to investigating authorities and other public bodies.....	53
45. Responsibility for supervision of accountable institutions.....	53
Chapter 4 : Compliance and Enforcement	55
45A. Appointment of inspectors	56
45B. Inspections	57
45C. Administrative sanctions	60
45D. Appeal	62
45E. Establishment of appeal board	65
45F. Application to court	66
46. Failure to identify persons	67
46A. Failure to comply with duty in regard to customer due diligence	67
47. Failure to keep records.....	67
48. Destroying or tampering with records	68
49. Failure to give assistance	68
49A. Contravention of prohibitions relating to persons and entities identified by Security Council of United Nations	68
50. Failure to advise Centre of client	68
51. Failure to report cash transactions	69
51A. Failure to report property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations	70
52. Failure to report suspicious or unusual transactions	70
53. Unauthorised disclosure	70
54. Failure to report conveyance of cash or bearer negotiable instrument into or out of Republic	70
55. Failure to send report to Centre	70
56. Failure to report electronic transfers	71
57. Failure to comply with request	71
58. Failure to comply with directives	71
59. Failure to comply with monitoring order	71
60. Misuse of information	72

61. Failure to formulate and implement internal rules	72
61A. Failure to register with Centre	73
61B. Failure to comply with duty in regard to governance	73
62. Failure to provide training or appoint compliance officer	73
62A. Offences relating to inspection	74
62B. Hindering or obstructing appeal board	74
62C. Failure to attend when summoned	74
62D. Failure to answer fully or truthfully	74
62E. Failure to comply with directives of Centre or supervisory body	75
63. Obstructing of official in performance of functions	75
64. Conducting transactions to avoid reporting duties	75
65. Unauthorised access to computer system or application or data	75
66. Unauthorised modification of contents of computer system	76
67. Definitions	76
68. Penalties	76
69. Defences	77
70. Search, seizure and forfeiture	77
71. Jurisdiction of courts	79
Chapter 5 : Miscellaneous	79
72. Act not to limit powers of investigating authorities or supervisory bodies	80
73. Amendment of list of accountable institutions	80
74. Exemptions for accountable institutions	80
75. Amendment of list of supervisory bodies	81
76. Amendment of list of reporting institutions	81
77. Regulations	82
77A. Arrangements for consultations with stakeholders	83
78. Indemnity	83
79. Amendment of laws	83
79A. Amendment of list of domestic prominent influential persons	83
79B. Amendment of list of foreign prominent public officials	84
80. Status of footnotes	84
81. Transitional arrangements	84
82. Short title and commencement	85
Schedules	85
Schedule 1 : List of Accountable Institutions	85
Schedule 2 : List of Supervisory Bodies	86
Schedule 3 : List of Reporting Institutions	87
Schedule 3A : Domestic Prominent Influential Person	87
Schedule 3B : Foreign Prominent Public Official	88
Schedule 4 : Amendment of sections of Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998)	89

Commencements 92

Commencement of Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)	92
Notice No. 563 of 2017	92

Notices 96

Guidance Note 2	96
Guidance to Financial Services Industries regulated by the Financial Services Board concerning the meaning of the word "Transaction"	
Notice No. 735 of 2004	96
1. Introduction	97
2. Meaning of "transaction" in relation to client identification duties	98
3. Examples of transactions	98
Second Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001	100
Notice No. R. 1354 of 2004	100
Guidance Note 3	102
Guidance for Banks on Customer Identification and Verification and Related Matters	102

Notice No. 715 of 2005	102
Preface	102
Anti-Money Laundering and Terrorist Financing Policies and Procedures	104
1. Board approval of a bank's anti-money laundering and terrorist financing policies	104
2. Implementation of Guidance Note 1 in respect of a risk-based approach	104
3. Risk indicators to be used to differentiate between clients	105
4. Client profiling procedures for high risk clients	105
5. Client acceptance policies	107
Establishing and Verifying Identities	107
Natural Persons - South African Citizens and Residents	107
6. Clarification of an official identity document	107
7. Clarification of whether the address slip found in identity documents	108
8. Alternate means of verification if identity document has been lost or stolen	108
9. Acceptable KYC procedures for non face-to-face verification	108
10. Status of "faxed copies"	109
11. Examples of acceptable documentation to verify residential address of natural per	109
12. Acceptable documents for third party verification	110
13. Legal incapacity	111
14. Ongoing client detail maintenance	111
Natural Persons - Foreign Nationals	112
15. Identification and verification	112
Legal Entities	112
16. Identification and verification of subsidiaries of listed companies	112
17. Identification and verification of pension and provident funds	113
18. Identification and verification of "off the shelf" companies	113
Partnerships	113
19. The definition of a partnership	113
20. Clarification of partnership agreements and whether all partners in a partnership	114
Trusts	114
21. Identification of trusts	114
22. Identification and verification of each trustee of a trust	115
Organs of State including Government Departments	115
23. Identification and verification of Government departments and organs of state	115
International Standards and Best Banking Practice	116
24. Extent to which international standards	116
Politically Exposed Persons (PEPs)	117
25. Definition of a politically exposed person (PEP)	117
26. Treatment of PEPS in relation to other high-risk clients	117
27. Policies for dealing with PEPs	118
Correspondent Banks	118
28. Measures that need to be put in place in respect of correspondent banking relatio	118
Exemptions	120
29. Clarification of Exemption 5 - foreign clients	120
30. Clarification of the difference between Exemptions 5 and 16	120
Glossary	121
Third Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001	123
Notice No. 1035 of 2006	123
Guidance Note 4 on Suspicious Transaction Reporting	124
Notice No. 301 of 2008	125
Preface	125
Glossary	126
Introduction	127

Part 1 - Who Must Report?	128
Part 2 - What Gives Rise to the Obligation to Report?	128
Part 3 - What is the Nature of a Suspicion?	130
Part 4 - Indicators of Suspicious and Unusual Transactions	131
Part 5 - What are the Implications of making a STR?	133
Part 6 - Process for Submitting STRs to the Centre	136
Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)	156
Notice No. R. 454 of 2010	156
1. Definitions	157
2. Exemption from Regulations made under Act 38 of 2001	157
Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)	158
Notice No. 471 of 2010	158
1. Definitions	159
2. Exemption from Regulations made under Act 38 of 2001	159
Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)	160
Notice No. 560 of 2010	160
1. Definitions	161
2. Exemption from Regulations made under Act 38 of 2001	161

Regulations

164

Money Laundering and Terrorist Financing Control Regulations	164
Notice No. R. 1595 of 2002	164
1. Definitions	164
1A. Prescribed amount of a single transaction	166
[Repealed] Chapter 1 : Establishment and verification of identity	166
[Repealed] Part 1 : Introduction.....	167
2. [Repealed] Introductory.....	167
[Repealed] Part 2 : Natural Persons.....	167
3. [Repealed] Information concerning South African citizens and residents	167
4. [Repealed] Verification of information concerning South-African citizens and residents	167
5. [Repealed] Information concerning foreign nationals	167
6. [Repealed] Verification of information concerning foreign nationals.....	168
[Repealed] Part 3 : Legal Persons.....	168
7. [Repealed] Information concerning close corporations and South African companies.....	168
8. [Repealed] Verification of information concerning close corporations and South African compa.....	168
9. [Repealed] Information concerning foreign companies.....	168
10. [Repealed] Verification of information concerning foreign companies	168
11. [Repealed] Information concerning other legal persons	168
12. [Repealed] Verification of information concerning other legal persons	169
[Repealed] Part 4 : Partnerships.....	169
13. [Repealed] Information concerning partnerships.....	169
14. [Repealed] Verification of information concerning partnerships.....	169
[Repealed] Part 5 : Trusts.....	169
15. [Repealed] Information concerning trusts.....	169
16. [Repealed] Verification of information concerning trusts.....	169
[Repealed] Part 6 : General.....	170
17. [Repealed] Additional requirements when person acts on authority of another.....	170
18. [Repealed] Verification in absence of contact person	170
19. [Repealed] Accountable institution maintain correctness of particulars	170
Chapter 2 : Record-Keeping	170
20. Particulars of third parties keeping records.....	170
[Repealed] Chapter 3 : Client Profile	171

21. [Repealed] Information to identify proceeds of unlawful activities or money laundering acti.....	171
Chapter 4 : Reporting	171
22. Manner of reporting.....	171
22A. Information to be reported concerning a terrorist property report	172
22B. Prescribed amount for cash transaction reporting.....	174
22C. Information to be reported concerning a cash threshold report.....	174
23. Information to be reported.....	176
23A. Information to be reported concerning a suspicious or unusual activity report	180
23B. Information to be reported concerning a terrorist financing transaction report	184
23C. Information to be reported concerning a terrorist financing activity report	188
24. Period for reporting.....	192
24A. Manner in which and period within additional information to be furnished.....	193
Chapter 5 : Measures to Promote Compliance and Appeals	193
25. [Repealed] Internal rules concerning establishment and verification of identities	193
26. [Repealed] Internal rules concerning the keeping of records.....	193
27. [Repealed] Internal rules concerning reporting of information.....	194
27A. Period for and manner of registration by accountable institutions and reporting institutions.....	194
27B. Period within and manner in which supervisory body must submit written report to Centre.....	194
27C. Manner in which appeal is to be lodged and payment of fee	195
27D. Criteria for supervisory body to request information relating to a report made in terms of section 29.....	195
Chapter 6 : Miscellaneous	196
28. Guidance.....	196
29. Offences and penalties and administrative sanctions for non-compliance	196
30. Title and commencement.....	198
Annexure	198
Form 1 - Suspicious or Unusual Transaction Report [Deleted].....	198
Exemptions	198
Interpretation - Definitions	199
Part 1 : General Exemptions	199
Part 2 : Exemptions for insurance and investment providers	200
Part 3 : Exemptions for members of Exchanges	202
Part 4 : Exemptions for attorneys and administrators of property.....	203
Part 5 : Exemptions for estate agents	204
Part 6 : Exemptions for gambling institutions.....	204
Part 7 : Exemptions for banks.....	205
Part 8 : Miscellaneous.....	206
Exchanges recognised for purposes of the exemption in respect of public companies the securities of which are listed on a stock exchange	206



Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

www.acts.co.za

Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

Notice No. 1262 of 2001

Act

1. Definitions

1A. Application of Act when in conflict with other laws

Chapter 1 : Financial Intelligence Centre

[Repealed] Chapter 2 : Counter-Money laundering advisory Council

Chapter 3 : Money Laundering, Financing of Terrorist and Related Activities and Financial Sanctions Control Measures

Chapter 4 : Compliance and Enforcement

Chapter 5 : Miscellaneous

Schedules

Notice No. 1262 of 2001

Notice No. 1262

3 December 2001

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:—

No. 38 of 2001: Financial Intelligence Centre Act, 2001

(English text signed by the President.)

(Assented to 28 November 2001.)

Act

To establish a Financial Intelligence Centre in order to combat money laundering activities and the financing of terrorist and related activities; to impose certain duties on institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities; to provide for customer due diligence measures including with respect to beneficial ownership and persons in prominent positions; to provide for a risk based approach to client identification and verification; to provide for the implementation of financial sanctions and to administer measures pursuant to resolutions adopted by the Security Council of the United Nations; to clarify the application of the Act in relation to other laws; to provide for the sharing of information by the Centre and supervisory bodies; to provide for risk management and compliance programmes, governance and training relating to anti-money laundering and counter terrorist financing; to provide for the issuance of directives by the Centre and supervisory bodies; to provide for the registration of accountable and reporting institutions; to provide for the roles and responsibilities of supervisory bodies; to provide for written arrangements relating to the respective roles and responsibilities of the Centre and supervisory bodies; to provide the Centre and supervisory bodies with powers to conduct inspections; to regulate certain applications to Court; to provide for administrative

sanctions that may be imposed by the Centre and supervisory bodies; to establish an appeal board to hear appeals against decisions of the Centre or supervisory bodies; to provide for arrangements on consultation with stakeholders; to amend the Prevention of Organised Crime Act, 1998, and the Promotion of Access to Information Act, 2000; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

[Long title substituted by section 60 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

1. Definitions

(1) In this Act, unless the context indicates otherwise—

"accountable institution"

means a person referred to in Schedule 1;

"administrative sanction"

means an administrative sanction contemplated in section 45C;

[Definition substituted by section 1(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"appeal board"

means the appeal board established by section 45E;

"authorised officer"

means any official of—

- (a) an investigating authority authorised by the head of that investigating authority to act under this Act;
- (b) the National Prosecuting Authority authorised by the National Director of Public Prosecutions to act under this Act;
- (c) an intelligence service authorised by the Director-General of that service to act under this Act; or
- (d) the South African Revenue Service authorised by the Commissioner for that Service to act under this Act;
- (e) the Independent Police Investigative Directorate authorised by the Executive Director of that Directorate to act under this Act;
- (f) the Intelligence Division of the National Defence Force authorised by the Inspector-General of the National Defence Force to act under this Act;
- (g) a Special Investigating Unit authorised by the head of the Special Investigating Unit to act under this Act;
- (h) the office of the Public Protector authorised by the Public Protector to act under this Act; or
- (i) an investigative division in an organ of state authorised by the head of the organ of state to act under this Act;

[Definition substituted by section 1(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"bearer negotiable instrument"

means any instrument that may on demand by the bearer thereof be converted to the currency of the Republic or that of another country, and includes, amongst others, cheques, promissory notes or money orders;

[Definition substituted by section 1(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"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;

[Definition inserted by section 1(d) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"business relationship"

means an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis;

"cash"

means—

- (a) coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue;
- (b) travellers' cheques;

"Centre"

means the Financial Intelligence Centre established by section 2;

"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;

[Definition inserted by section 1(e) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"Council"

[Definition deleted by section 1(f) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"Director"

means the Director of the Centre appointed in terms of section 6;

"domestic prominent influential person"

means a person referred to in Schedule 3A.

[Definition inserted by section 1(g) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"entity"

has a corresponding meaning with the definition in section 1 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;

[Definition substituted by section 1(h) of the Foreign Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"foreign prominent influential person"

means a person referred to in Schedule 3A;

[Definition inserted by section 1(i) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"Independent Police Investigative Directorate"

means the Independent Police Investigative Directorate established by section 3 of the Independent Police Investigative Directorate Act, 2011 (Act No. 1 of 2011);

[Definition inserted by section 1(i) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"inspector"

means a person appointed in terms of section 45A;

"Intelligence Division of the National Defence Force"

means the Intelligence Division of the National Defence Force referred to in section 33 of the Defence Act, 2002 (Act No. 42 of 2002);

[Definition inserted by section 1(j) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"intelligence service"

means the State Security Agency referred to in section 3 of the Intelligence Services Act, 2002 (Act No. 65 of 2002);

[Definition substituted by section 53 of the General Intelligence Laws Amendment Act, 2013 (Act No. 11 of 2013)]

"investigating authority"

means an authority that in terms of national legislation may investigate unlawful activities;

"investigative division in an organ of state"

means an investigative division in an organ of state in the Republic having a function by law to investigate unlawful activity within the organ of state;

[Definition inserted by section 1(k) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"legal person"

means any person, other than a natural person, that establishes a business relationship or enters into a single transaction, with an accountable institution, and includes a person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association, but excludes a trust, partnership or sole proprietor;

[Definition inserted by section 1(k) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"Minister"

means the Minister of Finance;

"money laundering" or "money laundering activity"

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 this Act or section 4, 5 or 6 of the Prevention Act;

"National Commissioner"

means the National Commissioner of the South African Police Service referred to in section 207 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996);

"National Director of Public Prosecutions"

means the National Director of Public Prosecutions referred to in section 179 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996);

"National Prosecuting Authority"

means the National Prosecuting Authority referred to in section 179 of the Constitution of the Republic of South Africa, 1996, and established in terms of section 2 of the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);

[Definition inserted by section 1(l) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"non-compliance"

means any act or omission that constitutes a failure to comply with a provision of this Act or any order, determination or directive made in terms of this Act and which does not constitute an offence in terms of this Act, and "fails to comply", "failure to comply", "non-compliant" and "not complying" have a corresponding meaning;

[Definition substituted by section 1(m) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"offence relating to the financing of terrorist and related activities"

means an offence under section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004);

[Definition inserted by section 1(n) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"offence relating to the financing of terrorist and related activities"

[Definition deleted by section 1(s) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"prescribed"

means prescribed by the Minister by regulation in terms of section 77;

"Prevention Act"

means, the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);

"proceeds of unlawful activities"

has the meaning attributed to that term in section 1 of the Prevention Act;

"property"

has the meaning attributed to that term in section 1 of the Prevention Act;

"Public Protector"

means the Public Protector referred to in Chapter 9 of the Constitution of the Republic of South Africa, 1996;

[Definition inserted by section 1(o) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"reporting institution"

means a person referred to in Schedule 3;

"Risk Management and Compliance Programme"

means the programme contemplated in section 42(1);

[Definition inserted by section 1(p) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"single transaction"

means a transaction—

- (a) other than a transaction concluded in the course of a business relationship; and
- (b) where the value of the transaction is not less than the amount prescribed, except in the case of section 20A;

[Definition substituted by section 1(q) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"South African Revenue Service"

means the South African Revenue Service established by section 2 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

"Special Investigating Unit"

means the Special Investigating Unit established under section 2 of the Special Investigating Units and Special Tribunals Act, 1996 (Act No. 74 of 1996);

[Definition inserted by section 1(r) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"supervisory body"

means a functionary or institution referred to in Schedule 2;

"terrorist and related activities"

has the meaning assigned to it in section 1 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004);

"this Act"

includes any regulation made or exemption given under this Act;

[Definition substituted by section 1(g) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

"transaction"

[Definition deleted by section 1(s) of the Financial Intelligence Centre Amendment Act,

2017 (Act No. 1 of 2017)]**"trust"**

means a trust defined in section 1 of the Trust Property Control Act, 1988 (Act No. 57 of 1988), other than a trust established—

- (a) by virtue of a testamentary disposition;
- (b) by virtue of a court order;
- (c) in respect of persons under curatorship; or
- (d) by the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund,

and includes a similar arrangement established outside the Republic;

[Definition inserted by section 1(t) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

"unlawful activity"

has the meaning attributed to that term in section 1 of the Prevention Act.

- (2) For the purposes of this Act a person has knowledge of a fact if—
 - (a) the person has actual knowledge of that fact; or
 - (b) the court is satisfied that :
 - (i) the person believes that there is a reasonable possibility of the existence of that fact, and
 - (ii) person fails to obtain information to confirm or refute the existence of that fact.
- (3) For the purposes of this Act a person ought reasonably to have known or suspected a fact; if the conclusions that he or she ought to have reached, are those which would have been reached by a reasonably diligent and vigilant person having both—
 - (a) the general knowledge, skill, training and experience that may reasonably be expected of a person in his or her position; and
 - (b) the general knowledge, skill, training and experience that he or she in fact has.

1A. Application of Act when in conflict with other laws

If any conflict, relating to the matters dealt with this Act, arises between this Act and the provisions of any other law existing at the commencement of this Act, save the Constitution, the provisions of this Act prevail.

Chapter 1 : Financial Intelligence Centre

- 2. Establishment
- 3. Objectives
- 4. Functions
- 5. General powers
- 6. Appointment of Director

-
7. Removal from office
 8. Acting Director
 9. Proof of appointment
 10. Responsibilities of Director
 11. Staff
 12. Security screening of staff of Centre other than Director
 13. Security screening of Director of Centre
 14. Funds and financial year of Centre
 15. Audit
 16. Delegation

2. Establishment

- (1) A Financial Intelligence Centre is hereby established as an institution outside the public service but within the public administration as envisaged in section 195 of the Constitution.
- (2) The Centre is a juristic person.

3. Objectives

- (1) The principal objective of the Centre is to assist in the—
 - (a) identification of the proceeds of unlawful activities;
 - (b) combating of money laundering activities and the financing of terrorist and related activities; and
 - (c) implementation of financial sanctions pursuant to resolutions adopted by the Security Council of the United Nations, under Chapter VII of the Charter of the United Nations;

[Subsection (1) substituted by section 2(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) The other objectives of the Centre are—
 - (a) to make information collected by it available to—
 - (i) an investigating authorities;
 - (ii) the National Prosecuting Authority;
 - (iii) an intelligence service;
 - (iv) the South African Revenue Service;
 - (v) the Independent Police Investigative Directorate;
 - (iv) the Intelligence Division of the National Defence Force;
 - (vii) a Special Investigating Unit;
 - (viii) the office of the Public Prosecutor;
 - (ix) an investigative division in an organ of state; or
 - (x) a supervisory body.

to facilitate the administration and enforcement of the laws of the Republic;
[Subsection (2)(a) substituted by section 2(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (aA) to administer measures requiring accountable institutions to freeze property and transactions pursuant to financial sanctions that may arise from resolutions adopted by the Security Council of the United Nations referred to in a notice contemplated in section 26A;
[Subsection (2)(aA) inserted by section 2(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (b) to exchange information with bodies with similar objectives in other countries regarding money laundering activities, the financing of terrorist and related activities, and other similar activities.
- (c) to supervise and enforce compliance with this Act or any directive made in terms of this Act and to facilitate effective supervision and enforcement by supervisory bodies.

4. Functions

To achieve its objectives the Centre must—

- (a) process, analyse and interpret information disclosed to it, and obtained by it, in terms of this Act;
- (aA) where appropriate, initiate analysis based on information in its possession or information received other than by means of reports made to it under Part 3 of Chapter 3;
[Paragraph (aA) inserted by section 3(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (b) inform, advise and co-operate with—
 - (i) an investigating authority;
 - (ii) the National Prosecuting Authority;
 - (iii) an intelligence service;
 - (iv) the South African Revenue Service;
 - (v) the Independent Police Investigative Directorate;
 - (vi) the Intelligence Division of the National Defence Force;
 - (vii) a Special Investigating Unit;
 - (viii) the Public Protector;
 - (ix) an investigative division in an organ of state; or
 - (x) a supervisory body;***[Paragraph (b) substituted by section 3(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (c) monitor and give guidance to accountable institutions, supervisory bodies and other persons regarding the performance and compliance by them of their duties and obligations in terms of this Act or any directive made in terms of this Act;
[Paragraph (c) substituted by section 4(a) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]
- (cA) provide information and guidance to accountable institutions that will assist accountable institutions in meeting requirements to freeze property and transactions pursuant to resolutions adopted by the Security Council of the United Nations referred to in a notice contemplated in section 26A;
[Paragraph (cA) substituted by section 3(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (d) retain the information referred to in paragraph (a) in the manner and for the period required by this Act;

-
- (e) annually review the implementation of this Act and submit a report thereon to the Minister;
[Paragraph (e) substituted by section 4(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]
 - (f) implement a registration system in respect of all accountable institutions and reporting institutions; and
[Paragraph (f) substituted by section 4(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]
 - (g) supervise and enforce compliance with this Act or any directive made in terms of this Act by accountable institutions, reporting institutions and other persons to whom the provisions of this Act apply that—
 - (i) are not regulated or supervised by a supervisory body in terms of this Act or any other law;
 - (ii) are regulated or supervised by a supervisory body in terms of this Act or any other law, if that supervisory body fails to enforce compliance despite any recommendation of the Centre made in terms of section 44(b).***[Paragraph (g) substituted by section 4(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]***

5. General powers

- (1) The Centre may do all that is necessary or expedient to perform its functions effectively, which includes the power to—
 - (a) determine its own staff establishment and the terms and conditions of employment for its staff within a policy framework determined by the Minister;
 - (b) appoint employees and seconded personnel to posts on its staff establishment;
 - (c) obtain the services of any person by agreement, including any state department, functionary or institution, to perform any specific act or function;
 - (d) acquire or dispose of any right in or to property, but rights in respect of immovable property may be acquired or disposed of only with the consent of the Minister;
 - (e) open and operate its own bank accounts, subject to the Public Finance Management Act, 1999 (Act No. 1 of 1999);
 - (f) insure itself against any loss, damage, risk or liability;
 - (g) perform legal acts or institute or defend any legal action in its own name;
 - (h) engage in any lawful activity, whether alone or together with any other organisation in the Republic or elsewhere, aimed at promoting its objectives;
 - (i) do anything that is incidental to the exercise of any of its powers.

6. Appointment of Director

- (1) The Minister must appoint a fit and proper person as the Director of the Centre.
 - (2) A person appointed as the Director holds office—
-

-
- (a) for a term not exceeding five years, but which is renewable; and
 - (b) on terms and conditions set out in a written employment contract, which must include terms and conditions setting specific, measurable performance standards.
- (3) ***[Subsection (3) deleted by section 4 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***

7. Removal from office

- (1) The Minister may remove the Director from office only on the grounds referred to in section 13 or on the grounds of misconduct, incapacity or incompetence.
- (2) The Minister may suspend the Director from office, pending—
 - (a) the determination of any enquiry as to whether grounds of misconduct, incapacity or incompetence exist; or
 - (b) the outcome of a security screening investigation referred to in section 13(3).

8. Acting Director

When the Director is absent or otherwise unable to perform the functions of office, or (during a vacancy in the office of Director, the Minister may designate another employee of the Centre to act as Director.

9. Proof of appointment

If the Minister has given notice in the *Gazette* of any appointment of a person as the Director or as acting director, this notice may be presented in a Court as proof of the appointment.

10. Responsibilities of Director

- (1) The Director—
 - (a) is responsible for the performance by the Centre of its functions;
 - (b) takes all decisions of the Centre in the exercise of its powers and the performance of its functions, except those decisions taken in consequence of a delegation or instruction in terms of section 16; and
 - (c) is the chief executive officer and also the accounting authority of the Centre.
 - (2) As the chief executive officer, the Director is responsible for—
 - (a) the formation and development of an efficient and performance driven
-

-
- administration;
 - (b) the management of the administration; and
 - (c) the control, and maintenance of discipline, of staff.
 - (3) As accounting authority of the Centre the Director must perform the functions assigned to accounting authorities in terms of the Public Finance Management Act, 1999 (Act No. 1 of 1999).
 - (4) The Director performs the functions of office subject to any policy framework, which may be prescribed by the Minister.

11. Staff

- (1) The staff of the Centre consists of—
 - (a) the Director; and
 - (b) persons appointed as employees of the Centre by the Director.
 - (2) An employee of an organ of state may be seconded to the Centre by agreement between the Centre and such organ of state.
 - (3) Staff members referred to in subsection (1)(b) and persons seconded to the Centre in terms of subsection (2) perform their duties subject to the control and directions of the Director.
 - (4) If an officer or employee in the public service is seconded to the Centre, the period of his or her service with the Centre must be calculated as part of and continuous with his or her employment in the public service, for purposes of leave, pension and any other condition of service.
 - (5) The provisions of any pension law applicable to an officer or employee referred to in subsection (4) or, in the event of his or her death, to his or her dependants, which are not inconsistent with this section, must, with the necessary changes, continue so to apply.
 - (6) No person seconded to the Centre or employed by the Centre to perform any of the functions of the Centre may strike or induce or conspire with any other member of the staff of the Centre to strike.
 - (7) The services of the Centre, for the purposes of the application of Chapter IV of the Labour Relations Act, 1995 (Act No. 66 of 1995), are deemed, to have been designated as an essential service in terms of section 71 of that Act.
 - (8) All other conditions of service of staff of the Centre are as determined in terms of this Act.
-

12. Security screening of staff of Centre other than Director

- (1) No person other than the Director may be appointed or seconded to perform any of the functions of the Centre unless—
 - (a) information with respect to that person has been gathered in a vetting investigation by the State Security Agency referred to in section 3 of the Intelligence Services Act, 2002 (Act No. 65 of 2002); and
[Subsection (1)(a) substituted by section 53 of the General Intelligence Laws Amendment Act, 2013 (Act No. 11 of 2013)]
 - (b) the Director, after evaluating the gathered information, is satisfied that such person may be so appointed without the possibility that such person might be a security risk or that he or she might act in any way prejudicial to the objectives or functions of the Centre.
- (2) If the Director is so satisfied, the Director must issue a certificate with respect to such person in which it is certified that such person has successfully undergone a security clearance.
- (3) Any person referred to in subsection (1) may at any time determined by the Director be subjected to a further security screening investigation as contemplated in subsection (1)(a).
- (4) The Director may withdraw a certificate referred to in subsection (2) if the Director obtains information from an investigation referred to in subsection (3) which, after evaluation by the Director, causes the Director to believe that the person in question could be a security risk or could possibly act in any manner prejudicial to the objectives or functions of the Centre.
- (5) If the certificate referred to in subsection (2) is withdrawn, the person concerned may not perform any functions of the Centre and the Director must discharge him or her from the Centre.

13. Security screening of Director of Centre

- (1) No person may be appointed as the Director of the Centre unless—
 - (a) information with respect to that person has been gathered in a vetting investigation by the State Security Agency referred to in section 3 of the Intelligence Services Act, 2002 (Act No. 65 of 2002); and
[Subsection (1)(a) substituted by section 53 of the General Intelligence Laws Amendment Act, 2013 (Act No. 11 of 2013)]
 - (b) the Minister, after evaluating the gathered information, is satisfied that such person may be so appointed without the possibility that such person might be a security risk or that he or she might act in any manner prejudicial to the objectives or functions of the Centre.
 - (2) If the Minister is so satisfied, he or she must issue a certificate with respect to such person in which it is certified that such person has successfully undergone a security clearance.
-

- (3) The Director may at any time determined by the Minister be subjected to a further security screening investigation as Contemplated in subsection (1)(a).
- (4) The Minister may withdraw a certificate referred to in subsection (2) if the Minister obtains information from an investigation referred to in subsection (3) which, after evaluation by the Minister, causes the Minister to believe that the Director could be a security risk or could possibly act in any manner prejudicial to the objectives or functions of the Centre.
- (5) If the certificate referred to in subsection (2) is withdrawn, the Director may not perform any functions of the Centre and the Minister must discharge him or her from the Centre.

14. Funds and financial year of Centre

- (1) The funds of the Centre consist of—
 - (a) money appropriated annually by Parliament for the purposes of the Centre;
 - (b) any government grants made to it; and
 - (c) any other money legally acquired by it, provided that the Centre may accept donations only with the prior written approval of the Minister.
- (2) The financial year of the Centre ends on 31 March in each year.

15. Audit

The Auditor-General must audit and report on the accounts and financial records of the Centre.

16. Delegation

- (1) The Director may—
 - (a) delegate, in writing, any of the powers entrusted to the Centre in terms of this Act to a member of the staff of the Centre; or
 - (b) instruct a member of the staff to perform any of the functions assigned to the Centre in terms of this Act.
- (2) A delegation or instruction in terms of subsection (1)—
 - (a) is subject to the limitations or conditions that the Director may impose; and
 - (b) does not divest the Director of the responsibility concerning the exercise of the delegated power or the performance of the assigned function.
- (3) The Director may confirm, vary or revoke any decision taken by a staff member in

consequence of a delegation or instruction in terms of subsection (1), as long as no such variation or revocation of a decision detracts from any rights that may have accrued as a result of the decision.

- (4) A person seconded to the Centre in terms of section 11(2) is for the purposes of this section regarded as being a staff member.

[Repealed] Chapter 2 : Counter-Money laundering advisory Council

[Chapter 2 repealed by section 5 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- 17. [Repealed] Establishment
- 18. [Repealed] Functions
- 19. [Repealed] Composition
- 20. [Repealed] Meetings and procedure

17. [Repealed] Establishment

[Section 17 repealed by section 5 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

18. [Repealed] Functions

[Section 18 repealed by section 5 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

19. [Repealed] Composition

[Section 19 repealed by section 5 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

20. [Repealed] Meetings and procedure

[Section 20 repealed by section 5 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Chapter 3 : Money Laundering, Financing of Terrorist and Related Activities and Financial Sanctions Control Measures

[Chapter 3 heading substituted by section 6 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Part 1 : Duty to identify clients

Part 2 : Duty to keep record

Part 3 : Reporting duties and access to information

Part 4 : Measures to promote compliance by accountable institutions

Part 5 : Referral and supervision

Part 1 : Customer due diligence

[Part 1 heading to Chapter 3 substituted by section 7 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

20A. Anonymous clients and clients acting under false or fictitious names

21. Identification of clients and other persons

21A. Understanding and obtaining information on business relationship

21B. Additional due diligence measures relating to legal persons, trusts and partnerships

21C. Ongoing due diligence

21D. Doubts about veracity of previously obtained information

21E. Inability to conduct customer due diligence

21F. Foreign prominent public official

21G. Domestic prominent influential person

21H. Family members and known close associates

20A. Anonymous clients and clients acting under false or fictitious names

An accountable institution may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name.

[Section 20A inserted by section 8 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21. Identification of clients and other persons

- (1) When an accountable institution engages with a prospective client to enter into a single transaction or to establish a business relationship, the institution must, in the course of concluding that single transaction or establishing that business relationship

and in accordance with its Risk Management and Compliance Programme—

- (a) establish and verify the identity of the client;
- (b) if the client is acting on behalf of another person, establish and verify—
 - (i) the identity of that other person; and
 - (ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and
- (c) if another person is acting on behalf of the client, establish and verify—
 - (i) the identity of that other person; and
 - (ii) that other person's authority to act on behalf of the client.

[Subsection (1) substituted by section 9 of the Financial Intelligence Centre Act, 2017 (Act No. 1 of 2017)]

- (2) If an accountable institution had established a business relationship with a client before this Act took effect, the accountable institution may not conclude a transaction in the course of that business relationship, unless the accountable institution has taken the prescribed steps—
 - (a) to establish and verify the identity of the client;
 - (b) if another person acted on behalf of the client in establishing the business relationship, to establish and verify—
 - (i) the identity of that other person; and
 - (ii) that other person's authority to act on behalf of the client;
 - (c) if the client acted on behalf of another person in establishing the business relationship, to establish and verify—
 - (i) the identity of that other person; and
 - (ii) the client's authority to act on behalf of that other person; and
 - (d) to trace all accounts at that accountable institution that are involved in transactions concluded in the course of that business relationship.

21A. Understanding and obtaining information on business relationship

When an accountable institution engages with a prospective client to establish a business relationship as contemplated in section 21, the institution must, in addition to the steps required under section 21 and in accordance with its Risk Management and Compliance Programme, obtain information to reasonably enable the accountable institution to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with the institution's knowledge of that prospective client, including information describing—

- (a) the nature of the business relationship concerned;
- (b) the intended purpose of the business relationship concerned; and
- (c) the source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship concerned.

[Section 21A inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21B. Additional due diligence measures relating to legal persons, trusts and partnerships

- (1) If a client contemplated in section 21 is a legal person or a natural person acting on behalf of a partnership, trust or similar arrangement between natural persons, an accountable institution must, in addition to the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme, establish—
 - (a) the nature of the client's business; and
 - (b) the ownership and control structure of the client.
 - (2) If a client contemplated in section 21 is a legal person, an accountable institution must, in addition to the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme—
 - (a) establish the identity of the beneficial owner of the client by—
 - (i) determining the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person;
 - (ii) if in doubt whether a natural person contemplated in subparagraph (i) is the beneficial owner of the legal person or no natural person has a controlling ownership interest in the legal person, determining the identity of each natural person who exercises control of that legal person through other means; or
 - (iii) if a natural person is not identified as contemplated in subparagraph (ii), determining the identity of each natural person who exercises control over the management of the legal person, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director or manager; and
 - (b) take reasonable steps to verify the identity of the beneficial owner of the client, so that the accountable institution is satisfied that it knows who the beneficial owner is.
 - (3) If a natural person, in entering into a single transaction or establishing a business relationship as contemplated in section 21, is acting on behalf of a partnership between natural persons, an accountable institution must, in addition to the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme—
 - (a) establish the identifying name of the partnership, if applicable;
 - (b) establish the identity of every partner, including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership;
 - (c) establish the identity of the person who exercises executive control over the partnership;
 - (d) establish the identity of each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the partnership;
 - (e) take reasonable steps to verify the particulars obtained in paragraph (a); and
 - (f) take reasonable steps to verify the identities of the natural persons referred to in paragraphs (b) to (d) so that the accountable institution is satisfied that it knows the identities of the natural persons concerned.
 - (4) If a natural person, in entering into a single transaction or establishing a business
-

relationship as contemplated in section 21, is acting in pursuance of the provisions of a trust agreement between natural persons, an accountable institution must, in addition to the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme—

- (a) establish the identifying name and number of the trust, if applicable;
 - (b) establish the address of the Master of the High Court where the trust is registered, if applicable;
 - (c) establish the identity of the founder;
 - (d) establish the identity of—
 - (i) each trustee; and
 - (ii) each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the trust;
 - (e) establish—
 - (i) the identity of each beneficiary referred to by name in the trust deed or other founding instrument in terms of which the trust is created; or
 - (ii) if beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined;
 - (f) take reasonable steps to verify the particulars obtained in paragraphs (a), (b) and (e)(ii); and
 - (g) take reasonable steps to verify the identities of the natural persons referred to in paragraphs (c), (d) and (e)(i) so that the accountable institution is satisfied that it knows the identities of the natural persons concerned.
- (5) This section applies in respect of a legal person, partnership or trust or a similar arrangement between natural persons, whether it is incorporated or originated in the Republic or elsewhere.

[Section 21B inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21C. Ongoing due diligence

An accountable institution must, in accordance with its Risk Management and Compliance Programme, conduct ongoing due diligence in respect of a business relationship, which includes—

- (a) monitoring of transactions undertaken throughout the course of the relationship, including, where necessary—
 - (i) the source of funds, to ensure that the transactions are consistent with the accountable institution's knowledge of the client and the client's business and risk profile; and
 - (ii) the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose; and
- (b) keeping information obtained for the purpose of establishing and verifying the identities of clients pursuant to sections 21, 21A and 21B of this Act, up to date.

[Section 21C inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017]

(Act No. 1 of 2017)]**21D. Doubts about veracity of previously obtained information**

When an accountable institution, subsequent to entering into a single transaction or establishing a business relationship, doubts the veracity or adequacy of previously obtained information which the institution is required to verify as contemplated in sections 21 and 21B, the institution must repeat the steps contemplated in sections 21 and 21B in accordance with its Risk Management and Compliance Programme and to the extent that is necessary to confirm the information in question.

[Section 21D inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21E. Inability to conduct customer due diligence

If an accountable institution is unable to—

- (a) establish and verify the identity of a client or other relevant person in accordance with section 21 or 21B;
 - (b) obtain the information contemplated in section 21A; or
 - (c) conduct ongoing due diligence as contemplated in section 21C,
- the institution—
- (i) may not establish a business relationship or conclude a single transaction with a client;
 - (ii) may not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction; or
 - (iii) must terminate, in accordance with its Risk Management and Compliance Programme, an existing business relationship with a client,
- as the case may be, and consider making a report under section 29 of this Act.

[Section 21E inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21F. Foreign prominent public official

If an accountable institution determines in accordance with its Risk Management and Compliance Programme that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a foreign prominent public official, the institution must—

- (a) obtain senior management approval for establishing the business relationship;
 - (b) take reasonable measures to establish the source of wealth and source of funds of the client; and
 - (c) conduct enhanced ongoing monitoring of the business relationship.
-

[Section 21F inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21G. Domestic prominent influential person

If an accountable institution determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a domestic prominent influential person and that, in accordance with its Risk Management and Compliance Programme, the prospective business relationship entails higher risk, the institution must—

- (a) obtain senior management approval for establishing the business relationship;
- (b) take reasonable measures to establish the source of wealth and source of funds of the client; and
- (c) conduct enhanced ongoing monitoring of the business relationship.

[Section 21G inserted by section 10 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

21H. Family members and known close associates

- (1) Sections 21F and 21G apply to immediate family members and known close associates of a person in a foreign or domestic prominent position, as the case may be.
- (2) For the purposes of subsection (1), an immediate family member includes—
 - (a) the spouse, civil partner or life partner;
 - (b) the previous spouse, civil partner or life partner, if applicable;
 - (c) children and step children and their spouse, civil partner or life partner;
 - (d) parents; and
 - (e) sibling and step sibling and their spouse, civil partner or life partner.

Part 2 : Duty to keep record

- 22. Obligation to keep customer due diligence records
 - 22A. Obligation to keep transaction records
 - 23. Period for which records must be kept
 - 24. Records may be kept by third parties
 - 25. Admissibility of records
 - 26. [Repealed] Centre's access to records
-

22. Obligation to keep customer due diligence records

[Section 22 heading substituted by section 11 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1) When an accountable institution is required to obtain information pertaining to a client or prospective client pursuant to sections 21 to 21H the institution must keep a record of that information.
- (2) Without limiting subsection (1), the records must—
 - (a) include copies of, or references to, information provided to or obtained by the accountable institution to verify a person's identity; and
 - (b) in the case of a business relationship, reflect the information obtained by the accountable institution under section 21A concerning—
 - (i) the nature of the business relationship;
 - (ii) the intended purpose of the business relationship; and
 - (iii) the source of the funds which the prospective client is expected to use in concluding transactions in the course of the business relationship.

[Section 22 substituted by section 11 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

22A. Obligation to keep transaction records

- (1) An accountable institution must keep a record of every transaction, whether the transaction is a single transaction or concluded in the course of a business relationship which that accountable institution has with the client, that are reasonably necessary to enable that transaction to be readily reconstructed.
- (2) Without limiting subsection (1), records must reflect the following information:
 - (a) The amount involved and the currency in which it was denominated;
 - (b) the date on which the transaction was concluded;
 - (c) the parties to the transaction;
 - (d) the nature of the transaction;
 - (e) business correspondence; and
 - (f) if an accountable institution provides account facilities to its clients, the identifying particulars of all accounts and the account files at the accountable institution that are related to the transaction.

[Section 22A inserted by section 12 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

23. Period for which records must be kept

An accountable institution must keep the records which relate to—

- (a) the establishment of a business relationship referred to in section 22, for at least five years from the date on which the business relationship is terminated;
-

-
- (b) a transaction referred to in section 22A which is concluded, for at least five years from the date on which that transaction is concluded; and
 - (c) a transaction or activity which gave rise to a report contemplated in section 29, for at least five years from the date on which the report was submitted to the Centre.

[Section 23 substituted by section 13 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

24. Records may be kept in electronic form and by third parties

[Section 24 heading substituted by section 14 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1) The duties imposed by sections 22 and 22A on an accountable institution to keep a record of the matters specified in those sections may be performed by a third party on behalf of the accountable institution as long as the accountable institution has free and easy access to the records and the records are readily available to the Centre and the relevant supervisory body for the purposes of performing its functions in terms of this Act.
- (2) If a third party referred to in subsection (1) fails to properly comply with the requirements of sections 22 and 22A on behalf of the accountable institution concerned, the accountable institution is liable for that failure.
- (3) If an accountable institution appoints a third party to perform the duties imposed on it by section 22 and 22A, the accountable institution must forthwith provide the Centre and the supervisory body concerned with the prescribed particulars regarding the third party.
- (4) Records kept in terms of sections 22 and 22A may be kept in electronic form and must be capable of being reproduced in a legible format.

[Section 24 substituted by section 14 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

25. Admissibility of records

A record kept in terms of section 22, 22A or 24, or a certified extract of any such record, or a certified printout of any extract of an electronic record, is on its mere production in a matter before a court admissible as evidence of any fact contained in it of which direct oral evidence would be admissible.

[Section 25 substituted by section 15 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

26. [Repealed] Centre's access to records

[Section 26 repealed by section 16 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Part 2A : Financial sanctions

26A. Notification of persons and entities identified by Security Council of the United Nations

26B. Prohibitions relating to persons and entities identified by Security Council of the United Nations

26C. Permitted financial services and dealing with property

26A. Notification of persons and entities identified by Security Council of the United Nations

- (1) Upon the adoption of a resolution by the Security Council of the United Nations under Chapter VII of the Charter of the United Nations, providing for financial sanctions which entail the identification of persons or entities against whom member states of the United Nations must take the actions specified in the resolution, the Minister must announce the adoption of the resolution by notice in the *Gazette* and other appropriate means of publication.
- (2) This section does not apply to resolutions of the Security Council of the United Nations contemplated in section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).
- (3) Following a notice contemplated in subsection (1) the Director must, from time to time and by appropriate means of publication, give notice of—
 - (a) persons and entities being identified by the Security Council of the United Nations pursuant to a resolution contemplated in subsection (1); and
 - (b) a decision of the Security Council of the United Nations to no longer apply a resolution contemplated in subsection (1) to previously identified persons or entities.
- (4) The Minister may revoke a notice contemplated in subsection (1) if the Minister is satisfied that the notice is no longer necessary to give effect to financial sanctions in terms of a resolution contemplated in subsection (1).

[Section 26A inserted by section 17 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

26B. Prohibitions relating to persons and entities identified by Security Council of the United Nations

- (1) No person may, directly or indirectly, in whole or in part, and by any means or method —
- (a) acquire, collect, use, possess or own property;
 - (b) provide or make available, or invite a person to provide or make available property;
 - (c) provide or make available, or invite a person to provide or make available any financial or other service;
 - (d) provide or make available, or invite a person to provide or make available economic support; or
 - (e) facilitate the acquisition, collection, use or provision of property, or the provision of any financial or other service, or the provision of economic support,
- intending that the property, financial or other service or economic support, as the case may be, be used, or while the person knows or ought reasonably to have known or suspected that the property, service or support concerned will be used, directly or indirectly, in whole or in part, for the benefit of, or on behalf of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1).
- (2) No person may, directly or indirectly, in whole or in part, and by any means or method deal with, enter into or facilitate any transaction or perform any other act in connection with property which such person knows or ought reasonably to have known or suspected to have been acquired, collected, used, possessed, owned or provided for the benefit of, or on behalf of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1).
- (3) No person who knows or ought reasonably to have known or suspected that property is property referred to in subsection (1), may enter into, or become concerned in, an arrangement which in any way has or is likely to have the effect of—
- (a) making it possible for a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1) to retain or control the property;
 - (b) converting the property;
 - (c) concealing or disguising the nature, source, location, disposition or movement of the property, the ownership thereof or any interest anyone may have therein;
 - (d) removing the property from a jurisdiction; or
 - (e) transferring the property to a nominee.

[Section 26B inserted by section 17 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

26C. Permitted financial services and dealing with property

- (1) The Minister may, in writing and on the conditions as he or she considers appropriate and in accordance with a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1), permit a person to conduct financial services or deal with property referred to in section 26B in the circumstances referred to in subsection (2).
 - (2) The Minister may permit the provision of financial services or the dealing with property if it is necessary to—
 - (a) provide for basic expenses, including, at least—
 - (i) foodstuffs;
 - (ii) rent or mortgage;
 - (iii) medicines or medical treatment;
 - (iv) taxes;
 - (v) insurance premiums;
 - (vi) public utility charges;
 - (vii) maintenance orders;
 - (viii) reasonable professional fees, and
 - (ix) reimbursement of expenses associated with the provision of legal services;
 - (b) satisfy a judgment or arbitral award that was made before the date on which the person or entity was identified by the Security Council of the United Nations;
 - (c) make a payment to a third party which is due under a contract, agreement or other obligation made before the date on which the person or entity was identified by the Security Council of the United Nations;
 - (d) accrue interest or other earnings due on accounts holding property affected by a prohibition under section 26B;
 - (e) make a payment due to a person or entity affected by a prohibition under section 26B by virtue of a contract, agreement or other obligation made before the date on which the person or entity was identified by the Security Council of the United Nations: Provided that the payment is not directly or indirectly being received by that person or entity.
 - (3) The Minister may permit the provision of financial services or the dealing with property under subsection (1) on his or her own initiative or at the request of a person affected by a prohibition under section 26B.
 - (4) The Director must, by appropriate means of publication, give notice of the Minister's permission of the provision of financial services or the dealing with property under subsection (1).
 - (5)
 - (a) The Minister may, in writing, delegate any power conferred in terms of this section, to the Director.
 - (b) A delegation in terms of paragraph (a)—
 - (i) is subject to any limitations or conditions that the Minister may impose;
 - (ii) does not divest the Minister of the responsibility concerning the exercise of the delegated power or the performance of the assigned duty.
-

-
- (c) The Minister may vary or revoke any decision taken by the Director as a result of a delegation in terms of paragraph (a), subject to any rights that may have vested as a consequence of the decision.

[Section 26C inserted by section 17 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Part 3 : Reporting duties and access to information

- 27. Accountable institutions to advise Centre of clients
- 27A. Powers of access by authorised representative to records in respect of reports required to be submitted to Centre
- 28. Cash transactions above prescribed limit
- 28A. Property associated with terrorist and related activities
- 29. Suspicious and unusual transactions
- 30. Conveyance of cash to or from Republic
- 31. Electronic transfers of money to or from Republic
- 32. Reporting procedures and furnishing of additional information
- 33. Continuation of transactions
- 34. Intervention by Centre
- 35. Monitoring orders
- 36. Information held by supervisory bodies and South African Revenue Service
- 37. Reporting duty and obligations to provide information not affected by confidentiality rules
- 38. Protection
- 39. Admissibility as evidence of reports made to Centre
- 40. Access to information held by Centre
- 41. Protection of confidential information
- 41A. Protection of personal information

27. Accountable institutions to advise Centre of clients

[Section 27 heading substituted by section 18 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

If an authorised representative of the Centre requests an accountable institution, a reporting institution or a person that is required to make a report in terms of section 29 of this Act to advise—

- (a) whether a specified person is or has been a client of the accountable institution, reporting institution or person;
 - (b) whether a specified person is acting or has acted on behalf of any client of the accountable institution, reporting institution or person;
 - (c) whether a client of the accountable institution, reporting institution or person is acting or has acted for a specified person;
 - (d) whether a number specified by the Centre was allocated by the accountable institution, reporting institution or person to a person with whom the accountable institution, reporting institution or person has or has had a business relationship; or
 - (e) on the type and status of a business relationship with a client of the accountable
-

institution, reporting institution or person,
the accountable institution, reporting institution or person must inform the Centre accordingly.

[Section 27 substituted by section 18 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

27A. Powers of access by authorised representative to records in respect of reports required to be submitted to Centre

- (1) Subject to subsection (2), an authorised representative of the Centre has access during ordinary working hours to any records kept by or on behalf of an accountable institution in terms of section 22, 22A or 24, and may examine, make extracts from or copies of, any such records for the purposes of obtaining further information in respect of a report made or ought to be made in terms of section 28, 28A, 29, 30(1) or 31.
- (2) The authorised representative of the Centre may, except in the case of records which the public is entitled to have access to, exercise the powers mentioned in subsection (1) only by virtue of a warrant issued in chambers by a magistrate or regional magistrate or judge of an area of jurisdiction within which the records or any of them are kept, or within which the accountable institution conducts business.
- (3) A warrant may only be issued if it appears to the judge, magistrate or regional magistrate from information on oath or affirmation that there are reasonable grounds to believe that the records referred to in subsection (1) may assist the Centre to identify the proceeds of unlawful activities or to combat money laundering activities or the financing of terrorist and related activities.
- (4) A warrant issued in terms of this section may contain such conditions regarding access to the relevant records as the judge, magistrate or regional magistrate considers appropriate.
- (5) An accountable institution must without delay give to an authorised representative of the Centre all reasonable assistance necessary to enable that representative to exercise the powers mentioned in subsection (1).

[Section 27A inserted by section 19 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

28. Cash transactions above prescribed limit

An accountable institution and a reporting institution must, within the prescribed period, report to the Centre the prescribed particulars concerning a transaction concluded with a client if in terms of the transaction an amount of cash in excess of the prescribed amount—

- (a) is paid by the accountable institution or reporting institution to the client, or to a person acting on behalf of the client, or to a person on whose behalf the client is
-

-
- (b) acting; or
is received by the accountable institution or reporting institution from the client, or from a person acting on behalf of the client, or from a person on whose behalf the client is acting.

28A. Property associated with terrorist and related activities

[Section 28A heading substituted by section 20(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1) An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of—
- (a) any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;
 - (b) a specific entity identified in a notice issued by the President, under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or
 - (c) a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1),
- must within the prescribed period report that fact and the prescribed particulars to the Centre.

[Subsection (1) substituted by section 20(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) The Director may direct an accountable institution which has made a report under subsection (1) to report—
- (a) at such intervals as may be determined in the direction that it is still in possession or control of the property in respect of which the report under subsection (1) had been made; and
 - (b) any change in the circumstances concerning the accountable institution's possession or control of that property.
- (3) An accountable institution must upon—
- (a) publication of a proclamation by the President under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or
 - (b) notice being given by the Director under section 26A(3),
- scrutinise its information concerning clients with whom the accountable institution has business relationships in order to determine whether any such client is a person or entity mentioned in the proclamation by the President or the notice by the Director.

[Subsection (3) inserted by section 20(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

29. Suspicious and unusual transactions

- (1) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that—
 - (a) the business has received or is about to receive the proceeds of unlawful activities;
 - (b) a transaction or series of transactions to which the business is a party—
 - (i) facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities;
 - (ii) has no apparent business or lawful purpose;
 - (iii) is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; or
 - (iv) may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service;
 - (vi) relates to the contravention of a prohibition under section 26B; or
[Subsection (1)(b)(vi) inserted by section 21(b) of the Financial Intelligence Amendment Act, 2017 (Act No. 1 of 2017)]
 - (c) the business has been used or is about to be used in any way for money laundering purposes,

must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.
- (2) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that a transaction or a series of transactions about which inquiries are made, may, if that transaction or those transactions had been concluded, have caused any of the consequences referred to in subsection (1)(a), (b) or (c), must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.
- (3) No person who made or must make a report in terms of this section may, subject to subsection 45B(2A), disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than—
[Words preceding subsection (3)(a) substituted by the Financial Intelligence Amendment Act, 2017 (Act No. 1 of 2017)]
 - (a) within the scope of the powers and duties of that person in terms of any legislation;
 - (b) for the purpose of carrying out the provisions of this Act;
 - (c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
 - (d) in terms of an order of court.
- (4) No person who knows or suspects that a report has been or is to be made in terms of this section may disclose that knowledge or suspicion or any information regarding the contents or suspected contents of any such report to any other person, including the person in respect of whom the report is or is to be made, otherwise than—

-
- (a) within the scope of that person's powers and duties in terms of any legislation;
 - (b) for the purpose of carrying out the provisions of this Act;
 - (c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
 - (d) in terms of an order of court.

30. Conveyance of cash to or from Republic

- (1) A person who intends conveying or who has conveyed or who is conveying an amount of cash or a bearer negotiable instrument in excess of the prescribed amount to or from the Republic must, on demand, report the prescribed particulars concerning that conveyance to a person authorised by the Minister for this purpose.
[Subsection (1) substituted by section 8 of the Financial Intelligence Centre Act, 2008 (Act No. 11 of 2008)]
- (2) A person authorised in terms of subsection (1) must without delay send a copy of the report to the Centre.

31. Electronic transfers of money to or from Republic

If an accountable institution through electronic transfer sends money in excess of a prescribed amount out of the Republic or receives money in excess of a prescribed amount from outside the Republic on behalf, or on the instruction, of another person, it must, within the prescribed period after the money was transferred, report the transfer, together with the prescribed particulars concerning the transfer, to the Centre.

32. Reporting procedures and furnishing of additional information

- (1) A report in terms of section 28, 29 or 31 to the Centre and a report in terms of section 30(1) to a person authorised by the Minister must be made in the prescribed manner.
 - (2) The Centre may request an accountable institution, a reporting institution or any other person that has made a report in terms of section 28, 29 or 31 to furnish the Centre with such additional information, including prescribed information relating to transactional activity and supporting documentation, concerning the report and the grounds for the report as the Centre may reasonably require for the performance by it of its functions.
[Subsection (2) substituted by section 22(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
 - (3) When an institution or a person referred to in subsection (2) receives a request under that subsection, that institution or person must furnish the Centre in the prescribed manner and within the prescribed period with such additional information concerning the report and the grounds for the report as that institution or person may have
-

available.

[Subsection (3) substituted by section 22(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

33. Continuation of transactions

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.

34. Intervention by Centre

- (1) If the Centre, after consulting an accountable institution, a reporting institution or a person required to make a report in terms of section 28 or 29, has reasonable grounds to suspect that a transaction or a proposed transaction may—
 - (a) involve—
 - (i) the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities; or
 - (ii) property owned or controlled by or on behalf of, or at the direction of 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); or
 - (b) constitute—
 - (i) money laundering; or
 - (ii) a transaction contemplated in section 29(1)(b),it may direct the accountable institution, reporting institution or person in writing not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 days as determined by the Centre, in order to allow the Centre to make the necessary inquiries concerning the transaction and, if the Centre considers it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions.
- (2) For the purposes of calculating the period of 10 days in subsection (1), Saturdays, Sundays and proclaimed public holidays must not be taken into account.
- (3) Subsection (1) does not apply to the carrying out of a transaction to which the rules of an exchange licensed in terms of the Financial Markets Act, 2012 (Act No. 19 of 2012), apply.

[Section 33 substituted by section 23 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

35. Monitoring orders

- (1) A judge designated by the Minister of Justice for the purposes of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), may, upon written application by the Centre, order an accountable institution to report to the Centre, on such terms and in such confidential manner as may be specified in the order, all transactions concluded by a specified person with the accountable institution or all transactions conducted in respect of a specified account or facility at the accountable institution, if there are reasonable ground, to suspect that—
- (a) that person has transferred or may transfer to the accountable institution—
 - (i) the proceeds of unlawful activities;
 - (ii) property which is connected to an offence relating to the financing of terrorist and related activities; or
 - (iii) property owned or controlled by or on behalf of, or at the direction of 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);
 - (b) that account or other facility has received or may receive—
 - (i) the proceeds of unlawful activities;
 - (ii) property which is connected to an offence relating to the financing of terrorist and related activities; or
 - (iii) property owned or controlled by or on behalf of, or at the direction of 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);
 - (c) that person is using or may use the accountable institution for money laundering purposes or for the financing of terrorist acts or for the purpose of any transaction contemplated in section 29(1)(b); or
 - (d) that account or other facility is being or may be used for money laundering purposes or for the financing of terrorist or related activities or for the purpose of any transaction contemplated in section 29(1)(b).
- [Subsection (1) substituted by section 24 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (2) An order in terms of subsection (1) lapses after three months unless extended in terms of subsection (3).
- (3) A judge referred to in subsection (1) may extend an order issued in terms of subsection (1) for further periods not exceeding three months at a time if—
- (a) the reasonable grounds for the suspicion on which the order is based still exist; and
 - (b) the judge is satisfied that the interest of justice is best served by monitoring the person, account or facility referred to in subsection (1) in the manner provided for in this section.
- (4) An application referred to in subsection (1) must be heard and an order must be issued without notice to or hearing the person or persons involved in the suspected money laundering activities.

36. Information held by supervisory bodies and South African Revenue Service

- (1) If a supervisory body or the South African Revenue Service knows or suspects that an accountable institution, wittingly or unwittingly has received or is about to receive the proceeds of unlawful activities or has been used or may be used in future for money laundering purposes or for the purpose of any transaction contemplated in section 29(1)(b), it must advise the Centre and any authority, service or body contemplated in section 3 or any other supervisory body that, in the opinion of the supervisory body or the South African Revenue Service, may have an interest therein, of that fact and furnish them with all information and any records regarding that knowledge or suspicion which they may reasonably require to identify the proceeds of unlawful activities or to combat money laundering activities or financing of terrorist and related activities.

[Subsection (1) substituted by section 10(a) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- (2) If the Centre believes that a supervisory body or the South African Revenue Service may have information indicating that an accountable institution, wittingly or unwittingly has received or is about to receive the proceeds of unlawful activities or has been used or may be used in future for money laundering purposes or for the purpose of any transaction contemplated in section 29(1)(b), the Centre may request that supervisory body or the South African Revenue Service to confirm or rebut that belief and the supervisory body or South African Revenue Service, as the case may be, must do so and, if that belief is confirmed, must furnish the Centre and any authority, service or body referred to in section 3 or any other supervisory body identified by the Centre that may have an interest in that matter with all information and any records regarding that knowledge or suspicion which the Centre may reasonably require for the achievement of its objectives.

[Subsection (2) substituted by section 10(a) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- (3) The Commissioner for the South African Revenue Service and the chief executive officer of a supervisory body may make such reasonable procedural arrangements and impose such reasonable safeguards regarding the furnishing of information referred to in subsections (1) and (2) as the Commissioner or such officer considers appropriate to maintain the confidentiality, if any, of that information.

37. Reporting duty and obligations to provide information not affected by confidentiality rules

- (1) Subject to subsection (2), 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 or agreement, affects compliance by an accountable institution, supervisory body, reporting institution, the South African Revenue Service or any other person with a provision of this Part, Part 4 and Chapter 4.

[Subsection (1) substituted by section 11 of the Financial Intelligence Centre

Amendment Act, 2008 (Act No. 11 of 2008)]

- (2) Subsection (1) does not apply to the common law right to legal professional privilege as between an attorney and the attorney's client in respect of communications made in confidence between—
- (a) the attorney and the attorney's client for the purposes of legal advice or litigation which is pending or contemplated or which has commenced; or
 - (b) a third party and an attorney for the purposes of litigation which is pending or contemplated or has commenced.

38. Protection

- (1) No action, whether criminal or civil, lies against an accountable institution, reporting institution, supervisory body, the South African Revenue Service or any other person complying in good faith with a provision of this Part, Part 4 and Chapter 4, including any director, employee or other person acting on behalf of such accountable institution, reporting institution, supervisory body, the South African Revenue Service or such other person.

[Subsection (1) substituted by section 12 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- (2) A person who has made, initiated or contributed to a report in terms of section 28, 29 or 31 or who has furnished additional information concerning such a report or the grounds for such a report in terms of a provision of this Part is competent, but not compellable, to give evidence in criminal proceedings arising from the report
- (3) No evidence concerning the identity of a person who has made, initiated or contributed to a report in terms of section 28, 29 or 31 or who has furnished additional information concerning such a report or the grounds for such a report in terms of a provision of this Part, or the contents or nature of such additional information or grounds, is admissible as evidence in criminal proceedings unless that person testifies at those proceedings.

39. Admissibility as evidence of reports made to Centre

A certificate issued by an official of the Centre that information specified in the certificate was reported or sent to the Centre in terms of section 28, 29, 30(2) or 31 is, subject to section 38(3), on its mere production in a matter before a court admissible as evidence of any fact contained in it of which direct oral evidence would be admissible.

40. Access to information held by Centre

- (1) Subject to this section, the Centre must make information reported to it, or obtained by it under this Part and information generated by its analysis of information so
-

reported or obtained, available to—

- (a) an investigating authority in the Republic;
- (aA) the National Prosecuting Authority;
- (aB) the Independent Police Investigative Directorate;
- (aC) an intelligence service;
- (aD) the Intelligence Division of the National Defence Force;
- (aE) a Special Investigating Unit;
- (aF) an investigative division in an organ of state;
- (aG) the Public Protector; or
- (aH) the South African Revenue Service;
- (b) an entity outside the Republic performing similar functions to those of the Centre, or an investigating authority outside the Republic;
- (c) a supervisory body;
- (d) a person who is entitled to receive such information in terms of an order of a court; or
- (e) a person who is entitled to receive such information in terms of other national legislation.

- (1A) Information contemplated in subsection (1) may only be made available to an entity referred to in subsection (1)(a), (aA), (aB), (aC), (aD), (aE), (aF), (aG) or (aH)—
 - (a) at the initiative of the Centre or at the request of an authorised officer of the entity; and
 - (b) if the Centre reasonably believes such information is required to investigate suspected unlawful activity.
 - (1B) Information contemplated in subsection (1) may only be made available to an entity or authority referred to in subsection (1)(b)—
 - (a) at the initiative of the Centre or at the request of the entity or authority; and
 - (b) if the Centre reasonably believes such information is relevant to the identification of the proceeds of unlawful activities or the combating of money laundering or financing of terrorist and related activities or similar offences in the country in which the entity or authority is established.
 - (1C) Information contemplated in subsection (1) may only be made available to a supervisory body referred to in subsection (1)(d)—
 - (a) at the initiative of the Centre or at the request of the supervisory body; and
 - (b) if the Centre reasonably believes such information is relevant to the exercise by the supervisory body of its powers or performance by it of its functions under any law.
 - (2) A request for information contemplated in subsection (1A) or (1C) must be in writing and must specify the required information and the purpose for which the information is required.
 - (3) The Director may, as a condition to the provision of any information contemplated in subsection (1), make the reasonable procedural arrangements and impose the reasonable safeguards regarding the furnishing of such information that the Director considers appropriate to maintain the confidentiality of that information before the information is provided.
 - (4) Information contemplated in subsection (1) may only be provided to an entity or
-

authority referred to in subsection (1)(b) pursuant to a written agreement between the Centre and the entity or the authority which is responsible for the entity or authority, regulating the exchange of information between the Centre and the entity or authority.

- (5) An agreement referred to in subsection (4) does not—
- (a) take effect until it has been approved in writing by the Minister;
 - (b) permit the Centre to provide any category of information to the entity or authority in respect of which the agreement is concluded which the entity or authority is not permitted to provide to the Centre.
- (6) A person who obtains information from the Centre may use that information only—
- (a) within the scope of that person's powers and duties; and
 - (b) in the case of a request contemplated in subsection (2), for the purpose specified in that request.
- (7) The Centre may make available any information obtained by it during an inspection to an organ of state, a supervisory body, other regulatory authority, self-regulating association or organisation which the Centre reasonably believes is affected by or has an interest in that information.
- (8) The Centre must make information it holds available to the appropriate National Intelligence Structure, as defined in section 1 of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), if it reasonably believes that the information relates to any potential threat or threat to the national security, as defined in section 1 of that Act.

[Subsection (8) inserted by section 25 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (9) The Centre may, at the initiative of the Centre or on written request, disclose information it holds, other than information contemplated in subsections (1), (7) and (8), to an accountable institution or class of accountable institutions or any other person unless the Centre reasonably believes that the disclosure may—
- (a) inhibit the achievement of the Centre's objectives or the performance of its functions, or the achievement of the objectives or the performance of the functions of another organ of state; or
 - (b) prejudice the rights of any person.

[Subsection (9) inserted by section 25 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

[Section 40 substituted by section 25 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

41. Protection of confidential information

No person may disclose confidential information held by or obtained from the Centre except—

- (a) within the scope of that person's powers and duties in terms of any legislation;
- (b) for the purpose of carrying out the provisions of this Act;

- (c) with the permission of the Centre;
- (d) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
- (e) in terms of an order of court.

41A. Protection of personal information

- (1) The Centre must ensure that appropriate measures are taken in respect of personal information in its possession or under its control to prevent—
 - (a) loss of, damage to or unauthorised destruction of the information; and
 - (b) unlawful access to or processing of personal information, other than in accordance with this Act and the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).
- (2) In order to give effect to subsection (1) the Centre must take reasonable measures to —
 - (a) identify all reasonable and foreseeable internal and external risks to personal information in its possession or under its control;
 - (b) establish and maintain appropriate safeguards against the risks identified;
 - (c) regularly verify that the safeguards are effectively implemented; and
 - (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

[Section 41A inserted by section 26 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Part 4 : Measures to promote compliance by accountable institutions

- 42. Risk Management and Compliance Programme
- 42A. Governance of anti-money laundering and counter terrorist financing compliance
- 42B. Consultation process for issuing guidance
- 43. Training and monitoring of compliance
- 43A. Directives
- 43B. Registration by accountable institution and reporting institution

42. Risk Management and Compliance Programme

[Section 42 heading substituted by section 27 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1) An accountable institution must develop, document, maintain and implement a programme for anti-money laundering and counter-terrorist financing risk management and compliance.
- (2) A Risk Management and Compliance Programme must—

-
- (a) enable the accountable institution to—
 - (i) identify;
 - (ii) assess;
 - (iii) monitor;
 - (iv) mitigate; and
 - (v) manage,the risk that the provision by the accountable institution of products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities;
 - (b) provide for the manner in which the institution determines if a person is—
 - (i) a prospective client in the process of establishing a business relationship or entering into a single transaction with the institution; or
 - (ii) a client who has established a business relationship or entered into a single transaction;
 - (c) provide for the manner in which the institution complies with section 20A;
 - (d) provide for the manner in which and the processes by which the establishment and verification of the identity of persons whom the accountable institution must identify in terms of Part 1 of this Chapter is performed in the institution;
 - (e) provide for the manner in which the institution determines whether future transactions that will be performed in the course of the business relationship are consistent with the institution's knowledge of a prospective client;
 - (f) provide for the manner in which and the processes by which the institution conducts additional due diligence measures in respect of legal persons, trust and partnerships;
 - (g) provide for the manner in which and the processes by which ongoing due diligence and account monitoring in respect of business relationships is conducted by the institution;
 - (h) provide for the manner in which the examining of—
 - (i) complex or unusually large transactions; and
 - (ii) unusual patterns of transactions which have no apparent business or lawful purpose,and keeping of written findings relating thereto, is done by the institution;
 - (i) provide for the manner in which and the processes by which the institution will confirm information relating to a client when the institution has doubts about the veracity of previously obtained information;
 - (j) provide for the manner in which and the processes by which the institution will perform the customer due diligence requirements in accordance with sections 21, 21A, 21B and 21C when, during the course of a business relationship, the institution suspects that a transaction or activity is suspicious or unusual as contemplated in section 29;
 - (k) provide for the manner in which the accountable institution will terminate an existing business relationship as contemplated in section 21E;
 - (l) provide for the manner in which and the processes by which the accountable institution determines whether a prospective client is a foreign prominent public official or a domestic prominent influential person;
 - (m) provide for the manner in which and the processes by which enhanced due diligence is conducted for higher-risk business relationships and when simplified customer due diligence might be permitted in the institution;
 - (n) provide for the manner in which and place at which the records are kept in
-

-
- terms of Part 2 of this Chapter;
 - (o) enable the institution to determine when a transaction or activity is reportable to the Centre under Part 3 of this Chapter;
 - (p) provide for the processes for reporting information to the Centre under Part 3 of this Chapter;
 - (q) provide for the manner in which—
 - (i) the Risk Management and Compliance Programme is implemented in branches, subsidiaries or other operations of the institution in foreign countries so as to enable the institution to comply with its obligations under this Act;
 - (ii) the institution will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under this Act; and
 - (iii) the institution will inform the Centre and supervisory body concerned if the host country contemplated in sub-paragraph (ii) does not permit the implementation of measures required under this Act;
 - (r) provide for the processes for the institution to implement its Risk Management and Compliance Programme; and
 - (s) provide for any prescribed matter.
- (2A) An accountable institution must indicate in its Risk Management and Compliance Programme if any paragraph of subsection (2) is not applicable to that accountable institution and the reason why it is not applicable.
- (2B) The board of directors, senior management or other person or group of persons exercising the highest level of authority in an accountable institution must approve the Risk Management and Compliance Programme of the institution.
- (2C) An accountable institution must review its Risk Management and Compliance Programme at regular intervals to ensure that the Programme remains relevant to the accountable institution's operations and the achievement of the requirements contemplated in subsection (2).
- (3) An accountable institution must make documentation describing its Risk Management and Compliance Programme available to each of its employees involved in transactions to which this Act applies.
- (4) An accountable institution must, on request, make a copy of its internal rules available to –
 - (a) the Centre; or
 - (b) a supervisory body which performs regulatory or supervisory functions in respect of that accountable institution.

[Section 42 substituted by section 27 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

42A. Governance of anti-money laundering and counter terrorist financing compliance

- (1) The board of directors of an accountable institution which is a legal person with a board of directors, or the senior management of an accountable institution without a board of directors, must ensure compliance by the accountable institution and its employees with the provisions of this Act and its Risk Management and Compliance Programme.
- (2) An accountable institution which is a legal person must—
 - (a) have a compliance function to assist the board of directors or the senior management, as the case may be, of the institution in discharging their obligations under subsection (1); and
 - (b) assign a person with sufficient competence and seniority to ensure the effectiveness of the compliance function contemplated in paragraph (a).
- (3) The person or persons exercising the highest level of authority in an accountable institution which is not a legal person must ensure compliance by the employees of the institution with the provisions of this Act and its Risk Management and Compliance Programme, in so far as the functions of those employees relate to the obligations of the institution.
- (4) An accountable institution which is not a legal person, except for an accountable institution which is a sole practitioner, must appoint a person or persons with sufficient competence to assist the person or persons exercising the highest level of authority in the accountable institution in discharging their obligation under subsection (3).

[Section 42A inserted by section 28 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

42B. Consultation process for issuing guidance

Before issuing guidance to accountable institutions, supervisory bodies and other persons regarding the performance and compliance by them of their duties and obligations in terms of this Act or any directive made in terms of this Act, the Centre must—

- (a) publish a draft of the guidance by appropriate means of publication and invite submissions; and
- (b) consider submissions received.

43. Training relating to anti-money laundering and counter terrorist financing compliance

An accountable institution must provide ongoing training to its employees, to enable them to comply with the provisions of this Act and the Risk Management and Compliance Programme which are applicable to them.

43A. Directives

- (1)
- (a) The Centre may, by notice in the *Gazette*, issue a directive to all institutions to whom the provisions of this Act apply—
 - (i) regarding the application of this Act; or
 - (ii) which reasonably may be required to give effect to the Centre's objectives contemplated in section 3.
 - (b) The Centre may issue a directive in terms of paragraph (a) only after consulting with supervisory bodies on that directive.

[Subsection 1 substituted by section 30(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) The Centre or a supervisory body may, in writing, issue a directive to any category of accountable institutions or category of reporting institutions or other category of persons to whom the provisions of this Act apply—
- (a) regarding the application of this Act; or
 - (b) which reasonably may be required to give effect to the Centre's objectives contemplated in section 3.

[Subsection 2 substituted by section 30(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3) The Centre or a supervisory body may in writing, over and above any directive contemplated in subsection (1) or (2), issue a directive to any accountable institution, category of accountable institutions, reporting institution, category of reporting institutions or other person to whom the provisions of this Act apply, to—
- (a) provide the Centre or that supervisory body, as the case may be—
 - (i) with the information, reports or statistical returns specified in the notice, at the time or at the intervals specified in the notice; and
 - (ii) within the period specified in the notice, with any document in its possession or custody or under its control;
 - (b) cease or refrain from engaging in any act, omission or conduct in contravention of this Act;
 - (c) perform acts necessary to remedy an alleged non-compliance with this Act; or
 - (d) perform acts necessary to meet any obligation imposed by this Act.

- (4) The Centre or supervisory body may examine a document submitted to it in terms of subsection (3)(a) or make a copy thereof or part thereof.

- (5) The costs incurred in complying with a directive must be borne by the accountable institution, reporting institution or person concerned.

- (6)
- (a) The Centre, in respect of any accountable institution or category of accountable institutions regulated or supervised by a supervisory body in terms of this Act or any other law, may issue a directive in accordance with subsections (2) and (3) only—
 - (i) if a supervisory body failed to issue a directive despite any recommendation of the Centre made in terms of section 44(b); or
 - (ii) after consultation with the relevant supervisory body; and

[Subsection (6)(a) substituted by section 30(b) of the Financial Intelligence

Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (b) A supervisory body may issue a directive in terms of this section only after consulting the Centre on that directive.
- (7) Before the Centre of supervisory body concerned issues a directive, it must—
 - (a) in the case of a directive in terms of—
 - (i) subsection (1), in the in the *Gazette*, give notice where a draft of the directive will be available and invite submissions;
 - (ii) subsection (2), publish a draft of the directive by appropriate means of publication and invite submissions; and
 - (b) consider submissions received.

[Subsection (7) inserted by section 30(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

[Section 43A inserted by section 14 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

43B. Registration by accountable institution and reporting institution

- (1) Every accountable institution referred to in Schedule 1 and every reporting institution referred to in Schedule 3 must, within the prescribed period and in the prescribed manner, register with the Centre.
- (2) The registration of an accountable institution and a reporting institution contemplated in subsection (1) must be accompanied by such particulars as the Centre may require.
- (3) The Centre must keep and maintain a register of every accountable institution and reporting institution registered in terms of subsection (1).
- (4) A registered accountable institution or reporting institution must notify the Centre, in writing, of any changes to the particulars furnished in terms of this section within 90 days after such a change.

[Section 43B inserted by section 14 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

Part 5 : Referral and supervision

- 44. Referral of suspected offences to investigating authorities and other public bodies
- 45. Responsibility for supervision of accountable institutions

44. Referral of suspected offences to investigating authorities and other public bodies

If the Centre in the performance of its functions has reasonable grounds to suspect that an accountable institution, or any other person other than a supervisory body who is subject to the provisions of this Act, has contravened or failed to comply with any provision of this Act or any rule or guideline applicable to that accountable institution or person which facilitates compliance with this Act, it may, if it considers it appropriate to do so, refer the matter to—

- (a) a relevant investigating authority; or
- (b) an appropriate supervisory body or other public body or authority affected by it, together with any recommendation the Centre considers appropriate.

45. Responsibility for supervision of accountable institutions

- (1) Every supervisory body is responsible for supervising and enforcing compliance with this Act or any order, determination or directive made in terms of this Act by all accountable institutions regulated or supervised by it.

[Subsection (1) substituted by section 15(a) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

(1A)

- (a) The obligation referred to in subsection (1) forms part of the legislative mandate of any supervisory body and constitutes a core function of that supervisory body.
- (b) Any Act that regulates a supervisory body or authorises that supervisory body to supervise or regulate any accountable institution must be read as including subsection (1), and a supervisory body may utilise any fees or charges it is authorised to impose or collect to defray expenditure incurred in performing its obligations under this Act or any order, determination or directive made in terms of this Act.

[Subsection (1A) inserted by section 15(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- (1B) A supervisory body, in meeting its obligation referred to in subsection (1), may—
 - (a) in addition to any powers it has in terms of another Act, exercise any power afforded to it in this Act;
 - (b) delegate the exercise of any power contemplated in paragraph (a) to any of its members, employees or any other suitable person;
 - (c) take any measures it considers necessary or expedient to meet its obligations imposed by this Act or any order, determination or directive made in terms of this Act, or to achieve the objectives of the Centre or this Act;
 - (d) require an accountable institution supervised or regulated by it to report on that institution's compliance with this Act or any order, determination or directive made in terms of this Act in the form, manner and timeframes determined by the supervisory body;
 - (e) issue or amend any licence, registration, approval or authorisation that the supervisory body may issue or grant in accordance with any Act, to include the following conditions:
 - (f) compliance with this Act; and

- (g) the continued availability of human, financial, technological and other resources to ensure compliance with this Act or any order, determination or directive made in terms of this Act; and
- (h) in making a determination in accordance with any Act applicable to it as to whether a person is fit and proper to hold office in an accountable institution, take into account any involvement, whether directly or indirectly, by that person in any non-compliance with this Act or any order, determination or directive made in terms of this act, or, prior to the commencement of this Act or at any time thereafter, any involvement in—
 - (i) any money laundering activity; or
 - (ii) any terrorist or related activity.

[Subsection (1B) inserted by section 15(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- (1C) A supervisory body must submit to the Centre, within the prescribed period and in the prescribed manner, a written report on any action taken against any accountable institution in terms of this Act or any order, determination or directive made in terms of this Act.

[Subsection (1C) inserted by section 15(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

(1D)

- (a) The Centre and a supervisory body must coordinate their approach to exercising their powers and performing their functions in terms of this Act to ensure the consistent application of the Act, and must enter into a written memorandum of understanding in respect thereof.
- (b) The memorandum of understanding must provide for—
 - (i) the sharing of information between the parties, which must include—
 - (aa) the types of information to be furnished by each party; or
 - (bb) measures to protect confidentiality of the information, including limiting access to specified persons or incumbents of specified positions, subject to section 40(3) and other provisions of this Act and other applicable legislation;
 - (ii) cooperation between the parties and assisting each other in the exercise of their respective powers and the performance of their respective duties in terms of this Act;
 - (iii) a dispute resolution mechanism; and
 - (iv) such other matters as may be prescribed.

[Subsection (1D) substituted by section 31 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) When the Centre refers a matter to a supervisory body or other public body or authority in terms of section 44, that supervisory body or other public body or authority must investigate the matter and may, after consultation with the Centre, take such steps within the scope of its powers as it considers appropriate to remedy the matter.
- (3) Should a supervisory body or other public body or authority to which a suspected contravention or failure is referred in term of section 44 fail to take adequate steps to ensure that the suspected contravention ceases or the suspected failure is rectified, the Centre may, after consultation with the supervisory body or other public body or

authority concerned, take such steps within the scope of its powers as the Centre considers appropriate to remedy the matter.

Chapter 4 : Compliance and Enforcement

[Chapter 4 heading substituted by section 16(a) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

- 45A. Appointment of inspectors
 - 45B. Inspections
 - 45C. Administrative sanctions
 - 45D. Appeal
 - 45E. Establishment of appeal board
 - 45F. Application to court
 - 46. Failure to identify persons
 - 46A. Failure to comply with duty in regard to customer due diligence
 - 47. Failure to keep records
 - 48. Destroying or tampering with records
 - 49. Failure to give assistance
 - 49A. Contravention of prohibitions relating to persons and entities identified by Security Council of United Nations
 - 50. Failure to advise Centre of client
 - 51. Failure to report cash transactions
 - 51A. Failure to report property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations Security Council
 - 52. Failure to report suspicious or unusual transactions
 - 53. Unauthorised disclosure
 - 54. Failure to report conveyance of cash or bearer negotiable instrument into or out of Republic
 - 55. Failure to send report to Centre
 - 56. Failure to report electronic transfers
 - 57. Failure to comply with request
 - 58. Failure to comply with directives
 - 59. Failure to comply with monitoring order
 - 60. Misuse of information
 - 61. Failure to formulate and implement internal rules
 - 61A. Failure to register with Centre
 - 62. Failure to provide training or appoint compliance officer
 - 62A. Offences relating to inspection
 - 62B. Hindering or obstructing appeal board
 - 62C. Failure to attend when summoned
 - 62D. Failure to answer fully or truthfully
 - 63. Obstructing of official in performance of functions
 - 64. Conducting transactions to avoid reporting duties
 - 65. Unauthorised access to computer system or application or data
 - 66. Unauthorised modification of contents of computer system
 - 67. Definitions
 - 68. Penalties
 - 69. Defences
-

- 70. Search, seizure and forfeiture
- 71. Jurisdiction of courts

45A. Appointment of inspectors

- (1) The Director or the head of a supervisory body, as the case may be, may appoint any person in the service of the Centre or supervisory body or any other suitable person as an inspector.
- (2) The Director or the head of a supervisory body may determine the remuneration to be paid to a person who is appointed in terms of subsection(1) that is not in the full-time service of the Centre or supervisory body.
- (3)
 - (a) The Director or the head of a supervisory body must issue an inspector contemplated in subsection (1) with a certificate of appointment signed by the Director or the head of that supervisory body.
 - (b) A certificate of appointment must specify—
 - (i) the full name of the person so appointed;
 - (ii) his or her identity number;
 - (iii) his or her signature;
 - (iv) his or her photograph;
 - (v) a description of the capacity in which he or she is appointed; and
 - (vi) the extent of his or her powers to inspect.
- (4)
 - (a) Where the head of a supervisory body is authorised by any other Act to appoint inspectors, the head may extend the appointment and functions of inspectors under that Act to include the undertaking of inspections under this Act.
 - (b) An inspector whose appointment or functions have been extended under paragraph (a) may, in undertaking inspections under this Act, in addition to the functions afforded to such inspector under the Act contemplated in paragraph (a), perform the functions afforded in this Act.
 - (c) Any extension contemplated in paragraph (a) must be reflected in any certificate or appointment document issued by the head of the supervisory body to an inspector under the Act contemplated in that paragraph.
- (5) When an inspector undertakes an inspection in terms of this Act, the inspector must—
 - (a) be in possession of a certificate of appointment issued in terms of subsection (3) or contemplated in subsection 4(c); and
 - (b) on request, show that certificate to any person who is—
 - (i) affected by the performance of the functions of the inspector; or
 - (ii) is in charge of any premises to be inspected.

[Section 45A inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

45B. Inspections

- (1)
- (a) In this section "**compliance**" means compliance with a provision of this Act or any order, determination or directive made in terms of this Act and which, if not complied with, constitutes non-compliance.
 - (b) An inspector appointed in terms of section 45A may enter the premises, excluding a private residence, of an accountable institution or reporting institution which is registered in terms of section 43B or otherwise licensed or authorised by a supervisory body and inspect the affairs of the accountable institution or reporting institution, as the case may be, for the purposes of determining compliance.
- [Subsection (1) substituted by section 32(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (1A) An inspector appointed in terms of section 45A may, for the purposes of determining compliance and on the authority of a warrant issued under subsection (1B), enter and inspect—
- (a) a private residence; or
 - (b) any premises other than premises contemplated in subsection (1)(b) or paragraph (a) (in this section referred to as "unlicensed business premises"),
- if the Centre or a supervisory body reasonably believes that the residence or premises are used for a business to which the provisions of this Act apply.
- [Subsection (1A) inserted by section 32(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (1B) A magistrate or judge may issue a warrant contemplated in subsection (1A)—
- (a) on written application by the Centre or a supervisory body setting out under oath or affirmation why it is necessary for an inspector to enter and inspect the private residence or unlicensed business premises; and
 - (b) if it appears to the magistrate or judge from the information under oath or affirmation that—
 - (i) there are reasonable grounds for suspecting that an act of non-compliance has occurred;
 - (ii) entry and inspection of the private residence or unlicensed business premises are likely to yield information pertaining to the non-compliance; and
 - (iii) entry and inspection of that residence or those premises are reasonably necessary for the purposes of determining compliance.
- [Subsection (1B) inserted by section 32(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (1C) An inspector otherwise required to obtain a warrant for entry and inspection of a private residence or unlicensed business premises in terms of subsection (1A), may enter and inspect that residence or those premises without a warrant—
- (a) with the consent of—
 - (i) in the case of a private residence—
 - (aa) the person apparently in control of the business reasonably believed to be conducted at the private residence; and
 - (bb) the occupant of the part of the private residence to be entered and inspected; or
-

- (ii) in the case of unlicensed business premises, the person apparently in control of the business reasonably believed to be conducted at the premises, after informing him or her that he or she is under no obligation to admit the inspector in the absence of a warrant; or
- (b) with the prior authority of the Director or the head of a supervisory body, or a senior staff member of the Centre or supervisory body delegated to perform the function, if the Director, head or senior staff member on reasonable grounds believes that—
 - (i) a warrant will be issued under subsection (1B) if applied for;
 - (ii) the delay in obtaining the warrant is likely to defeat the purpose for which entry and inspection of the private residence or unlicensed business premises is sought; and
 - (iii) it is necessary to enter and inspect that residence or those premises to perform any or all of the actions contemplated in section 45B(2)(a) to (f).

[Subsection (1C) inserted by section 32(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1D) Where an inspector enters and inspects premises in terms of subsection (1)(b), or a private residence or unlicensed business premises in terms of subsection (1C), he or she must do so—
 - (a) at a reasonable time within ordinary business hours or, in the case of an entry and inspection in terms of subsection (1C)(b), if the inspector on reasonable grounds believes that the purpose for which the entry and inspection is sought, is likely to be defeated by a delay, as closely to ordinary business hours as the circumstances reasonably permit;
 - (b) on reasonable notice, where appropriate;
 - (c) with strict regard to an affected person's right to—
 - (i) dignity;
 - (ii) freedom and security;
 - (iii) privacy; and
 - (iv) other constitutional rights; and
 - (d) with strict regard to decency and good order as the circumstances require, in particular by—
 - (i) entering and inspecting only such areas or objects as are reasonably required for purposes of section 45B(2);
 - (ii) conducting the inspection discreetly and with due decorum;
 - (iii) causing as little disturbance as possible; and
 - (iv) concluding the inspection as soon as possible.

[Subsection (1D) inserted by section 32(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (1E) Subsection (1D)(c) and (d) apply with the necessary changes where an inspector enters and inspects premises on the authority of a warrant issued under subsection (1B).

[Subsection (1E) inserted by section 32(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) An inspector, in conducting an inspection, may—
 - (a) in writing direct a person to appear for questioning before the inspector at a time and place determined by the inspector;

-
- (b) order any person who has or had any document in his, her or its possession or under his, her or its control relating to the affairs of the accountable institution, reporting institution or person—
 - (i) to produce that document; or
 - (ii) to furnish the inspector at the place and in the manner determined by the inspector with information in respect of that document;
 - (c) open any strongroom, safe or other container, or order any person to open any strongroom, safe or other container, in which the inspector suspects any document relevant to the inspection is kept;
 - (d) use any computer system or equipment on the premises or require reasonable assistance from any person on the premises to use that computer system to—
 - (i) access any data contained in or available to that computer system; and
 - (ii) reproduce any document from that data;
 - (e) examine or make extracts from or copy any document in the possession of an accountable institution, reporting institution or person or, against the issue of a receipt, remove that document temporarily for that purpose; and
 - (f) against the issue of a receipt, seize any document obtained in terms of paragraphs (c) to (e), which in the opinion of the inspector may constitute evidence of non-compliance with a provision of this Act or any order, determination or directive made in terms of this Act.
- (2A) When acting in terms of subsection (2)(b) or (d), an inspector of—
- (a) the Centre;
 - (b) a supervisory body referred to in item 1 or 2 of Schedule 2; or
 - (c) any other supervisory body meeting the prescribed criteria,
- may order from an accountable institution or reporting institution under inspection, the production of a copy of a report, or the furnishing of a fact or information related to the report, contemplated in section 29.
- [Subsection (2A) inserted by section 32(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (2B) If the inspector of a supervisory body, referred to in subsection (2A)(b) or (c), obtained a report, or a fact or information related to the report, under subsection (2A), that supervisory body must request information from the Centre under section 40(1C) relating to the report contemplated in section 29 which may be relevant to such inspection.
- [Subsection (2B) inserted by section 32(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (2C) For purposes of subsection (2B), the Centre must provide the information to the inspector of the supervisory body in accordance with section 40.
- [Subsection (2C) inserted by section 32(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (3) An accountable institution, reporting institution or other person to whom this Act applies, must without delay provide reasonable assistance to an inspector acting in terms of subsection (2).
- (4) The Centre or a supervisory body may recover all expenses necessarily incurred in conducting an inspection from an accountable institution or reporting institution inspected.
-

[Subsection (4) substituted by section 32(d) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (5)
- (a) Subject to section 36 and paragraph (b), an inspector may not disclose to any person not in the service of the Centre or supervisory body any information obtained in the performance of functions under this Act.
 - (b) An inspector may disclose information—
 - (i) for the purpose of enforcing compliance with this Act or any order, determination or directive made in terms of this Act;
 - (ii) for the purpose of legal proceedings;
 - (iii) when required to do so by a court; or
 - (iv) except information contemplated in subsection (2A) and (2C), if the Director or supervisory body is satisfied that it is in the public interest.
- [Subsection (5)(b)(iv) substituted by section 32(e) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***

- (6)
- (a) An inspector appointed by the Director may, in respect of any accountable institution regulated or supervised by a supervisory body in terms of this Act or any other law, conduct an inspection only if a supervisory body failed to conduct an inspection despite any recommendation of the Centre made in terms of section 44(b) or failed to conduct an inspection within the period recommended by the Centre.
 - (b) ***[Subsection (6)(b) deleted by section 32(f) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
 - (c) An inspector appointed by the Director may on the request of a supervisory body accompany and assist an inspector appointed by the head of a supervisory body in conducting an inspection in terms of this section.
- (7) ***[Subsection (7) deleted by section 32(g) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***

[Section 45C inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

45C. Administrative sanctions

- (1) The Centre or a supervisory body may impose an administrative sanction on any accountable institution, reporting institution or other person to whom this Act applies when satisfied on available facts and information that the institution or person—
- (a) has failed to comply with a provision of this Act or any order, determination or directive made in terms of this Act;
 - (b) has failed to comply with a condition of a licence, registration, approval or authorisation issued or amended in accordance with section 45(1B)(V);
 - (c) has failed to comply with a directive issued in terms section 34(1) or 43A(3); or
 - (d) has failed to comply with a non-financial administrative sanction imposed in terms of this section.
-

-
- (2) When determining an appropriate administrative sanction, the Centre or the supervisory body must consider the following factors:
- (a) The nature, duration, seriousness and extent of the relevant noncompliance;
 - (b) whether the institution or person has previously failed to comply with any law;
 - (c) any remedial steps taken by the institution or person to prevent a recurrence of the non-compliance;
 - (d) any steps taken or to be taken against the institution or person by—
 - (i) another supervisory body; or
 - (ii) a voluntary association of which the institution or person is a member; and
 - (e) any other relevant factor, including mitigating factors.
- (3) The Centre or supervisory body may impose any one or more of the following administrative sanctions:
- (a) A caution not to repeat the conduct which led to the non-compliance referred to in subsection (1);
 - (b) a reprimand;
 - (c) a directive to take remedial action or to make specific arrangements;
 - (d) the restriction or suspension of certain specified business activities; or
 - (e) a financial penalty not exceeding R10 million in respect of natural persons and R50 million in respect of any legal person.
- (4) The Centre or supervisory body may—
- (a) in addition to the imposition of an administrative sanction, make recommendations to the relevant institution or person in respect of compliance with this Act or any order, determination or directive made in terms of this Act;
 - (b) direct that a financial penalty must be paid by a natural person or persons for whose actions the relevant institution is accountable in law, if that person or persons was or were personally responsible for the non-compliance;
 - (c) suspend any part of an administrative sanction on any condition the Centre or the supervisory body deems appropriate for a period not exceeding five years.
- (5) Before imposing an administrative sanction, the Centre or supervisory body must give the institution or person reasonable notice in writing—
- (a) of the nature of the alleged non-compliance;
 - (b) of the intention to impose an administrative sanction;
 - (c) of the amount or particulars of the intended administrative sanction; and
 - (d) that the institution or person may, in writing, within a period specified in the notice, make representations as to why the administrative sanction should not be imposed.
- (6)
- (a) After considering any representations and the factors referred to in subsection (2), the Centre, subject to paragraph (c), or supervisory body may impose an administrative sanction the Centre or supervisory body considers appropriate.
 - (b) Upon imposing the administrative sanction the Centre or supervisory body must, in writing, notify the institution or person—
 - (i) of the decision and the reasons therefor; and
 - (ii) of the right to appeal against the decision in accordance with section
-

45D.

- (c) The Centre must, prior to taking a decision contemplated in paragraph (a), consult the relevant supervisory body, if applicable.
- (7)
- (a) Any financial penalty imposed must be paid into the National Revenue Fund within the period and in the manner as may be specified in the relevant notice.
[Subsection (7)(a) substituted by section 33 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
 - (b) If the institution or person fails to pay the financial penalty within the specified period and an appeal has not been lodged within the required period, the Centre or supervisory body may forthwith file with the clerk or registrar of a competent court a certified copy of the notice contemplated in subsection (6)(b), and the notice thereupon has the effect of a civil judgment lawfully given in that court in favour of the Centre or supervisory body.
- (8) An administrative sanction contemplated in this section may not be imposed if the respondent has been charged with a criminal offence in respect of the same set of facts.
- (9) If a court assesses the penalty to be imposed on a person convicted of an offence in terms of this Act, the court must take into account any administrative sanction imposed under this section in respect of the same set of facts.
- (10) An administrative sanction imposed in terms of this Act does not constitute a previous conviction as contemplated in Chapter 27 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).
- (11) Unless the Director or supervisory body is of the opinion that there are exceptional circumstances present that justify the preservation of the confidentiality of a decision the Director or supervisory body must make public the decision and the nature of any sanction imposed if—
- (a) an institution or person does not appeal against a decision of the Centre or supervisory body within the required period; or
 - (b) the appeal board confirms the decision of the Centre or supervisory body.

[Section 45C inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

45D. Appeal

- (1)
- (a) Any institution or person may appeal against a decision of the Centre or supervisory body made in terms of section 45C(6) to the appeal board.
 - (b) An appeal must be lodged within 30 days in the manner, and on payment of the fees, prescribed by the Minister.
 - (c) The appeal board may, on good cause shown, grant condonation to an appellant who has failed to lodge an appeal timeously as provided for in

paragraph (b).

[Subsection (1)(c) inserted by section 34(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (2) An appeal under subsection (1) shall take place on the date and at the place and time determined by the appeal board.
- (3) An appeal is decided on the written evidence, factual information and documentation submitted to the Centre or the supervisory body before the decision which is subject to the appeal was taken.

[Subsection (3) substituted by section 34(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3A) Subject to subsection (4), no oral or written evidence or factual information and documentation, other than that which was available to the Centre or supervisory body and the written reasons for the decision of the Centre or the supervisory body, may be submitted to the appeal board by a party to the appeal.

[Subsection (3A) inserted by section 34(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3B) Despite subsection (3), the chairperson of the appeal board may on application by—
- (a) the appellant concerned, and on good cause shown, allow further oral and written evidence or factual information and documentation not made available to the Centre or the supervisory body prior to the making of the decision against which the appeal is lodged; or
 - (b) the Centre or the supervisory body concerned, and on good cause shown, allow further oral and written evidence or factual information and documentation to be submitted and introduced into the record of the appeal.

[Subsection (3B) inserted by section 34(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3C) If introduction by an appellant of further oral and written evidence or factual documentation is allowed into the record of the appeal under subsection (3B)(a), the matter must be submitted to the Centre or the supervisory body in question for reconsideration.

[Subsection (3C) inserted by section 34(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3D) When an appeal is submitted to the Centre or a supervisory body as contemplated in subsection (3C), the appeal is deferred pending the final decision of the Centre or the supervisory body.

[Subsection (3D) inserted by section 34(c) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

- (3E) If, after the Centre or the supervisory body concerned has made a final decision as contemplated in subsection (3D), the appellant continues with the appeal by giving written notice to the appeal board, the record must include the further oral evidence properly transcribed, the written evidence or factual information or documentation allowed, and the further reasons or documentation submitted by the Centre or the supervisory body concerned.

[Subsection (3E) inserted by section 34(c) of the Financial Intelligence Centre

Amendment Act, 2017 (Act No. 1 of 2017)]

- (4) For the purposes of allowing further oral evidence in terms of subsection (3B) the appeal board may—
[Words preceding subsection (4)(a) substituted by section 34(d) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (a) summon any person who, in its opinion, may be able to give information for the purposes of the appeal or who it believes has in his, her or its possession, custody or control any document which has any bearing upon the decision under appeal, to appear before it at a time and place specified in the summons, to be questioned or to produce that document, and retain for examination any document so produced;
 - (b) administer an oath to or accept an affirmation from any person called as a witness at an appeal; and
 - (c) call any person present at the appeal proceedings as a witness and interrogate such person and require such person to produce any document in his, her or its possession, custody or control, and such a person shall be entitled to legal representation at his or her own expense.
- (5) The chairperson of the appeal board determines the rules of the appeal and any other procedural matters relating to an appeal.
[Subsection (5) substituted by section 34(e) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (6) Any party to an appeal is entitled to be represented at an appeal by a legal representative.
- (6A) The chairperson of the appeal board manages the case load of the appeal board and must assign each appeal to an adjudication panel comprising of not less than three members of the appeal board.
[Subsection (6A) inserted by section 34(f) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (6B) The chairperson of the appeal board appoints a chairperson of an adjudication panel who presides over the proceedings of that panel and that chairperson has a deciding vote in the case of an equality of votes.
[Subsection (6B) inserted by section 34(f) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- (7) The appeal board may—
- (a) confirm, set aside or vary the relevant decision of the Centre or supervisory body; or
 - (b) refer a matter back for consideration or reconsideration by the Centre or the supervisory body concerned in accordance with the directions of the appeal board.
- (8) The decision of a majority of the members of an adjudication panel shall be the decision of the appeal board.
[Subsection (8) substituted by section 34(g) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
-

-
- (9) The decision of the appeal board must be in writing, and a copy thereof must be made available to the appellant and the Centre or supervisory body.
- (10)
- (a) If the appeal board sets aside any decision of the Centre or supervisory body, the fees contemplated in subsection (1)(b) paid by the appellant in respect of the appeal in question must be refunded to the appellant.
 - (b) If the appeal board varies any such decision, it may in its discretion direct that the whole or any part of such fees be refunded to the appellant.
- (11)
- (a) Subject to paragraph (b), a decision of the appeal board may be taken on appeal to the High Court as if it were a decision of a magistrate in a civil matter.
 - (b) The launching of appeal proceedings in terms of paragraph (a) does not suspend the operation or execution of a decision, unless the chairperson of the appeal board directs otherwise.

[Section 45D inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

45E. Establishment of appeal board

- (1) An appeal board is hereby established.
 - (2) The Minister must appoint as members of the appeal board so many persons as the Minister may consider necessary, with an alternate for each of them, of whom—
 - (a) one must be an advocate or attorney with at least ten years experience, who will be the chairperson; and
 - (b) at least two must be persons with experience and expert knowledge of financial institutions and financial services.
 - (3) A member of the appeal board holds office for a period of three years and is eligible for reappointment on the expiration of his or her term of office.
 - (4) An alternate acts as a member when—
 - (a) a member is absent, has recused himself or herself or is suspended; or
 - (b) the filling of a vacancy on the appeal board is pending.
 - (5) Any vacancy that occurs on the appeal board must be filled in accordance with subsection (2) and any person so appointed holds office for the unexpired portion of the period of office of his or her predecessor.
 - (6) The appeal board may co-opt any person having expert knowledge of a particular matter to assist the board in considering an appeal.
 - (7) A person co-opted under subsection (6) may not participate in any decision of the appeal board.
-

-
- (8) If before or during the consideration of any appeal it transpires that any member of the appeal board has any direct or indirect personal interest in the outcome of that appeal, that member must recuse himself or herself and must be replaced by the alternate member.
 - (9) The Minister may terminate the period of office of a member of the appeal board—
 - (a) if the performance of the member is unsatisfactory; or
 - (b) if the member, either through illness or for any other reason, is unable to perform the functions of office effectively.
 - (10)
 - (a) The Minister may, if the performance of the appeal board is unsatisfactory, terminate the period of office of all the members of the appeal board.
 - (b) In the event of the dismissal of all the members of the appeal board, the Minister may appoint persons to act as caretakers until competent persons are appointed in terms of subsection (2).
 - (11) A member of the appeal board may be paid such remuneration and allowances as the Minister may from time to time determine.
 - (12) The Centre must provide administrative support for the appeal board.
 - (13) The Centre is responsible for the expenditure of the appeal board.

[Section 45E inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

45F. Application to court

- (1)
 - (a) The Centre, in respect of any accountable institution regulated or supervised by a supervisory body in terms of this Act or any other law, may institute proceedings in accordance with this section only if a supervisory body failed to institute proceedings despite any recommendation of the Centre made in terms of section 44(b) or failed to institute proceedings within the period recommended by the Centre.
 - (b) A supervisory body may institute proceedings in accordance with this section only after consultation with the Centre on that application to court.
 - (2) Subject to subsection (1), the Centre or any supervisory body may institute proceedings in the High Court having jurisdiction against any accountable institution, reporting institution or person to whom this Act applies, to—
 - (a) discharge any obligation imposed on the Centre or supervisory body in terms of this Act;
 - (b) compel that institution or person to comply with any provision of this Act or to cease contravening a provision of this Act;
 - (c) compel that institution or person to comply with a directive issued by the Centre or supervisory body under this Act; or
 - (d) obtain a declaratory order against that institution or person on any point of law
-

relating to any provision of this Act or any order, determination or directive made in terms of this Act.

- (3) Subject to subsection (1), if the Centre or a supervisory body has reason to believe that an institution or person is not complying with this Act or any order, determination or directive made in terms of this Act, it may, if it appears that prejudice has occurred or might occur as a result of such non-compliance, apply to a court having jurisdiction for—
- (a) an order restraining that institution or person from continuing business pending an application to court by the Centre or supervisory body as contemplated in subsection (2); or
 - (b) any other legal remedy available to the Centre or supervisory body.

[Section 45F inserted by section 16(b) of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

46. Failure to identify persons

- (1) An accountable institution that performs any act to give effect to a business relationship or single transaction in contravention of section 21(1) or (1A) is non-compliant and is subject to an administrative sanction.
- (2) An accountable institution that concludes any transaction in contravention of section 21(2) is non-compliant and is subject to an administrative sanction.

[Subsection (3E) substituted by section 35 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

46A. Failure to comply with duty in regard to customer due diligence

An accountable institution that fails to comply with the duty to perform additional due diligence measures in accordance with section 21A, 21B, 21C, 21D, 21E, 21F, 21G or 21H is non-compliant and is subject to an administrative sanction.

[Section 46A inserted by section 36 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

47. Failure to keep records

An accountable institution that fails to—

- (a) keep a record of information in terms of section 22(1), or 22A(1) or (2);
 - (b) keep such records in accordance with section 23 or 24(1); or
 - (c) comply with the provisions of section 24(3),
-

is non-compliant and is subject to an administrative sanction.

[Section 47 substituted by section 36 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

48. Destroying or tampering with records

Any person who wilfully tampers with a record kept in terms of section 22 or section 24(1), or wilfully destroys such a record, otherwise than in accordance with section 23, is guilty of an offence.

49. Failure to give assistance

An accountable institution that fails to give assistance to a representative of the Centre in accordance with section 27A(5), is guilty of an offence.

[Section 49 substituted by section 38 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

49A. Contravention of prohibitions relating to persons and entities identified by Security Council of United Nations

Any person who contravenes a provision of section 26B is guilty of an offence.

[Section 49A inserted by section 39 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

50. Failure to advise Centre of client

An accountable institution, reporting institution or person that is required to make a report in terms of section 29 that fails to inform the Centre in accordance with section 27, is guilty of an offence.

[Section 50 substituted by section 40 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

51. Failure to report cash transactions

- (1) An accountable institution or reporting institution that fails, within the prescribed period, to report to the Centre the prescribed information in respect of a cash transaction in accordance with section 28, is guilty of an offence.
- (2) An accountable institution or reporting institution that fails, within the prescribed period, to report to the Centre the prescribed information in respect of a cash transaction in accordance with section 28, is non-compliant and is subject to an administrative sanction.

[Section 51 substituted by section 41 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

51A. Failure to report property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations Security Council Nations Security Council

- (1) An accountable institution that has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of an entity contemplated in section 28A(1), and that fails, within the prescribed period, to report that fact and the prescribed information in respect of such property to the Centre in accordance with that section, is guilty of an offence.
- (2) An accountable institution that fails to comply with a direction by the Director in accordance with section 28A(2), is guilty of an offence.
- (3) An accountable institution that fails to scrutinise the information as contemplated in section 28A(3), is guilty of an offence.
- (4) An accountable institution that fails to—
 - (a) report to the Centre in accordance with section 28A(1), within the prescribed period, the prescribed information in respect of its possession or control of property owned or controlled by or on behalf of, or at the direction of an entity contemplated in that section;
 - (b) comply with a direction by the Director in accordance with section 28A(2); or
 - (c) scrutinise the information as contemplated in section 28A(3),is non-compliant and is subject to an administrative sanction.

[Section 51A substituted by section 42 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

52. Failure to report suspicious or unusual transactions

- (1) Any person who fails, within the prescribed period, to report to the Centre the prescribed information in respect of a suspicious or unusual transaction or series of transactions or enquiry in accordance with section 29(1) or (2), is guilty of an offence.
- (2) Any person referred to in section 29(1) or (2) who reasonably ought to have known or suspected that any of the facts referred to in section 29(1)(a), (b) or (c) or section 29(2) exists, and who negligently fails to report the prescribed information in respect of a suspicious or unusual transaction or series of transactions or enquiry, is guilty of an offence.

53. Unauthorised disclosure

- (1) Any person referred to in section 29(3) who discloses a fact or information contemplated in that section, otherwise than in the circumstances or for the purposes authorised in that section, is guilty of an offence.
- (2) Any person referred to in section 29(4) who discloses a knowledge or suspicion or any information contemplated in that section, otherwise than in the circumstances and for the purposes authorised in that section, is guilty of an offence.

54. Failure to report conveyance of cash or bearer negotiable instrument into or out of Republic

Any person, who wilfully fails to report the conveyance of cash or a bearer negotiable instrument into or out of the Republic in accordance with section 30(1), is guilty of an offence.

[Section 54 substituted by section 18 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

55. Failure to send report to Centre

A person referred to in section 30(2) who fails to send a report regarding the conveyance of cash or bearer negotiable instrument to the Centre in accordance with that section, is guilty of an offence.

[Section 55 substituted by section 19 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

56. Failure to report electronic transfers

- (1) An accountable institution that fails to report to the Centre the prescribed information in respect of an electronic transfer of money in accordance with section 31, is guilty of an offence.
- (2) An accountable institution that fails to report to the Centre the prescribed information in respect of an electronic transfer of money in accordance with section 31, is non-compliant and is subject to an administrative sanction.

[Section 56 substituted by section 43 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

57. Failure to comply with request

An accountable institution, reporting, institution or any other person that fails to comply with a request made by—

- (a) the Centre or an investigating authority acting under the authority of an authorised officer in terms of section 32(2); or
 - (b) a supervisory body in terms of section 45(1B)(d),
- is guilty of an offence.

[Section 57 substituted by section 20 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

58. Failure to comply with directives

- (1) An accountable institution, that fails to comply with a direction of the Centre in terms of section 34(1), is guilty of an offence.
- (2) An accountable institution that fails to comply with a direction of the Centre in terms of section 34(1), is non-compliant and is subject to an administrative sanction.

[Substituted by section 21 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

59. Failure to comply with monitoring order

An accountable institution that fails to comply with an order by a judge in accordance with section 35, is guilty of an offence.

60. Misuse of information

- (1) Any person who—
- (a) discloses confidential information held by or obtained from the Centre otherwise than in accordance with section 40 or 41; or
[Subsection (1)(a) substituted by section 22 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]
 - (b) wilfully destroys or in any other way tampers with information kept by the Centre for the purposes of this Act;
[Subsection (1)(b) substituted by section 45(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
 - (c) uses information from the Centre otherwise than in accordance with—
 - (i) any arrangements or safeguards made or imposed by the Director in terms of section 40(3); or
 - (ii) section 40(6); or
[Subsection (1)(c) substituted by section 45(a) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
 - (d) discloses a fact or information contemplated in section 45B(2A), or uses such information, otherwise than as permitted by section 45B(5),
[Subsection (1)(d) inserted by section 45(b) of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]
- is guilty of an offence.
- (2) Any person who knows, suspects, or ought reasonably to have known or suspected—
- (a) that information has been disclosed to the Centre; or
 - (b) that an investigation is being, or may be, conducted as a result of information that has been or is to be disclosed to the Centre,
- and who directly or indirectly alerts, or brings information to the attention of, another person which will or is likely to prejudice such an investigation, is guilty of an offence.

61. Failure to formulate and implement internal rules

[Section 61 heading substituted by section 46 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

An accountable institution that fails to—

- (a) develop, document, maintain and implement an anti-money laundering and counter terrorist financing risk management and compliance programme in accordance with section 42(1), (2) and (2A);
 - (aA) obtain approval for its Risk Management and Compliance Programme in accordance with section 42(2B);
 - (aB) review its Risk Management and Compliance Programme at regular intervals in accordance with section 42(2C);
 - (b) make the Risk Management and Compliance Programme available to its employees in accordance with section 42(3); or
 - (c) make a copy of its Risk Management and Compliance Programme available to the Centre or a supervisory body in terms of section 42(4),
- is non-compliant and is subject to an administrative sanction.

[Section 61 substituted by section 46 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

61A. Failure to register with Centre

Any accountable institution or reporting institution that—

- (a) fails to register with the Centre in terms of section 43B; or
 - (b) fails to provide information in terms of section 43B,
- is non-compliant and is subject to an administrative sanction.

[Section 61A substituted by section 46 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

61B. Failure to comply with duty in regard to governance

- (1) The board of directors or senior management, or both, of an accountable institution that fails to ensure compliance in accordance with section 42A(1) is non-compliant and is subject to an administrative sanction.
- (2) An accountable institution that fails to appoint a person in accordance with section 42A(2) or 42A(4) is non-compliant and is subject to an administrative sanction.
- (3) A person that fails to ensure compliance in accordance with section 42A(3) is non-compliant and is subject to an administrative sanction.

[Section 61B inserted by section 47 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

62. Failure to provide training or appoint compliance officer

[Section 62 heading substituted by section 48 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

An accountable institution that fails to provide training to its employees in accordance with section 43(a) is non-compliant and is subject to an administrative sanction.

[Section 62 substituted by section 48 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

62A. Offences relating to inspection

A person who—

- (a) fails to appear for questioning in terms of section 45B(2)(a);
 - (b) fails to comply with an order contemplated in section 45B(2)(b);
 - (c) wilfully gives false information to an inspector;
 - (d) fails to comply with any reasonable request by an inspector in the performance of his or her functions; or
 - (e) wilfully hinders an inspector in the performance of his or her functions,
- is guilty of an offence.

[Section 62A inserted by section 24 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

62B. Hindering or obstructing appeal board

Any person who wilfully interrupts the proceedings of the appeal board or who wilfully hinders or obstructs the appeal board in the performance of its functions, is guilty of an offence.

[Section 62B inserted by section 24 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

62C. Failure to attend when summoned

Any person who, having been summoned to attend and give evidence or to produce any book, document or object before the Centre or a supervisory body or the appeal board—

- (a) fails without sufficient cause to appear at the time and place specified or to remain in attendance until excused; or
 - (b) attends as required, but—
 - (i) refuses to take an oath or to make affirmation; or
 - (ii) fails to produce a book, document or other item as ordered, if it is in the possession of, or under the control of, that person,
- is guilty of an offence.

[Section 62C inserted by section 24 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

62D. Failure to answer fully or truthfully

Any person who, having been sworn in or having made an affirmation before the Centre or a supervisory body or the appeal board—

-
- (a) fails to answer any question fully and to the best of that person's ability: or
 - (b) gives false evidence, knowing or believing it to be false, is guilty of an offence.

[Section 62D inserted by section 24 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

62E. Failure to comply with directives of Centre or supervisory body

An accountable institution that fails to comply with a directive of the Centre or a supervisory body in terms of section 43A(3) or 45C(3)(c) is non-compliant and is subject to an administrative sanction.

63. Obstructing of official in performance of functions

Any person who obstructs, hinders or threatens an official or representative of the Centre in the performance of their duties or the exercise of their powers in terms of this Act, is guilty of an offence.

64. Conducting transactions to avoid reporting duties

Any person who conducts, or causes to be conducted, two or more transactions with the purpose, in whole or in part, of avoiding giving rise to a reporting duty under this Act, is guilty of an offence.

65. Unauthorised access to computer system or application or data

- (1) Any person who, without authority to do so, wilfully accesses or causes any other person to access any computer system that belongs to, or is under the control of, the Centre, or any application or data held in such a computer system, is guilty of an offence.
 - (2) Any person who, without authority to do so, wilfully causes any computer system that belongs to, or is under the control of, the Centre, to perform or fail to perform a function, is guilty of an offence.
-

66. Unauthorised modification of contents of computer system

Any person who, without authority to do so, wilfully causes a computer system that belongs to, or is under the control of, the Centre, or any application or data held in such a computer system, to be modified, destroyed, erased or the operation or reliability of such a computer system, application or data to be otherwise impaired, is guilty of an offence.

67. Definitions

For the purposes of sections 65 and 66—

- (a) **"access"** in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data, and includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form or to a storage medium or by means of any output device, whether attached to the computer system in which the application or data are held or not;
- (b) **"application"** means a set of instructions that, when executed in a computer system, causes a computer system to perform a function;
- (c) **"computer system"** means an electronic, magnetic, optical, electrochemical or other data processing device, including the physical components thereof, and any removable storage medium that is for the time being therein or connected thereto, or a group of such interconnected or related devices, one or more of which is capable of —
 - (i) containing data; or
 - (ii) performing a logical, arithmetic or any other function in relation to data;
- (d) **"data"** means any representation of information, knowledge, facts or concepts, capable of being processed in a computer system.

68. Penalties

- (1) A person convicted of an offence mentioned in this Chapter, other than an offence mentioned in subsection (2), is liable to imprisonment for a period not exceeding 15 years or to a fine not exceeding R100 million.
- (2) A person convicted of an offence mentioned in section 55, 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million.

[Subsection (2) substituted by section 50 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

[Section 68 substituted by section 25 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

69. Defences

If a person who is an employee, director or trustee of, or a partner in, an accountable institution is charged with committing an offence under section 52, that person may raise as a defence the fact that he or she had—

- (a) complied with the applicable obligations in terms of the Risk Management and Compliance Programme relating to the reporting of information of the accountable institution; or
- (b) reported the matter to the person charged with the responsibility of ensuring compliance by the accountable institution with its duties under this Act; or
- (c) reported the matter to his or her superior, if any, if—
 - (i) the accountable institution had not appointed such a person or established such Risk Management and Compliance Programme;
 - (ii) the accountable institution had not complied with its obligations in section 42(3) in respect of that person; or
 - (iii) the Risk Management and Compliance Programme was not applicable to that person.

[Section 69 substituted by section 51 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

70. Search, seizure and forfeiture

- (1) A police official or person authorised by the Minister to receive a report under section 30(1), who has reasonable grounds to suspect that an offence under section 54 has been or is about to be committed, may at any time search any person, container or other thing in which any cash or bearer negotiable instrument contemplated in section 30(1) is suspected to be found.
 - (2) A police official or person authorised by the Minister referred to in subsection (1) may seize any cash or bearer negotiable instrument contemplated in section 30(1).
 - (3) Any cash or bearer negotiable instrument seized under subsection (2) must be returned to the person from whom it was seized as soon as possible—
 - (a) after the expiry of a period of 90 days from the date of the seizure, unless, before the expiry of that period—
 - (i) that person has been arrested, without a warrant of arrest being issued;
 - (ii) a warrant for the arrest of that person has been issued; or
 - (iii) a summons has been issued for that person to appear in court, in connection with the suspected (commission of an offence under section 54 in respect of that cash or bearer negotiable instrument or any portion of it;
 - (b) after the expiry of a period of 90 days from the date of the seizure, unless, before the expiry of that period, an application for a preservation order in terms of section 38 of the Prevention Act in respect of that cash or bearer negotiable instrument is pending before the High Court;
 - (c) if that person is acquitted on a charge of committing an offence under section
-

-
- 54; or
- (d) if a forfeiture order in terms of section 50 of the Prevention Act is not made in respect of that cash or bearer negotiable instrument.
- (4) Whenever any person is convicted of an offence under section 54 the court convicting that person must, in addition to any punishment which that court may impose in respect of the offence, declare any cash or bearer negotiable instrument contemplated in section 30(1) that was seized under subsection (2), or is in the possession or custody or under the control of the convicted person, to be forfeited to the State.
- (5) Whenever a person is convicted of an offence under section 64 the court convicting that person must, in addition to any punishment which that court may impose in respect of the offence, declare any property in respect of which those transactions were conducted to be forfeited to the State.
- (6) A declaration of forfeiture shall not affect any interest which any person other than the convicted person may have in the cash or bearer negotiable instrument or property concerned if that person proves—
- (a) that he or she acquired the interest in that cash or bearer negotiable instrument or property in good faith; and
- (b) that he or she did not know that the cash or bearer negotiable instrument or property in question was—
- (i) conveyed as contemplated in section 30(1) or that he or she could not prevent the cash or bearer negotiable instrument from being so conveyed; or
- (ii) used in the transactions contemplated in section 64 or that he or she could not prevent the property from being so used, as the case may be.
- (7) Subject to subsection (6), the court concerned or, if the judge or judicial officer concerned is not available, any judge or judicial officer of that court, may at any time within a period of three years from the date of the declaration of forfeiture, on the application of any person other than the convicted person who claims that he or she has any interest in the cash or bearer negotiable instrument in question, inquire into and determine any such interest.
- (8) Subject to subsection (6), if a court referred to in subsection (7) finds that—
- (a) the cash or bearer negotiable instrument or bearer negotiable instrument or property in question belonged to the applicant at the time of the forfeiture, the court must set aside the declaration of forfeiture in question and direct that the cash or bearer negotiable instrument or property be returned to the applicant or, if the State has disposed of it, direct that the applicant be compensated by the State in an amount equal to the amount of cash or bearer negotiable instrument or the value of the property forfeited; or
- (b) the applicant had an interest in the cash or bearer negotiable instrument or property in question at the time of the forfeiture, the court must direct that the applicant be compensated by the State in an amount equal to the value of his or her interest in the cash or bearer negotiable instrument or property.
- (9) Any person aggrieved by a determination made by a court under subsection (8), may appeal against the determination as if it were a conviction by the court making the
-

determination, and such appeal may be heard either separately or jointly with an appeal against the conviction as a result of which the declaration of forfeiture was made, or against a sentence imposed as a result of such conviction.

- (10) In order to make a declaration of forfeiture or to determine any interest under subsection (8), the court may refer to the evidence and proceedings at the trial or hear such further evidence, either orally or by affidavit, as it may deem fit.

[Section 70 substituted by section 26 of the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)]

71. Jurisdiction of courts

- (1) A regional court has penal jurisdiction to impose any penalty mentioned in section 68(1), even though that penalty may exceed the penal jurisdiction of that court.
- (2) A magistrate's court has penal jurisdiction to impose any penalty mentioned in section 68(2), even though that penalty may exceed the penal jurisdiction of that court.
- (3) A magistrate's court or regional court has jurisdiction to make any order of forfeiture referred to in section 70, even though the amount forfeitable under that order may exceed the civil jurisdiction of a magistrate's court or regional court.

Chapter 5 : Miscellaneous

72. Act not to limit powers of investigating authorities or supervisory bodies
73. Amendment of list of accountable institutions
74. Exemptions for accountable institutions
75. Amendment of list of supervisory bodies
76. Amendment of list of reporting institutions
77. Regulations
- 77A. Arrangements for consultations with stakeholders
78. Indemnity
79. Amendment of laws
- 79A. Amendment of list of domestic prominent influential persons
- 79B. Amendment of list of foreign prominent public officials
80. Status of footnotes
81. Transitional arrangements
82. Short title and commencement

72. Act not to limit powers of investigating authorities or supervisory bodies

This Act does not detract from—

- (a) an investigating authority's powers in terms of other legislation to obtain information for the purpose of criminal investigations; or
- (b) a supervisory body's duties or powers in relation to the entities supervised or regulated by it.

73. Amendment of list of accountable institutions

- (1) The Minister may, by notice in the *Gazette*, amend the list of accountable institutions in Schedule 1 to—
 - (a) add to the list any person or category of persons if the Minister reasonably believes that that person or category of persons is used, or is likely to be used in future, for money laundering purposes;
 - (b) delete any institution or category of institutions from the list if the Minister reasonably believes that that institution or category of institutions is not being used, and is not likely to be used in the future, for money laundering purposes; or
 - (c) make technical changes to the list.
- (2) Before the Minister amends Schedule 1 in terms of subsection (1)(a) or (b), the Minister must consult the Centre, and—
[Words preceding subsection (2)(a) substituted by section 52 of the Financial Intelligence Amendment Act, 2017 (Act No. 1 of 2017)]
 - (a) if only one person or institution will be affected by the proposed amendment, give that person or institution at least 30 days' written notice to submit written representations to the Minister; or
 - (b) if a category of persons or institutions will be affected by the proposed amendment, by notice in the *Gazette* give persons or institutions belonging to that category at least 60 days' written notice to submit written representations to the Minister.
- (3) Any addition to or deletion from the list of accountable institutions in Schedule 1 in terms of subsection (1)(a) or (b) must, before publication in the *Gazette*, be approved by parliament.

74. Exemptions for accountable institutions

- (1) The Minister may, after consulting the Centre, and on conditions and for a period determined by the Minister, exempt from compliance with—
 - (a) any of the provisions of this Act—
 - (i) a person;
 - (ii) an accountable institution; or
 - (iii) a category of persons or accountable institutions;
-

-
- (b) any or all of the provisions of this Act, a person or category of persons or an accountable institution or category of accountable institutions in respect of any one or more categories of transactions.
 - (2) Any exemption referred to in subsection (1)—
 - (a) must be by notice in the *Gazette* and may be withdrawn or amended by the Minister, after consulting the Centre; and
 - (b) must be tabled in Parliament before being published in the *Gazette*.
 - (3) Before the Minister issues, withdraws or amends an exemption referred to in subsection (1), the Minister must—
 - (a) in the *Gazette*, give notice where a draft of the exemption or withdrawal notice of an exemption will be available and invite submissions; and
 - (b) consider submissions received.

[Section 74 substituted by section 54 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

75. Amendment of list of supervisory bodies

- (1) The Minister may, by notice in the *Gazette*, amend the list of supervisory bodies in Schedule 2 to—
 - (a) add to the list any entity or functionary which performs supervisory or regulatory functions in relation to any category of accountable institutions;
 - (b) delete any supervisory body from the list if that supervisory body no longer performs supervisory or regulatory functions in relation to any category of accountable institutions; or
 - (c) make technical changes to the list.
- (2) Before the Minister amends Schedule 2 in terms of subsection (1)(a) or (b), the Minister must consult the Council and the Centre, and give the entity or functionary concerned, or the supervisory body concerned, as the case may be, at least 60 days' written notice to submit written representations to the Minister.
- (3) Any addition to or deletion from the list of supervisory bodies in Schedule 2 in terms of subsection (1)(a) or (b) must, before publication in the *Gazette*, be approved by Parliament.

76. Amendment of list of reporting institutions

- (1) The Minister may, by notice in the *Gazette*, amend the list of reporting institutions in Schedule 3 to—
 - (a) add to the list any person or category of persons if the Minister reasonably believes that the person or category of persons is used, or is likely to be used in future, for money laundering purposes but it is not appropriate to impose on such person or category of persons the duties which apply to an
-

-
- accountable institution under this Act;
 - (b) delete any person or category of persons from the list if—
 - (i) the Minister reasonably believes that the person or category of persons is not being used, and is not likely to be used in the future, for money laundering purposes; or
 - (ii) the person or category of persons is to be added to the list of accountable institutions; or
 - (c) make technical changes to the list.
- (2) Before the Minister amends Schedule 3 in terms of subsection (1)(a) or (b), the Minister must consult the Centre, and—
- [Words preceding subsection (2) substituted by section 55 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
- (a) if only one person will be affected by the proposed amendment, give the person at least 30 days' written notice to submit written representations to the Minister; or
 - (b) if a category of persons will be affected by the proposed amendment, by notice in the *Gazette* give persons belonging to that category at least 60 days' written notice to submit written representations to the Minister.
- (3) Any addition to or deletion from the list of reporting institutions in Schedule 3 in terms of subsection (1)(a) or (b) must, before publication in the *Gazette*, be approved by Parliament.

77. Regulations

- (1) The Minister, after consulting the Centre, may make, repeal and amend regulations concerning—
 - (a) any matter that may be prescribed in terms of this Act; and
 - (b) any ancillary or incidental administrative or procedural matter which is necessary to prescribe for the proper implementation or administration of this Act.
 - (2) Regulations in terms of subsection (1) may—
 - (a) differ for different accountable institutions, reporting institutions, persons, categories of accountable institutions, reporting institutions and persons and different categories of transactions;
 - (b) be limited to a particular accountable institution or reporting institution or person or category of accountable institutions or reporting institutions or persons or a particular category of transactions; and
 - (c) for a contravention of or failure to comply with any specific regulation, prescribe imprisonment for a period not exceeding three years or a fine not exceeding R1 000 000 or such administrative sanction as may apply
 - (3) ***[Subsection (3) deleted by section 56 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***
 - (4) The Minister must table regulations, repeals and amendments made under subsection (1) in Parliament before publication in the *Gazette*.
-

- (5) Before making, repealing or amending regulations in terms of subsection (1), the Minister must—
- (a) in the *Gazette*, give notice where a draft of the regulations will be available and invite submissions; and
 - (b) consider submissions received.
- [Subsection (5) inserted by section 56 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]***

[Section 77 substituted by section 56 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

77A. Arrangements for consultations with stakeholders

The Centre must, after consulting with supervisory bodies, establish and give effect to arrangements to facilitate consultation with, and the exchange of information with, relevant stakeholders on matters of mutual interest.

[Section 77A inserted by section 57 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

78. Indemnity

The Minister, the Centre or an employee or representative of the Centre, or any other person performing a function or exercising a power in terms of this Act, is not liable for anything done in good faith in terms of or in furthering the objectives of this Act.

79. Amendment of laws

The Acts mentioned in Schedule 4 are hereby amended to the extent set out in Schedule 4.

79A. Amendment of list of domestic prominent influential persons

- (1) The Minister may, by notice in the *Gazette*, amend the list of domestic prominent influential persons in Schedule 3A to—
- (a) add to the list any person or category of persons;
 - (b) delete any person or category of persons mentioned in paragraph (a)(x) in the list; or
 - (c) make technical changes to the list.

-
- (2) Before the Minister amends Schedule 3A in terms of subsection (1), the Minister must —
 - (a) in the *Gazette*, give notice where a draft of the amendments will be available and invite submissions; and
 - (b) consider submissions received.
 - (3) Any addition to or deletion from the list of persons in Schedule 3A in terms of subsection (1) must, before publication in the *Gazette*, be submitted to Parliament for its approval.

[Section 79A inserted by section 58 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

79B. Amendment of list of foreign prominent public officials

- (1) The Minister may, by notice in the *Gazette*, amend the list of foreign prominent public officials in Schedule 3B to—
 - (a) add to the list any person or category of persons;
 - (b) delete any person or category of persons from the list; or
 - (c) make technical changes to the list.
- (2) Before the Minister amends Schedule 3B in terms of subsection (1), the Minister must —
 - (a) in the *Gazette*, give notice where a draft of the amendments will be available and invite submissions; and
 - (b) consider submissions received.
- (3) Any addition to or deletion from the list of persons in Schedule 3B in terms of subsection (1) must, before publication in the *Gazette*, be submitted to Parliament for its approval.

[Section 79B inserted by section 58 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

80. Status of footnotes

The footnotes in this Act have been inserted only for ease of reference to relevant provisions of the Prevention Act. They are not part of this Act. They do not have the force of law.

81. Transitional arrangements

- (1) Until the date referred to in section 82(2), the person designated for the purposes of section 7 of the Prevention Act will be deemed to have been duly designated and will
-

continue to hold office as if this Act had not been passed.

- (2) All proceedings in relation to an offence in terms of section 7(7) of the Prevention Act that were instituted before the date on which section 79 of this Act takes effect and that are pending before any court of law or reviewing authority on that date, must be dealt with as if this Act had not been passed.
- (3) An investigation or prosecution or other legal proceeding in respect of conduct which would have constituted an offence under section 7(7) of the Prevention Act and which occurred after the commencement of that Act but before section 79 of this Act takes effect, may be instituted and continued as if this Act had not been passed.

82. Short title and commencement

- (1) This Act is called the Financial Intelligence Centre Act, 2001, and takes effect on a date fixed by the President by proclamation in the *Gazette*.
- (2) Despite subsection (1)—
 - (a) section 79 does not take effect before the date on which section 29 takes effect; and
 - (b) section 21(2) takes effect one year after section 21(1) takes effect.

Schedules

Schedule 1 : List of Accountable Institutions

Schedule 2 : List of Supervisory Bodies

Schedule 3 : List of Reporting Institutions

Schedule 4 : Amendment of sections of prevention of Organised Crime Act, 1998 (Act 121 of 1998)

Schedule 1 : List of Accountable Institutions

- (1) A practitioner who practices as defined in section 1 of the Attorneys Act, 1979 (Act 53 of 1979).
 - (2) A board of executors or a trust company or any other person that invests, keeps in safe custody, controls or administers trust property within the meaning of the Trust Property Control Act, 1988 (Act 57 of 1988).
 - (3) An estate agent as defined in the Estate Agency Affairs Act, 1976 (Act 112 of 1976).
 - (4) An authorised user of an exchange as defined in the Securities Services Act, 2004 (Act 36 of 2004).
-

-
- (5) A manager registered in terms of the Collective Investment Schemes Control Act, 2002 (Act 45 of 2002), but excludes managers who only conduct business in Part VI of the Collective Investment Schemes Control Act (Act 45 of 2002).
 - (6) A person who carries on the "business of a bank" as defined in the Banks Act, 1990 (Act 94 of 1990).
 - (7) A mutual bank as defined in the Mutual Banks Act, 1993 (Act 124 of 1993).
 - (8) A person who carries on a "long-term insurance business" as defined in the Long-Term Insurance Act, 1998 (Act 52 of 1998).
 - (9) A person who carries on a business in respect of which a gambling licence is required to be issued by a provincial licensing authority.
 - (10) A person who carries on the business of dealing in foreign exchange.
 - (11) A person who carries on the business of lending money against the security of securities.
 - (12) 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 (Act 37 of 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 (Act 53 of 1998) and a health service benefit provided by a medical scheme as defined in section 1(1) of the Medical Schemes Act, 1998 (Act 131 of 1998).
 - (13) A person who issues, sells or redeems travelers' cheques, money orders or similar instruments.
 - (14) The Postbank referred to in section 51 of the Postal Services Act, 1998 (Act 124 of 1998).
 - (15) ***[Subsection (15) deleted by amendment Notice No. 1104 dated 26 November 2010]***
 - (16) The Ithala Development Finance Corporation Limited.
 - (17) ***[Subsection (17) deleted by amendment Notice No. 1104 dated 26 November 2010]***
 - (18) ***[Subsection (18) deleted by amendment Notice No. 1104 dated 26 November 2010]***
 - (19) A person who carries on the business of a money remitter.

Schedule 2 : List of Supervisory Bodies

- (1) The Financial Services Board established by the Financial Services Board Act, 1990 (Act 97 of 1990).
-

- (2) The South African Reserve Bank in respect of the powers and duties contemplated in section 10(1)(c) in the South African Reserve Bank Act, 1089, (Act No. 90 of 1989) and the Registrar as defined in sections 3 and 4 of the Banks Act, 1990, (Act 94 of 1990) and the Financial Surveillance Department in terms of Regulation 22.E of the Exchange Control Regulations, 1961.
- (3) ***[Deleted by Amendment Notice No. 1105 dated 26 November 2010]***
- (4) The Estate Agency Affairs Board established in terms of the Estate Agency Affairs Act, 1976 (Act 112 of 1976).
- (5) The Independent Regulatory Board for Auditors established in terms of the Auditing Professions Act, 2005 (Act 26 of 2005).
- (6) The National Gambling Board established in terms of the National Gambling Act, and retained in terms of the National Gambling Act, 2004 (Act 7 of 2004).
- (7) ***[Deleted by Amendment Notice No. 1105 dated 26 November 2010]***
- (8) A law society as contemplated in section 56 of the Attorneys Act, 1979 (Act 53 of 1979).
- (9) A provincial licensing authority as defined in section 1 of the National Gambling Act, 2004 (Act 7 of 2004).

Schedule 3 : List of Reporting Institutions

- (1) A person who carries on the business of dealing in motor vehicles.
- (2) A person who carries on the business of dealing in Kruger rands.

Schedule 3A : Domestic Prominent Influential Person

A domestic prominent influential person is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the Republic—

- (a) a prominent public function including that of—
 - (i) the President or Deputy President;
 - (ii) a government minister or deputy minister;
 - (iii) the Premier of a province;
 - (iv) a member of the Executive Council of a province;
 - (v) an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998);
 - (vi) a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996);
 - (vii) a member of a royal family or senior traditional leader as defined in the

-
- Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003);
- (viii) the head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);
 - (ix) the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), or a chief financial officer designated in terms of section 80(2) of the Municipal Finance Management Act, 2003 (Act No. 56 of 2003);
 - (x) the chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999);
 - (xi) the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000);
 - (xii) a constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001);
 - (xiii) an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; or
 - (xiv) an officer of the South African National Defence Force above the rank of major-general;
- (b) the position of—
- (i) chairperson of the board of directors;
 - (ii) chairperson of the audit committee;
 - (iii) executive officer; or
 - (iv) chief financial officer,
- of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the *Gazette*; or
- (c) the position of head, or other executive directly accountable to that head, of an international organisation based in the Republic.

[Schedule 3A inserted by section 59 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Schedule 3B : Foreign Prominent Public Official

A foreign prominent public official is an individual who holds, or has held at any time in the preceding 12 months, in any foreign country a prominent public function including that of a—

- (a) Head of State or head of a country or government;
 - (b) member of a foreign royal family;
 - (c) government minister or equivalent senior politician or leader of a political party;
 - (d) senior judicial official;
 - (e) senior executive of a state owned corporation; or
 - (f) high-ranking member of the military.
-

[Schedule 3B inserted by section 59 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)]

Schedule 4 : Amendment of sections of Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998)

- (1) The repeal of section 7.
- (2) The substitution for section 7A of the following section:

7A. Defence

- (1) If a person is charged with committing an offence under section 2(1)(a) or (b), 4, 5 or 6, that person may raise as a defence the fact that he or she had reported a knowledge or suspicion in terms of section 29 of the Financial Intelligence Centre Act, 2001.
- (2) If a person who is an employee of an accountable institution as defined in the Financial Intelligence Centre Act, 2001, is charged with committing an offence under section 2(1)(a) or (b), 4, 5 or 6, that person may also raise as a defence that fact that he or she had—
 - (a) complied with the applicable obligations in terms of the internal rules relating to the reporting of information of the accountable institution; or
 - (b) reported the matter to the person charged with the responsibility of ensuring compliance by the accountable institution with its duties under that Act; or
 - (c) reported a suspicion to his or her superior, if any, if—
 - (i) the accountable institution had not appointed such a person or established such rules;
 - (ii) the accountable institution had not complied with its obligations in section 42(3) of that Act in respect of that person; or
 - (iii) those rules were not applicable to that person.
- (3) The amendment of section 8 by the deletion of subsection (2).
- (4) The amendment of section 77—
 - (4.1) by the deletion from subsection (1) of paragraph (b); and
 - (4.2) by the deletion from subsection (1) of paragraph (c).

Amendment of Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)

The amendment of Part 1 of the Schedule by the addition of the following item:
 "Act 38 of 2001 Financial Intelligence Centre Act Section 36"



Commencements

www.acts.co.za

Commencements

Commencement of Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017) :
Notice No. 563 of 2017

Commencement of Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)

Notice No. 563 of 2017

Notice No. 563 of 2017

Notice No. 563
13 June 2017

National Treasury

In terms of section 61 of the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017) (herein Called "the Act"), I, Malusi KN Gigaba, Minister of finance, determine that—

- (a) the provisions of the Act specified in the following table take effect on the date of publication of this notice in the *Gazette*:

Section 1(a), (b), (c), (f), (h), (i) in respect of the definition of " Independent Police Investigative Directorate ", (j), (k) in respect of the definition of " investigative division in an organ of state ", (l), (m), (o) and (r)
Section 2(b)
Section 3(a) and (b)
Sections 4 and 5
Section 18
Section 21(a) and (c)
Section 23
Section 25
Section 26
Section 28 insofar as it inserts section 42B of the Financial Intelligence Centre Act, 2001
Sections 30 to 34
Sections 40 to 41
Sections 44 and 45

Section 46 insofar as it substitutes section 61A of the Financial Intelligence Centre Act, 2001

Section 49

Section 50 insofar as it deletes the reference to section 61A in section 68(2) of the Financial Intelligence Centre Act, 2001

Sections 52 to 57

Section 60

[Paragraph (a) amended by paragraphs (a), (b) and (c) of Notice No. 601 of 2017]

- (b) the provisions of the Act specified in the following table take effect on 2 October 2017:

Section 1(d), (e), (g), (i) in respect of the definition of " foreign prominent public official ", (k) in respect of the definition of " legal person ", (n), (p), (q), (s) and (t)

Sections 7 to 16

Section 19

Section 22

Section 27

Section 28 insofar as it inserts section 42A in the Financial Intelligence Centre Act, 2001

Section 29

Sections 35 to 38

Section 46 insofar as it substitutes section 61 of the Financial Intelligence Centre Act, 2001
--

Sections 47 and 48

Section 50 insofar as it deletes the references to sections 61 and 62 in section 68(2) of the Financial Intelligence Centre Act, 2001

Section 51

Sections 58 and 59

[Paragraph (b) amended by paragraphs (d) and (e) of Notice No. 601 of 2017]

Malusi K N Gigaba
Minister of Finance



Notices

www.acts.co.za

Notices

Guidance Note 2 - Guidance to Financial Services Industries regulated by the Financial Services Board concerning the meaning of the word "Transaction" : Notice No. 735 of 2004

Second Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001 : Notice No. R. 1354 of 2004

Guidance Note 3 - Guidance for Banks on Customer Identification and Verification and Related Matters : Notice No. 715 of 2005

Third Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001 : Notice No. 1035 of 2006

Guidance Note 4 on Suspicious Transaction Reporting : Notice No. 301 of 2008

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) : Notice No. R. 454 of 2010

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) : Notice No. 471 of 2010

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) : Notice No. 560 of 2010

Guidance Note 2

Guidance to Financial Services Industries regulated by the Financial Services Board concerning the meaning of the word "Transaction" : Notice No. 735 of 2004

Guidance to Financial Services Industries regulated by the Financial Services Board concerning the meaning of the word "Transaction"

Notice No. 735 of 2004

1. Introduction
2. Meaning of "transaction" in relation to client identification duties
3. Examples of transactions

Notice No. 735 of 2004

Notice No. 735
18 June 2004

The Financial Intelligence Centre has, in terms of its statutory function under section 4(c) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued the guidance note in the Schedule.

M Michell

Acting Director: Financial Intelligence Centre

Date: 11/06/2004

1. Introduction

Guidance Note 2

Money Laundering is criminalised in section 4 of the Prevention of Organised Crime Act, 1998. The money laundering offence can be described as the performing of any act which may result in concealing the nature of the proceeds of crime or of enabling a person to avoid prosecution or in the diminishing of such proceeds.

Apart from criminalising the activities constituting money laundering, South African law also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, as contained in the Act, are based on three basic principles of money laundering detection and investigation i.e. that:

- intermediaries to the financial system must know with whom they are doing business,
- the paper trail of transactions through the financial system must be preserved, and
- possible money laundering transactions must be brought to the attention of investigating authorities.

The control measures introduced by the Act include requirements for institutions to establish and verify the identities of their clients, to keep certain records, to report certain information and to implement measures that will assist them in complying with the Act.

The majority of obligations under the Act apply to "accountable institutions". These are institutions which fall within any one of the categories of institutions listed in Schedule 1 to the Act. This Guidance Note is aimed at those accountable institutions that are referred to in items 4, 5, 8, 11, 12, 15, 17 and 18 of Schedule 1 to the Act.

The Act also established the Financial Intelligence Centre as the agency responsible for the collection, analysis and disclosure of information to assist in the detection, prevention and deterrence of money laundering in South Africa. The Act empowers the Centre to provide guidance in relation to a number of matters.

This Guidance Note provides general guidelines which the relevant accountable institutions may apply in order to interpret the term "transaction" in relation to each institution's obligations to identify and verify the identities of its clients. It is not the purpose of this

Guidance Note to provide a complete definition of the term which could be applied rigidly across all sectors of the financial services industry. This Guidance Note is not legal advice and is not intended to replace the Act and Money Laundering Control Regulations ("the Regulations") issued under the Act in December 2002.

2. Meaning of "transaction" in relation to client identification duties

Accountable institutions are prevented by section 21 of the Act from concluding certain transactions unless they have established and verified the identities of their clients.

The term "transaction" is defined in the Act as follows:

"transaction" means a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution;"

While this definition does not attribute a particular meaning to the term "transaction", it conveys the concept that the term may have different meanings depending on the type of business, undertaken by different accountable institutions and would be applied differently among them. In short, the term must be applied in each instance in accordance with the nature of the business carried on by the accountable institution in question.

This definition also indicates that the term refers to activities which take place between an accountable institution and a client.

The dictionary meaning of the term "transaction", as taken from the Concise Oxford Dictionary, includes "management of business" and "piece of especially commercial business done". Applying this definition, a transaction can therefore generally be described as an instance of commercial activity between two or more parties.

Transactions are concluded on the basis of agreements between the parties to a transaction. Following the definition of the term "transaction" in the Act, as well as the dictionary meaning of the term, these agreements must be aimed at a piece of business done between an accountable institution and a client, in accordance with the nature of the business carried on by the institution concerned. A basic guideline, which can be inferred from this, is that any instruction or request by a client to an accountable institution to perform some act to give effect to the business relationship between them can be regarded as a transaction.

3. Examples of transactions

For the purpose of the obligation to establish and verify clients' identities as referred to in this guidance note, the term "transaction" is not understood to include activities which happen automatically, or which an intermediary will perform automatically, without instructions from the client. These consequences include, for example, periodic contractual payments by clients to institutions and periodic automatic increases in such payments, as well as further business that accountable institutions may do with others in the course of giving effect to the clients' original mandate.

Examples of what might be regarded as "transactions" for the purposes of client identification in respect of the accountable institutions supervised by the Financial Services Board follow below. This is not an exhaustive list of "transactions" performed by the relevant accountable institutions, but is intended to provide an indication of the types of activities which might be regarded as transactions.

- a) Collective investment Schemes
 - The giving of a mandate to invest in any collective investment scheme;
 - Any amendment in the original investment mandate of the client;
 - An instruction to transfer or switch the investment to another collective investment scheme;
 - The offering of participating interests for repurchase;
 - The repayment of participants' interests following the closure of a fund or portfolio.
- b) Long-Term Insurance
 - The entering into a new long-term insurance policy;
 - An amendment or variation of the terms and conditions of a long-term insurance policy, including a change in the beneficiary or policyholder;
 - An instruction by the client to the long-term insurer to switch or reinvest the underlying assets of a linked policy with linked investment service providers or investment managers;
 - Termination (including the lapsing and surrender), withdrawal, or reinvestment of a long-term insurance policy.

The above activities apply both to the intermediary and service provider.

- c) Investment Managers
 - The entering into a new investment contract;
 - Additional amounts invested in terms of an investment mandate with a client;
 - An amendment or variation of the terms and conditions of an investment mandate;
 - An instruction by the client to switch or reinvest the investment to other linked investment service providers or investment managers;
 - An instruction by the client for a partial withdrawal of investment and the subsequent repayment of the investment in any form;
 - Termination or withdrawal of an investment mandate and the subsequent repayment of the investments in any form.
- d) Linked Investment Service Providers (LISP's)
 - The entering into a new investment contract;
 - Additional amounts invested in terms of an investment mandate with a client;
 - An amendment or variation of the terms and conditions of an investment mandate;
 - An instruction by the client to switch or reinvest the investment to other linked investment service providers or investment managers;
 - Termination or withdrawal of an investment mandate and the subsequent repayment of the investments in any form;

-
- An instruction by the client for a partial withdrawal of investment and the subsequent repayment of the investment in any form.
- e) Brokers trading securities (including derivatives) on the JSE Securities Exchange
- A trading instruction by a client to buy or sell securities or derivatives;
 - An amendment or variation of a trading instruction from a client;
 - The receipt from, or payment of money (including a dividend) to, a client in giving effect to a mandate.
- f) Brokers trading financial instruments on the Bond Exchange of South Africa
- A trading instruction from a client to buy or sell a financial instrument;
 - An amendment or variation of a trading instruction from a client;
 - The receipt from or payment of money (including a coupon payment) to, a client in giving effect to a mandate.

Second Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001

Notice No. R. 1354 of 2004

Notice No. R. 1354 of 2004

Notice No. R. 1354
19 November 2004

By virtue of the powers vested in me by section 74 of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001, "the Act"), I, Trevor Andrew Manuel, Minister of Finance, hereby make the exemption set out in the Schedule hereto, with immediate effect.

Dated at Pretoria this 1st day of November 2004.

T A Manuel, MP
Minister of Finance

Every person who carries on a business or is in charge of or manages a business or who is employed by a business and in that capacity assists or advises a client in connection with funds, or receives funds, in respect of which an application for amnesty in terms of the Exchange Control Amnesty and Amendment of Taxation Laws Act, 2003 (Act No. 12 of 2003) is yet to be approved, is exempt from compliance with the provisions of section 29 of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001, "the Act"), in respect of making a report under that section of the Act concerning such funds disclosed in such application for amnesty, and involved in a transaction which such a person would have reported for no other reason than that the transaction concerns such funds, had it not been for this

exemption.

EXPLANATORY MEMORANDUM ON THE SECOND REPORTING EXEMPTION IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001: THE USE OF FUNDS DISCLOSED IN AN AMNESTY APPLICATION PRIOR TO A DETERMINATION OF THE AMNESTY APPLICATION

01. The exemption from the obligations of section 29 of the Act is aimed at facilitating the role of financial institutions, financial advisors and intermediaries in further assisting persons, who have applied for amnesty under the Exchange Control Amnesty and Amendment of Taxation Laws Act, 2003 (Amnesty Act), while the determination of the amnesty application is pending.
 02. The exemption will apply to financial institutions, financial advisors and intermediaries, as well as any other person who carries on a business or is in charge of or manages a business or who is employed by a business, by operation of law and will not have to be applied for. The exemption is limited and applies only in respect of funds disclosed in amnesty applications under the Amnesty Act (amnesty related funds).
 03. The exemption will exempt persons to whom it applies from the duty under section 29 of the Financial Intelligence Centre Act, 2001 (the FIC Act) to report suspicious and unusual transactions to the Financial Intelligence Centre specifically in respect of the reinvestment or other usage of funds which are the subject of a pending amnesty application under the Amnesty Act.
 04. The proposed exemption cannot absolve any person from liability for their own involvement in contraventions of the Exchange Control Regulations or Tax Evasion or any other criminal activity associated therewith, since that liability does not arise from the provisions of the FIC Act.
 05. The full force of the law also remains applicable to any undisclosed funds that should have been disclosed under the amnesty process. Accordingly, where an applicant sought and received amnesty advice, but failed to file an amnesty application, or where an applicant did not seek amnesty advice and did not file an amnesty application, financial advisors and intermediaries must report any proposed transactions concerning such funds to the Centre under section 29 of the FIC Act.
 06. In all other matters unrelated to the amnesty, the financial institution, financial advisor or intermediary concerned remains obliged to file reports concerning financial transactions of a suspicious or unusual nature with the Centre under section 29 of the FIC Act.
 07. In conclusion, financial institutions, financial advisors and intermediaries are cautioned to ascertain at all times that funds under their control/administration are subject to a pending amnesty application before proceeding with a new transaction relating to such funds.
-

Guidance Note 3

Guidance for Banks on Customer Identification and Verification and Related Matters : Notice No. 715 of 2005

Guidance for Banks on Customer Identification and Verification and Related Matters

Notice No. 715 of 2005

Preface

Anti-Money Laundering and Terrorist Financing Policies and Procedures

Establishing and Verifying Identities

Partnerships

Trusts

Organs of State including Government Departments

International Standards and Best Banking Practice

Politically Exposed Persons (PEPs)

Correspondent Banks

Exemptions

Glossary

Notice No. 715 of 2005

Notice No. 715

18 July 2005

Financial Intelligence Centre

The Financial Intelligence Centre has, in terms of its statutory function under section 4(c) of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), issued the guidance note in the Schedule.

M Michell

Director: Financial Intelligence Centre

Date: 14/07/2005

Preface

Money laundering has been criminalised in section 4 of the Prevention of Organised Crime Act, 1998. A money laundering offence may be described as the performing of any act that may result in concealing the nature of the proceeds of crime or of enabling a person to avoid prosecution or in the diminishing of the proceeds of crime.

Apart from criminalising the activities constituting money laundering, South African law also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, as contained in the Financial Intelligence Centre Act, 2001 (the "FIC Act"), are based on three basic principles of money laundering detection and investigation, i.e. that:

- intermediaries in the financial system must know with whom they are doing business;
- the paper trail of transactions through the financial system must be preserved;
- possible money laundering transactions must be brought to the attention of the Financial Intelligence Centre and the investigating authorities.

The control measures introduced by the FIC Act include requirements for institutions to establish and verify the identities of their clients, to keep certain records, to report certain information and to implement measures that will assist them in complying with the FIC Act.

The majority of obligations under the FIC Act apply to "accountable institutions". These are institutions that fall within any one of the categories of institutions listed in Schedule 1 to the FIC Act.

The FIC Act also established the Financial Intelligence Centre ("the Centre") as the agency responsible for the collection, analysis and disclosure of information to assist in the detection, prevention and deterrence of money laundering in South Africa. In addition, section 4(c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations of the FIC Act.

Application of this Guidance Note

This Guidance Note applies to the accountable institutions that are referred to in the following items of Schedule 1 to the FIC Act:

- Item 6 (a person who carries on "the business of a bank" as defined in the Banks Act, 1990).
- Item 7 (a mutual bank as defined in the Mutual Banks Act, 1993).
- Item 14 (The Post bank referred to in section 51 of the Postal Services Act, 1998).
- Item 16 (The Ithala Development Finance Corporation Limited).

This Guidance Note is published by the Centre under section 4(c) of the FIC Act to assist these accountable institutions and the relevant supervisory bodies with the practical application of certain client identification and client verification requirements of the FIC Act. Some of the terminology used in this Guidance Note is explained in the glossary.

Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Regulations issued under the Act. Guidance emanating from industry associations or other organisations, therefore, in the Centre's view, does not have a bearing on compliance with the obligations imposed by the FIC Act or interpretation of its provisions.

The guidance provided by the Centre in this Guidance Note, although authoritative, is provided as general information only. The Guidance Note does not provide legal advice and is not intended to replace the FIC Act or the Money Laundering Control Regulations ("the Regulations") issued under the FIC Act in December 2002.

Anti-Money Laundering and Terrorist Financing Policies and Procedures

1. Board approval of a bank's anti-money laundering and terrorist financing policies
2. Implementation of Guidance Note 1 in respect of a risk-based approach
3. Risk indicators to be used to differentiate between clients
4. Client profiling procedures for high risk clients
5. Client acceptance policies

1. Board approval of a bank's anti-money laundering and terrorist financing policies

Board of directors' approval of a bank's own internal policies and procedures to address money laundering and terrorist financing is critical if a bank wishes to be seen to be fully committed to its appreciation of, and willingness to, mitigate money laundering and terrorist financing risks in its daily banking operations.

The Centre therefore expects that the internal anti-money laundering and terrorist financing policies and procedures of a bank should be adopted and approved by the board of directors of that bank.

This will also ensure that the board of a particular bank takes ownership of its obligations in terms of the FIC Act. The criminal penalties for failure to comply with the obligations under the FIC Act are severe, and directors may be held personally liable. Forbearance in prosecuting criminal matters under the FIC Act must not be expected.

2. Implementation of Guidance Note 1 in respect of a risk-based approach

Although the FIC Act and the Regulations do not expressly make reference to a risk-based approach, in respect of identification and verification of client particulars, this issue is covered in Guidance Note 1 issued by the Centre in April 2004, and distributed by the Registrar of Banks in terms of Banks Act Circular 4/2004.

Guidance Note 1 indicates that application of a risk-based approach to the verification of the relevant particulars implies that a bank can accurately assess the risk involved. It also implies that a bank can take an informed decision on the basis of its risk assessment as to the appropriate methods and levels of verification that should be applied in a given circumstance.

Guidance Note 1 further states that the assessment of these risk factors should best be done by means of a systematic approach to determine different risk classes and to identify criteria to characterize clients and products. In order to achieve this, a bank would need to document and make use of a risk framework. Such a risk framework should preferably form part of the bank's internal policies and procedures to address money laundering and terrorist financing referred to in paragraph 1, above.

3. Risk indicators to be used to differentiate between clients

Risk Indicators

The FIC Act and the Regulations require that banks identify all clients with whom they do business unless an exemption applies in a given circumstance. Banks, however, are not required to follow a "one size fits all" approach in the methods that they use and the levels of verification that they apply to all relevant clients.

It is imperative that the money laundering risk in any given circumstance be determined on a holistic basis. In other words, the ultimate risk rating accorded to a particular business relationship or transaction must be a function of all factors that may be relevant to the combination of a particular client profile, product type and transaction.

A combination of the following factors may be applied to differentiate between high risk, medium risk and low risk clients:

- product type;
- business activity;
- client attributes, for example, whether the client is on the United Nations list, duration of client relationship with bank, etc;
- source of funds;
- jurisdiction of client;
- transaction value;
- type of entity.

Please refer to Guidance Note 1 for further particulars on the implementation of a risk-based approach.

4. Client profiling procedures for high risk clients

In terms of Regulation 21 of the Regulations, a bank must obtain certain additional information whenever this information may reasonably be required to identify:

- a business relationship or single transaction that poses a particularly high risk of facilitating money laundering activities; or
- the proceeds of unlawful activity or money laundering activities.

In most instances it is a combination of factors, not any one factor that will lead to a conclusion that a transaction or relationship poses a money laundering risk. All circumstances surrounding a business relationship or transaction should be reviewed.

The risk factors referred to in paragraph 3, above, may be helpful to banks in assessing when additional information may be required in order to enhance the institution's profile of a particular client. In addition there are a number of further factors that may indicate that a business relationship or single transaction poses a high risk of facilitating money laundering activities, or the presence of the proceeds of unlawful activity such as the following:

- a client appears to have accounts with several banks in one geographical area;
 - a client makes cash deposits to a general account of a foreign correspondent bank;
 - a client wishes to have credit and debit cards sent to destinations other than his or her
-

-
- address;
- a client has numerous accounts and makes or receives cash deposits in each of them amounting to a large aggregated amount;
 - a client frequently exchanges currencies;
 - a client wishes to have unusual access to safe deposit facilities;
 - a client's accounts show virtually no normal business related activities, but are used to receive or disburse large sums;
 - a client has accounts that have a large volume of deposits in bank cheques, postal orders or electronic funds transfers;
 - a client is reluctant to provide complete information regarding the client's activities;
 - a client's financial statements differ noticeably from those of similar businesses;
 - a business client's representatives avoid contact with the branch;
 - a client's deposits to, or withdrawals from, a corporate account are primarily in cash, rather than in the form of debit and credit normally associated with commercial operations;
 - a client maintains a number of trustee accounts or client subaccounts;
 - a client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere;
 - a client makes a large volume of cash deposits from a business that is not normally cash intensive;
 - a small business in one location makes deposits on the same day at different branches;
 - there is a remarkable transaction volume and a significant change in a client's account balance;
 - a client's accounts show substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services;
 - a client's accounts show a sudden and inconsistent change in transactions or patterns.

The circumstances referred to above may be legitimate features of certain categories of businesses, or may make business sense if viewed in the context of the client's business activities. However, it is equally possible that these features would be unexpected in relation to certain categories of businesses, or would have no apparent business purpose, given a particular client's business activities. The purpose of obtaining additional information concerning certain clients in these circumstances is to assist the bank to more accurately identify truly suspicious behavior or relationships and transactions that pose a risk of money laundering, on the basis of a broader profile of the client than the mere client identification particulars.

The information that a bank must obtain in the circumstances referred to above must be adequate to reasonably enable the bank to determine whether transactions involving a client are consistent with the bank's knowledge of that client and that client's business activities and must include particulars concerning:

- the source of that client's income; and
 - the source of the funds that the particular client expects to use in concluding the single transaction or transactions in the course of the business relationship.
-

5. Client acceptance policies

In terms of the Core Principles, banks should develop clear customer acceptance policies and procedures, including a description of the type of customer that is likely to pose a higher than average risk to a bank. In preparing such policies, banks should take into account all risk indicators, including factors such as the customer's:

- background;
- country of origin;
- public or high profile position;
- linked accounts and;
- business activities.

Banks should develop graduated customer acceptance policies and procedures that require extensive due diligence for higher risk clients. These policies and procedures should form part of a bank's risk framework, referred to in paragraph 2 above.

Establishing and Verifying Identities

Natural Persons - South African Citizens and Residents

Natural Persons - Foreign Nationals

Legal Entities

Natural Persons - South African Citizens and Residents

6. Clarification of an official identity document
7. Clarification of whether the address slip found in identity documents
8. Alternate means of verification if identity document has been lost or stolen
9. Acceptable KYC procedures for non face-to-face verification
10. Status of "faxed copies"
11. Examples of acceptable documentation to verify residential address of natural per
12. Acceptable documents for third party verification
13. Legal incapacity
14. Ongoing client detail maintenance

6. Clarification of an official identity document

The Regulations define "identification document" in respect of a natural person who is a citizen of, or resident in, the Republic of South Africa, as an official identity document. The Department of Home Affairs describes an official identity document as a green bar-coded identity document. Therefore, old identity documents may not be construed as official identity documents.

Regulation 4 of the Regulations, however, provides for exceptional cases in which a person is

unable to produce an official identity document. In such instances, the bank must be satisfied that the client has an acceptable reason for being unable to produce an official identity document. This reason should be noted in the records of the bank. The note should also reflect the details of the staff member who recorded the information. The bank may then accept an alternative valid, meaning current and unexpired, document, which contains the person's:

- photograph;
- full names or initials and surname;
- date of birth; and
- identity number,

The following are examples of documents that may be accepted in such exceptional circumstances as an alternative form of verification:

- valid South African driver's licence; or
- valid South African passport.

Decisions concerning the reasons for being unable to produce an official identity document, which may be accepted by a bank, and the documents that may be regarded as acceptable alternatives, should be based on a bank's risk framework referred to in paragraph 2 above.

7. Clarification of whether the address slip found in identity documents

Regulation 4(3) of the Regulations requires that a bank use "information which can reasonably be expected to achieve" verification of an address. It is the view of the Centre that the address slips issued by the Department of Home Affairs do not constitute information that can reasonably be expected to achieve verification of a person's current address. The Centre does not regard these address slips as independent source documents. In addition, the information contained in an address slip may be outdated and, therefore, may not reflect current information.

8. Alternate means of verification if identity document has been lost or stolen

This issue is addressed under paragraph 6 above.

9. Acceptable KYC procedures for non face-to-face verification

Regulation 4 of the Regulations concerning the verification of a person's identity is based on a view that the customer is met face-to-face when his or her particulars are obtained.

Regulation 18 of the Regulations provides for instances in which client information is obtained in a non face-to-face situation. In such cases, banks "must take reasonable steps" to confirm the existence of the client and to verify the identity of the natural person involved.

Additional guidance may be taken from the Core Principles. These indicate that banks should

apply equally effective customer identification procedures and ongoing monitoring standards for non face-to-face customers. In accepting business from non face-to-face customers:

- banks should apply customer identification procedures to non face-to-face customers that are as effective as those that were applied to customers who were available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

According to the Core Principles, examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those that are required for face-to-face customers;
- independent contact with customer by the bank;
- third party introduction.

Decisions concerning the additional steps to be taken in cases of a non face-to-face situation should be based on a bank's risk framework, referred to in paragraph 2 above.

10. Status of "faxed copies"

Faxed copies of documents may be relevant in instances when client information is obtained in a non face-to-face situation. In such cases, the principles discussed in paragraph 9 above would apply. This implies that documents that are certified as true copies of originals may be accepted, but a bank would have to take additional steps to confirm that the said documents are in fact those of the client in question.

In cases when client information is received in a face-to-face situation, the relevant documents will be sighted as part of the verification process. If copies of those documents are not made at that stage for record keeping purposes, they may be faxed to the bank in question shortly thereafter. The bank should then record that the originals or certified copies of the documents, as the case may be, were sighted as part of the verification process.

11. Examples of acceptable documentation to verify residential address of natural per

Regulation 4(3) of the Regulations sets out instances in which the residential address of a natural person needs to be verified. The most secure form of verification of a residential address would be achieved if a staff member and/or agent of the bank were to visit the residential address of such a natural person to confirm that the person resides at the particular residential address.

In most instances, however, it would be sufficient to review the original document and to obtain a copy of a document that offers a reasonable confirmation of the information in question. Since the documentation must be current, a good practice would be to require documentation that is less than three months old.

Below are examples of documents that may, depending on the circumstances, offer confirmation of a residential address. This list is not exhaustive, and other forms of documentation may be used in the verification process. Decisions as to how residential addresses are to be verified should be based on a bank's risk framework, referred to in paragraph 2 above.

Documents that may offer confirmation of residential address include the following:

- a utility bill reflecting the name and residential address of the person;
- a bank statement from another bank reflecting the name and residential address of the person if the person previously transacted with a bank registered in terms of the Banks Act and that bank had confirmed the person's particulars;
- a recent lease or rental agreement reflecting the name and residential address of the person;
- municipal rates and taxes invoice reflecting the name and residential address of the person;
- mortgage statement from another institution reflecting the name and residential address of the person;
- telephone or cellular account reflecting the name and residential address of the person;
- valid television licence reflecting the name and residential address of the person;
- recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the person; or
- recent motor vehicle license documentation reflecting the name and residential address of the person.

When a recent utility bill from a telephone or cellular account, Eskom or a local authority does not identify the physical street address of the property owner (that is, if the bill is sent to a postal address), the utility bill will still be acceptable provided the customer's name and the erf/stand and township details are reflected on the utility bill. The customer's physical address, erf number and township should be recorded, and the township cross-referenced to the suburb in which the customer resides.

If thereafter there is any doubt about the customer or the physical address of the customer, the erf/stand and township details should be verified by reference to the Deeds Office.

If none of the above is available banks may explore other means to verify a client's address such as an affidavit containing the following particulars from a person co-habiting with the client or an employer of the client:

- name, residential address, identity number of the client and the deponent of the affidavit;
- relationship between the client and the deponent of the affidavit; and
- confirmation of the client's residential address.

12. Acceptable documents for third party verification

In terms of section 21 of the FIC Act, if a client (A) is acting on behalf of another person (B), the bank needs to establish and verify the identity of that other person (B) and the client's (A) authority to establish the business relationship or conclude the single transaction on behalf of that other person (B).

In terms of Regulation 17 of the Regulations, the bank must obtain from the person acting on behalf of another person (A) information that provides proof of that person's authority (A) to act on behalf of that other natural person, legal person or trust (B).

A bank must verify the information obtained by:

comparing the particulars of the natural or legal person, partnership or trust with information obtained by the bank from, or in respect of, the natural or legal person, partnership or trust in accordance with Regulation 4 (Verification of information concerning South African citizens and residents), Regulation 6 (Verification of information concerning foreign nationals), Regulation 8 (Verification of information concerning close corporations and South African companies), Regulation 10 (Verification of information concerning foreign companies), Regulation 12 (Verification of information concerning other legal persons), Regulation 14 (Verification of information concerning partnerships) or Regulation 16 (Verification of information concerning trusts) of the Regulations, as may be applicable; and establishing whether that information, on the face of it, provides proof of the necessary authorisation.

The following are examples of documents that may be accepted to confirm the authority of a person to act on behalf of another person and to confirm the particulars of the person authorising the third party to establish the relationship:

- power of attorney;
- mandate;
- resolution duly executed by authorised signatories; or
- a court order authorising the third party to conduct business on behalf of another person.

13. Legal incapacity

Regulation 3(2) of the Regulations provides for instances in which a natural person needs to be assisted by another person owing to his/her legal incapacity. Regulation 4 of the Regulations also applies to the verification of the particulars referred to in Regulation 3(2) of the Regulations, namely, the name, date of birth, identity number and residential address of the person assisting the person without legal capacity.

14. Ongoing client detail maintenance

Regulation 19 of the Regulations states that a bank must take reasonable steps, concerning the verification of client identities that may apply to that bank in respect of an existing business relationship so as to maintain the correctness of particulars that are susceptible to change.

Decisions concerning the method by means of which such maintenance is to be achieved should be based on a bank's risk framework, referred to in paragraph 2 above. Some guidance may be taken from international best practice and FATF standards that refer to ongoing risk-sensitive programmes to maintain relevant client details.

The following procedure for ongoing maintenance of client information may be considered:

- banks should apply their know your client (KYC) procedures to existing clients on the basis of materiality and risk, and should conduct due diligence reviews of such existing relationships at appropriate times;
- banks need to undertake regular reviews of their existing client records. An appropriate time to do so is when a transaction of significance takes place; or when there is a material change in the way the account is operated; and
- if a bank becomes aware at any time that it lacks sufficient information about an existing client, it should take steps to ensure that all relevant KYC information is obtained as quickly as possible.

Natural Persons - Foreign Nationals

15. Identification and verification

15. Identification and verification

Regulation 6(3) of the Regulations provides for instances in which a bank deems it reasonably necessary to obtain, in addition to a person's identity document (foreign passport), further information or documentation verifying the identity of such a person.

In instances when a bank requires further confirmation of the identity of a foreign national, the bank may obtain such confirmation:

- a letter of confirmation from a person in authority (for example, from the relevant embassy), which confirms authenticity of that person's identity document (passport).

Decisions concerning when further confirmation of the identity of a foreign national may be required and the nature of such information should be based on a bank's risk framework, referred to in paragraph 2 above.

Legal Entities

- 16. Identification and verification of subsidiaries of listed companies
- 17. Identification and verification of pension and provident funds
- 18. Identification and verification of "off the shelf" companies

16. Identification and verification of subsidiaries of listed companies

Exemption 6(1) of the Exemptions, applies to companies that are listed on a stock exchange mentioned in the Schedule to the Exemptions.

This Exemption does not apply to subsidiaries, whether wholly owned or not, of listed

companies.

17. Identification and verification of pension and provident funds

As a general rule, a bank has to establish and verify the identity of a pension and a provident fund. A pension and a provident fund will fall into the category of "other legal person" (Regulation 11 of the Regulations).

The bank must obtain from the natural person acting or purporting to act on behalf of the pension or provident fund:

- the name of the pension or provident fund;
- the address of the legal entity establishing the fund;
- the full names, date of birth and identity number or passport number of the trustees or any other persons appointed to act on behalf of the pension and provident fund or who purports to establish a business relationship or to enter into a transaction with the bank on behalf of the pension and provident fund; and
- the residential address of the trustees or any other persons appointed to act on behalf of the pension and provident fund or who purports to establish a business relationship or to enter into a transaction with the bank on behalf of the pension and provident fund.

18. Identification and verification of "off the shelf" companies

Banks should identify and verify the information pertaining to "off the shelf" companies in the same way they would identify and verify any other company.

Partnerships

19. The definition of a partnership

20. Clarification of partnership agreements and whether all partners in a partnership

19. The definition of a partnership

A partnership is a form of business enterprise. A partnership exists when there is a voluntary association of two or more persons engaged together for the purpose of doing lawful business as a partnership, for profit. Partnerships are assumed to exist when the partners actually share profits and losses proportionately, even though there may not be a written partnership agreement signed between the partners.

A partnership is not a legal entity and cannot conduct transactions in its own name. When a person conducts a transaction on behalf of a partnership, the transaction is conducted on behalf of all partners in that partnership jointly. All partners in a partnership are jointly and

severally liable for the partnership's liabilities.

20. Clarification of partnership agreements and whether all partners in a partnership

In terms of Regulation 13(b)(i) of the Regulations, banks are required to identify all partners within a partnership.

In most instances, the interest of a prospective client to open an account will prompt the bank to obtain the information that it needs to undertake its KYC function in terms of the FIC Act and the Regulations.

In some instances, a bank would be able (and would even be expected) to obtain information from third parties in order to establish and/or verify a prospective client's identity. The bank must have policies and procedures at the account opening stage that are designed to capture all the relevant information.

The Centre cannot prescribe to banks the form that such procedures should take, but the Centre would expect such procedures to inform a prospective client that the relationship with the bank is dependent on them providing all required information (which, in the absence of a written partnership agreement would include disclosing all partners and identifying and verifying all disclosed partners).

Where two or more persons are co-signatories on an account the Centre expects those co-signatories to sign a declaration to the bank that they do not act as a partnership.

Decisions concerning account opening policies and procedures, in respect of whether confirmation of the identities of partners should be obtained from third parties, should be based on a bank's risk framework, referred to in paragraph 2, above.

Trusts

21. Identification of trusts

22. Identification and verification of each trustee of a trust

21. Identification of trusts

The following documents are required to identify a trust in terms of Regulations 15 and 16 of the Regulations:

- trust deed or other founding document;
 - letter of authority from the Master of the High Court in South Africa or letter of authority from a competent trust registering authority in a foreign jurisdiction;
 - trustees' resolution authorising person/s to act;
 - personal details of each trustee, each beneficiary referred to by name in the trust deed or other founding document, the founder and the person/s authorised to act (refer to
-

applicable the FIC Act requirements).

22. Identification and verification of each trustee of a trust

The following Regulations provide clarity on this matter:

- Regulation 15(d)(i) of the Regulations requires that a bank must establish the identity of each trustee.
- Regulation 15(g) of the Regulations requires that the residential address and contact particulars in relation to each trustee be established.
- Regulation 16 of the Regulations further explains how the identity of a trustee, as well as the residential address, must be verified.
- There is therefore an obligation on all banks to establish and verify the identity and residential address of each trustee.

Organs of State including Government Departments

23. Identification and verification of Government departments and organs of state

23. Identification and verification of Government departments and organs of state

The FIC Act places an obligation on all banks to establish and verify the identity of their clients. A client of a bank may include a natural person, a juristic person, such as a close corporation and a company, a partnership, a trust and an organ of state including government departments.

There is an obligation on all banks to establish and verify the identity of their client even if the client is an organ of state including a government department.

Certain organs of state are incorporated as companies and registered with the Registrar of Companies to conduct business and must be identified as companies. In other instances, Government institutions are constituted as legal persons by statute. Regulations 11 and 12 provide for a category of client referred to as "other legal person", which includes organs of state constituted as legal persons by statute.

Sound business practice would indicate that organs of state that are neither incorporated as companies nor constituted as legal persons by a statute should be dealt with in a manner similar to that used in respect of "other legal persons". This would apply to national, provincial and local government departments.

This implies that, among others, the identities of the persons acting on behalf of an organ of state would have to be established and verified.

In some circumstances, this may include the Chief Financial Officer (CFO) acting on behalf of a Government department. In such instances, the full name, date of birth and identity number

in respect of individuals acting on behalf of the relevant organs of state should be obtained and verified. In addition, information concerning the contact particulars of such persons should be obtained.

International Standards and Best Banking Practice

24. Extent to which international standards

24. Extent to which international standards

In interpreting and applying the relevant legislation, international best practice should serve as a reference to clarify what is expected from the banking industry. The FATF Recommendations form the contextual basis for the implementation of the FIC Act. International standards such as the FATF Recommendations and the Core Principles provide the minimum requirements with which countries must comply.

The international standard for banking supervision is based on the Core Principles, which set out the standards that have been designed to be applied by all countries in the supervision of the banks in their jurisdictions. Similarly, all banks supervised by a banking supervisor that adopts the Core Principles are duty bound to adhere to the Principles as a matter of best banking practice.

The approach of the Basel Committee on Banking Supervision to KYC adopts a wider prudential method of review.

Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme which involves more extensive due diligence for higher risk clients and which includes proactive account monitoring for suspicious activities.

In terms of principle 15 of the Core Principles, banking supervisors must determine that:

"Banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements".

As a result it is fundamental to the market integrity and financial stability of the South African domestic banking system that international standards, as set out in the Core Principles and best banking practice, is adopted by the banking industry as an extra prudential measure when legislation does not adequately address a specific issue. Supervisory bodies should be enforcing the implementation of best practices in the industries that they supervise.

Politically Exposed Persons (PEPs)

- 25. Definition of a politically exposed person (PEP)
- 26. Treatment of PEPs in relation to other high-risk clients
- 27. Policies for dealing with PEPs

25. Definition of a politically exposed person (PEP)

A politically exposed person or PEP is the term used for an individual who is or has in the past been entrusted with prominent public functions in a particular country. The principles issued by the Wolfsberg Group of leading international financial institutions give an indication of best banking practice guidance on these issues. These principles are applicable to both domestic and international PEPs.

The following examples serve as aids in defining PEPs:

- Heads of State, Heads of Government and cabinet ministers;
- influential functionaries in nationalised industries and government administration;
- senior judges;
- senior political party functionaries;
- senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations;
- members of ruling or royal families;
- senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities).

According to the Wolfsberg principles, families and closely associated persons of PEPs should also be given special attention by a bank. The term "families" includes close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage. The category of "closely associated persons" includes close business colleagues and personal advisers/consultants to the PEP as well as persons, who obviously benefit significantly from being close to such a person.

A bank should conduct proper due diligence on both a PEP and the persons acting on his or her behalf. Similarly, KYC principles should be applied without exception to PEPs, families of PEPs and closely associated persons to the PEP.

26. Treatment of PEPs in relation to other high-risk clients

In terms of the FATF standards, specific action should be taken in relation to PEPs as a category of high-risk client. In addition to performing customer due diligence measures, banks should put in place appropriate risk management systems to determine whether a customer, a potential customer or the beneficial owner is a PEP. In addition banks:

- should obtain senior management approval for establishing business relationships with a PEP. When the client has been accepted, the bank should be required to obtain senior management approval to continue the business relationship;
-

- should take reasonable measures to establish the source of wealth and the source of funds of customers and the beneficial owners identified as PEPs;
- should conduct enhanced ongoing monitoring of a relationship with a PEP.

27. Policies for dealing with PEPs

It is crucial that banks address the issue of PEPs in their risk framework, referred to in paragraph 2, and group money laundering control policy. PEPs should be regarded as high-risk clients and, as a result, enhanced due diligence should be performed on this category of client. Heightened scrutiny has to be applied whenever PEPs or families of PEPs or closely associated persons of the PEP are the contracting parties or the beneficial owners of the assets concerned, or have power of disposal over assets by virtue of a power of attorney or signature authorisation.

The Wolfsberg principles provide additional guidance on how to recognise and deal with a PEP. In addition to the standardised KYC procedures, the following prompts are appropriate to recognise a PEP:

- the question whether clients or other persons involved in the business relationship perform a political function should form part of the standardised account opening process, especially in cases of clients from corruption prone countries;
- client advisers should deal exclusively with clients from a specific country/region to improve their knowledge and understanding of the political situation in that country/region;
- the issue of PEPs should form part of a banks regular KYC training programs;
- banks may use databases listing names of PEPs including their families, closely associated persons and advisors.

Correspondent Banks

28. Measures that need to be put in place in respect of correspondent banking relatio

28. Measures that need to be put in place in respect of correspondent banking relatio

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "responent bank"). Correspondent bank accounts enable banks to conduct business and provide services that the banks do not offer directly.

According to the Core Principles, banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

In particular, the Core Principles provide that banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (ie. shell

banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified by FATF as being "non co-operative" in the fight against anti-money laundering.

The Wolfsberg principles sets out the following risk indicators that a Bank shall consider, to ascertain what reasonable due diligence or enhanced due diligence it will undertake:

- **the correspondent banking client's domicile** - the jurisdiction where the correspondent banking client is based and/or where its ultimate parent is headquartered may present greater risk. Certain jurisdictions are internationally recognised as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Institutions will review pronouncements from regulatory agencies and international bodies, such as the **FATF**, to evaluate the degree of risk presented by the jurisdiction in which the correspondent banking client is based and/or in which its ultimate parent is headquartered.
- **the correspondent banking client's ownership and management structures** - the location of owners, their corporate legal form and the transparency of ownership structure may present greater risks. The involvement of a PEP in the management or ownership of certain correspondent banking clients may also increase the risk.
- **the correspondent banking client's business and customer base** - the type of businesses the correspondent banking client engages in, as well as the type of the markets the correspondent banking client serves, may present greater risks. Consequently, a correspondent banking client that derives a substantial part of its business income from higher risk clients may present greater risk. Higher risk clients are those clients of a correspondent banking client that may be involved in activities or are connected to jurisdictions that are identified by credible sources as activities or countries being especially susceptible to money laundering. Each institution may give the appropriate weight to each risk factor, as it deems necessary.

FATF Recommendation 7 states that financial institutions such as banks should, in addition to performing normal due diligence measures, do the following in relation to cross-border correspondent banking and other similar relationships:

- gather sufficient information about a respondent bank to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the bank and the quality of supervision, including whether the institution has been subject to a money laundering or terrorist financing investigation or regulatory action;
- assess the respondent bank's anti-money laundering and terrorist financing controls;
- obtain approval from senior management before establishing new correspondent relationships;
- document the respective responsibilities of each bank;
- with respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that the respondent bank is able to provide relevant customer identification data upon request to the correspondent bank.

Exemptions

29. Clarification of Exemption 5 - foreign clients

30. Clarification of the difference between Exemptions 5 and 16

29. Clarification of Exemption 5 - foreign clients

Exemption 5 of the Exemptions deals with countries situated in a foreign jurisdiction. According to Exemption 5 accountable institutions, including banks, are exempted from compliance with the provisions of section 21 of the FIC Act that require the verification of the identity of a client of that institution, if:

- the client is situated in a country, where, to the satisfaction of the relevant supervisory body, anti-money laundering regulation and supervision of compliance with such anti-money laundering regulation, which is equivalent to that applicable to the bank, are in force;
- a person or institution in that country, which is subject to antimoney laundering regulation confirms in writing, to the satisfaction of the bank that the person or institution, has verified the particulars concerning that client that the bank had obtained in accordance with section 21 of the FIC Act; and
- the person or institution undertakes to forward all documents obtained in the course of verifying such particulars to the bank.

The country in which the client is situated has to have anti-money laundering regulation and supervision of compliance with such antimoney laundering regulation in force. All FATF member countries are deemed to have adequate anti-money laundering legislation and supervision of compliance with such legislation in place.

If a country is not a FATF member country, more careful scrutiny of the anti-money laundering/combating of terrorist financing systems in that country should be undertaken to establish whether the requirements applicable to a specific institution are equivalent to the requirements of the South African legislation. If this is not the case, this exemption does not apply, and the entity has to be identified and verified as stipulated in the FIC Act and the Regulations.

30. Clarification of the difference between Exemptions 5 and 16

In terms of Exemption 16 of the Exemptions, a bank in South Africa is exempted from having to identify a bank in another country when the anti money laundering regulation and supervision that applies to that foreign bank is to the satisfaction of the supervisory body. This exemption applies in the case of transactions between the two banks and not to transactions of the underlying clients of the foreign bank.

Exemption 5 of the Exemptions relates to the underlying clients of a foreign institution, such as a bank. This exemption exempts a bank in South Africa from the verification of a foreign client's identity in cases when a regulated institution in the relevant country can verify that client's identity. The South African bank still has to establish the client's identity, but can rely

on the verification undertaken by the foreign institution. The conditions to exemption 5 are that the institution providing the verification of the client's identity must be subject to antimoney laundering regulation and supervision to a standard that meets the satisfaction of the relevant supervisory body. The foreign institution should forward all documents relative to the verification of the client's identity to the South African bank, in due course.

Both of these exemptions require an indication from the appropriate supervisory body as to which countries it considers to be applying satisfactory anti money laundering regulation and supervision to the relevant institutions. In the absence of such an indication, the best practice is to use the FATF issued list of non-cooperative countries and territories ("the NCCT") as an indication of jurisdictions that lack the intent to apply AML and CFT procedures. Extreme caution should be applied in transactions with these black listed jurisdictions. It would also be acceptable for supervisors and accountable institutions to regard those countries, which are actual FATF member countries, as being jurisdictions applying adequate AML and CFT procedures.

Glossary

The term **"bank"** in this guidance note refers to institutions that conduct banking business, in other words accountable institutions referred to in:

- Item 6 (A person who carries on the "business of a bank as defined in the Banks Act, 94 of 1990), or
- Item 7 (A Mutual Bank as defined in the Mutual Banks Act, 124 of 1993), which may be expected to be licensed as banks or mutual banks, respectively, and accountable institutions, which conduct similar activities, namely those referred to in:
 - Item 14 (A Postbank referred to in section 51 of the Postal Services Act 124 of 1998), or
 - Item 16 (The Ithala Development Finance Corporation Limited) of Schedule 1 to the FIC Act.

"The Centre" means the Financial Intelligence Centre established by section 2 of the FIC Act.

"Financial Intelligence Centre Act" (herein referred to as the FIC Act) refers to the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001).

"Money Laundering Control Regulations" (herein referred to as "the Regulations") refers to the regulations made in terms of section 77 of FIC Act and promulgated in Government Notice 1595 published in Government Gazette No. 24176 of 20 December 2002.

"Money Laundering Control Exemptions" (herein referred to as "the Exemptions") refers to exemptions made under section 74 of FIC Act and promulgated in Government Notice 1596 published in Government Gazette No. 24176 of 20 December 2002.

"The Financial Action Task Force" ("FATF") is an inter-governmental body that engages in the development and promotion of national and international policies and standards to combat money laundering and terrorist financing. The FATF is both a policy-making and standard setting body. It was created in 1989 and works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. Further information concerning the FATF is available at www.fatf-gafi.org.

The FATF Recommendations refers to the 40 Recommendations on combating money laundering plus 9 Special Recommendations on combating terror financing of the FATF that set out the basic framework to combat money laundering and terrorist financing. The FATF Recommendations are intended to be of universal application and have come to be accepted by organisations such as the World Bank and the International Monetary Fund to be the international standard to benchmark efforts to combat money laundering and terrorist financing. Since its creation the FATF has spearheaded the effort to adopt and implement measures designed to counter the use of the financial system by criminals. The FATF Recommendations can be accessed from www.fatf-gafi.org.

The Core Principles refer to the Basel Core Principles for Effective Banking Supervision which is the comprehensive set of twenty-five Core Principles that have been developed by the Basel Committee on Banking Supervision, a Committee of banking supervisory authorities which was established by the central bank Governors of the Group of Ten countries in 1975, as a basic reference for effective banking supervision. The Core Principles were designed to be applied by all countries in the supervision of the banks in their jurisdictions. The Core Principles can be accessed from www.bis.org.

The **Wolfsberg Principles** refer to **Global Anti Money Laundering Guidelines for Private Banks**, which sets out global guidance for sound business conduct in international private banking, **Correspondent Banks** and Politically Exposed Persons. The principles can be accessed from www.wolfsberg-principles.com.

The **United Nations List** means the list of individuals and entities as issued by the United Nations 1267 Sanctions Committee. The updated UN list can be accessed from www.un.org/Docs/sc/committees/1267/1267ListEng.

This list is published in a *Government Gazette* of the Republic of SA from time to time by proclamation under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004). The current proclamation can be accessed from http://www.saps.gov.za/docs_publs/legislation/terrorism/gazette27598pg33_64.pdf.

Organs of State as defined under section 239 of the **Constitution of the Republic of South Africa 1996 (Act 108 of 1999)** means—

- (a) any department of state or administration in the national, provincial or local sphere of government; or
- (b) any other functionary or institution
 - (i) exercising a power or performing a function in terms of the Constitution or a provincial Constitution; or
 - (ii) exercising a public power or performing a public function in terms of any legislation,but does not include a court or judicial officer.

Shell Banks refers to a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

Payable through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

**Issued by the Director
Financial Intelligence Centre
14 July 2005**

Third Reporting Exemption in terms of the Financial Intelligence Centre Act, 2001

Notice No. 1035 of 2006

Notice No. 1035 of 2006

Notice No. 1035
13 October 2006

By virtue of the powers vested in me by section 74 of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001, "the Act"), I, Trevor Andrew Manuel, Minister of Finance, hereby make the exemption set out in the Schedule hereto, with immediate effect.

Every person who carries on a business or is in charge of or manages a business or who is employed by a business and in that capacity assists or advises a client in connection with an application or prospective application for amnesty in terms of the Small Business Tax Amnesty and Amendment of Taxation Laws Act, 2006 (Act No 9 of 2006) is exempt from compliance with the provisions of section 29 (1) (b) (iv) of the Act, in respect of information disclosed to such a person for the purpose of obtaining advice or assistance in connection with the application or prospective application for amnesty referred to above, whether such an application is in fact made by or on behalf of the client or not.

EXPLANATORY MEMORANDUM TO THE THIRD REPORTING EXEMPTION IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001

1. The exemption from the obligations of section 29 (1) (b) (iv) of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001, hereafter "the Act") is aimed at facilitating the role of tax advisers in assisting their clients to apply for the small business tax amnesty provided for in the Small Business Tax Amnesty and Amendment of Taxation Laws Act, 2006 (Act No 9 of 2006, hereafter "the Small Business Tax Amnesty Act").
 2. The exemption relates to section 29 (1) (b) (iv) of the Act which covers a transaction or series of transactions to which a business is a party and which "may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service".
 3. The exemption applies to tax advisers by operation of law and does not have to be applied for. The exemption applies to a specific category of advisers namely those who
-

render assistance or advice to clients in connection with the amnesty in terms of the Small Business Tax Amnesty Act.

4. The exemption applies to advisers referred to in paragraph 3 whether the client in fact applies for the amnesty or not.
5. The exemption does not absolve any person from liability for their own involvement in unlawful activity such as tax evasion, since that liability does not arise from the provisions of the Act.
6. The amnesty in terms of the Small Business Tax Amnesty Act may become relevant to tax advisers in one of three scenarios:
 - An owner of a small business may approach a tax adviser to establish whether he or she qualifies for the small business tax amnesty and to obtain assistance in submitting his or her applications to the Commissioner of the South African Revenue Service. In these circumstances this exemption exempts tax advisers from having to report information which the person may disclose concerning past failures to comply with tax obligations relating to the business in question.
 - An owner of a small business may approach a tax adviser to obtain generic tax advice without referring specifically to the small business tax amnesty. During the consultation it may become apparent to the tax adviser that the person has previously failed to comply with certain tax obligations pertaining to the business in question. The tax adviser would have to advise the person of the small business tax amnesty and recommend that the person apply for the amnesty. In these circumstances this exemption exempts tax advisers from having to report information which the person may disclose concerning past failures to comply with tax obligations relating to the business in question. However, should the tax adviser not advise the person of the small business tax amnesty, or fail to recommend that the person apply for the amnesty, the information disclosed to the adviser would not be regarded as being "disclosed for the purpose of obtaining advice or assistance in connection with" an application or prospective application for amnesty. In these circumstances the exemption does not apply.
 - An owner of a small business may approach a tax adviser in circumstances which lead the adviser to suspect that his or her services will be abused to conceive of, carry out or perpetuate a scheme to conceal the source or the nature of proceeds of unlawful activities or to evade tax. In these circumstances the exemption does not apply.

Guidance Note 4 on Suspicious Transaction Reporting

Notice No. 301 of 2008

Part 1 : Who Must Report?

Part 2 : What Gives Rise to the Obligation to Report?

Part 3 : What is the Nature of a Suspicion?

Part 4 : Indicators of Suspicious and Unusual Transactions

Part 5 : What are the Implications of making a STR?

Part 6 : Process for Submitting STRs to the Centre

Notice No. 301 of 2008

Notice No. 301
14 March 2008

Financial Intelligence Centre

The Financial Intelligence Centre has, in terms of its statutory function under section 4(c) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued the guidance note in the Schedule.

M Michell
Director: Financial Intelligence Centre
Date: 13/03/2008

Preface

Money laundering has been criminalised in section 4 of the Prevention of Organised Crime Act, 1998. A money laundering offence may be described as the performing of any act that may result in concealing the nature of the proceeds of crime or of enabling a person to avoid prosecution or in the diminishing of the proceeds of crime.

Apart from criminalising the activities constituting money laundering, South African law also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, as contained in the Financial Intelligence Centre Act, 38 of 2001, ("the FIC Act") are based on three basic principles of money laundering detection and investigation, i.e, that:

- intermediaries in the financial system must know with whom they are doing business;
- the paper trail of transactions through the financial system must be preserved;
- possible money laundering transactions must be brought to the attention of the Financial Intelligence Centre ("the Centre") and the investigating authorities.

The control measures introduced by the FIC Act include requirements for institutions to establish and verify the identities of their customers, to keep certain records, to report certain information and to implement measures that will assist them in complying with the Act.

The FIC Act also established the Financial Intelligence Centre which is South Africa's financial intelligence unit, a government agency created to collect, analyse and interpret information disclosed to it and obtained by it. The Centre is an integral part of our country's fight against the global crime of money laundering. In addition, section 4 (c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations of the Act. This Guidance Note is published by the Centre in terms of section 4(c) of the FIC Act.

Application of this Guidance Note

The Centre has prepared this Guidance Note to assist accountable institutions, reporting institutions and any other person as described in section 29 of the FIC Act in meeting their reporting obligations under the Act. It provides general guidance on the nature of reporting under section 29 and explains reporting timelines, how reports have to be sent to the Centre, what information has to be included in these reports and how to use the electronic reporting mechanism.

Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Money Laundering and Terrorist Financing Control Regulations ("the Regulations") issued under the FIC Act.

Guidance emanating from industry associations or other organisation, therefore, in the Centre's view, does not have a bearing on assessing compliance with the obligations imposed by the FIC Act or the interpretation of its provisions.

The guidance provided by the Centre in this Guidance Note, although authoritative, is provided as general information only. The Guidance Note does not provide legal advice and is not intended to replace the FIC Act or the Regulations issued under the FIC Act. However, failure to forward suspicious transaction reports through to the Centre is an offence in terms of section 52 of the FIC Act.

Glossary

"The Centre"

means the Financial Intelligence Centre established in terms of section 2 of the FIC Act.

"FIC Act"

refers to the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001), as amended.

"POCA"

refers to the Prevention of Organised Crime Act, 1998 (Act No 121 of 1998), as amended.

"Regulations"

refer to the Money Laundering and Terror Financing Control Regulations made in terms of section 77 of the FIC Act and promulgated in Government Notice 1595 of 20 December 2002 as amended by Government Notice R456 of 20 May 2005.

"Reporter"

refers to the person or entity making the report.

"STR"

refers to a suspicious or unusual transaction report submitted in terms of Section 29 of the FIC Act.

Introduction

The FIC Act provides for the reporting of suspicious and unusual transactions. The FIC Act repealed section 7 of the POCA and from 3 February 2003 the duty to report suspicious and unusual transactions is governed by section 29 of the FIC Act.

Accountable institutions, reporting institutions and any other person as described in section 29 of the FIC Act have a role to play in South Africa's efforts to prevent money laundering and terrorist financing. It is imperative that accountable institutions, reporting institutions and any other person that comes into contact with a financial transaction that is potentially linked to money laundering or terrorist financing, report his or her suspicion to the Centre.

The reporting of suspicious and unusual transactions is regarded as an essential element of the anti-money laundering programme for every country. The international standard on measures to combat money laundering and terrorist financing, in the form of the Forty Recommendations of the Financial Action Task Force ("the FATF") on Money Laundering, provides the following concerning the reporting of suspicious transactions:

"Recommendation 13

If financial institutions suspect that funds stem from criminal activity, they should be required to report promptly their suspicions to the competent authorities".

The FATF is an inter-governmental body that engages in the development and promotion of national and international policies and standards to combat money laundering and terrorist financing. It works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has developed internationally recognised standards for measures to combat money laundering and terror financing in the form of the Forty Recommendations and the Nine Special Recommendations on Terrorist Financing. Further information concerning the FATF is available at <http://www.fatf-gafi.org>.

This Guidance Note is divided into six parts:

- Part 1 provides information to help persons determine whether they fall within the category of persons for whom a reporting obligation under section 29 of the FIC Act could arise.
 - Part 2 provides information to help persons determine when the obligation to report under section 29 of the FIC Act arises.
 - Part 3 provides information to help persons understand the nature of a suspicion.
 - Part 4 provides examples of indicators that may be taken into consideration to determine whether a transaction should give rise to a suspicion.
 - Part 5 provides information on the implications of masking a report under section 29 of the FIC Act to the Centre.
 - Part 6 provides a step-by-step guideline to the use of the internet-based reporting mechanism.
-

Part 1 - Who Must Report?

- 1.1 The obligation to report suspicious and unusual transactions under section 29 of the FIC Act applies to a very wide category of persons and institutions. The FIC Act imposes this obligation on any person who:
- carries on a business,
 - is in charge of a business,
 - manages a business, or
 - is employed by a business.
- 1.2 The term "business" is not defined in the FIC Act. The ordinary meaning of the term, within the context of the FIC Act, is that of a commercial activity or institution, as opposed to a charitable undertaking or public sector institution. This means that any person associated with a commercial undertaking as an owner, manager or employee of that undertaking, can become subject to the obligation to report suspicious or unusual transactions.

Part 2 - What Gives Rise to the Obligation to Report?

- 2.1 The obligation under section 29 of the FIC Act to report a transaction arises when a person knows of certain facts, on the one hand, or in circumstances in which a person ought reasonably to have known or suspected that certain facts exist, on the other. This means that a person associated with a business, as described above, must report his or her knowledge or suspicion to the Centre whenever:
- he or she becomes aware of something, or
 - circumstances arise in which a person can reasonably be expected to be aware of something, or
 - circumstances arise in which a person can reasonably be expected to suspect something.
- 2.2 Section 29(1) of the FIC Act describes the "something" referred to above. This can relate to situations concerning the business itself or concerning transactions to which the business is a party. Situations relating to the business itself are that the business: has received the proceeds of unlawful activities, or it is about to receive such proceeds,
- has received property which is connected to an offence relating to the financing of terrorist activities, or it is about to receive such property,
 - has been used in some way for money laundering purposes, or it is about to be used for money laundering purposes, or
 - has been used in some way to facilitate an offence relating to the financing of terrorist activities, or it is about to be used for this purpose.
- 2.3 These do not have to relate to any particular transactions involving the business. Instead they relate more to the way in which the affairs of a business are conducted. These include, for example, instances where the business is used as a front to disguise the movement of proceeds of unlawful activities, or where the facilities of a business (such as its bank accounts) are being used to facilitate the transfer of proceeds of
-

unlawful activities.

- 2.4 The situations concerning transactions to which the business is a party relate to transactions between the business in question and its customers and the customers' motives for engaging in those transactions. These can relate to a particular transaction or to a series of transactions. These are situations where a person is aware or suspects that a transaction or series of transactions with the business:
- facilitated the transfer of the proceeds of unlawful activity or is likely to do so,
 - facilitated the transfer of property which is connected to an offence relating to the financing of terrorist activities or is likely to do so,
 - does not appear to have a business purpose,
 - does not appear to have a lawful purpose,
 - may be relevant to the investigation of the evasion of any tax administered by the South African Revenue Service, or
 - somehow relates to an offence relating to the financing of terrorist activities.
- 2.5 The FIC Act defines "*proceeds of unlawful activity*" and "*unlawful activity*" by reference to the definitions of the same terms in the POCA. Thus the term "*proceeds of unlawful activity*" for the purposes of the FIC Act means:
- any property or any service, advantage, benefit or reward;
 - which was derived, received or retained:
 - directly or indirectly,
 - in South Africa or elsewhere,
 - at any time before or after the commencement of POCA,
 - in connection with or as a result of any unlawful activity carried on by any person.
- 2.6 The term "*unlawful activity*" means any conduct, which constitutes a crime or which contravenes any law whether such conduct occurred in the Republic or elsewhere.
- 2.7 It is important to note that Section 29 of the FIG Act refers to reports being made in connection with the **proceeds** of unlawful activities and **money laundering or terror financing** offences as opposed to criminal activity in general. The FIG Act therefore does not require reports to be made on suspected crimes or unlawful conduct by a person (apart from money laundering and terror financing activities).

This may best be explained by means of an example:

A stolen or fraudulent cheque is presented for payment to a bank. This action constitutes an element of a fraud, namely a misrepresentation that the person presenting the cheque is the legitimate holder of the cheque and is entitled to receive the amount reflected on the cheque. The presentation of the cheque is therefore part of an action to commit an offence, namely fraud. As a result this transaction should be reported to the appropriate investigating authorities as a fraud or attempted fraud. However, if the stolen or fraudulent cheque is honoured, the funds collected as a result would constitute the proceeds of the fraud. Any subsequent transaction involving those funds would be a transaction relating to the proceeds of unlawful activities and possibly a money laundering transaction which would fall within the scope of section 29 of the FIC Act.

Part 3 - What is the Nature of a Suspicion?

- 3.1 In addition to circumstances where a person has actual knowledge, the reporting obligation under section 29 of the FIC Act also applies in circumstances where a mere suspicion may exist. The FIG Act does not define what constitutes a suspicion. The ordinary meaning of this term includes state of mind of someone who has an impression of the existence or presence of something or who believes something without adequate proof, or the notion of a feeling that something is possible or probable. This implies an absence of proof that a fact exists.
- 3.2 This interpretation of the term "suspicion" was also applied in South African case law: In **Powell NO and others v Van dar Merwe NO and Others** 2005 (5) South Africa 62 (SCA) the Supreme Court of Appeal confirmed that South African courts have endorsed the following interpretation of the term used by Lord Develin in the English case of **Shabaan Bin Hussein and Others v Chong Fook Kam and Another** [1970] AC 942 (PC) ([1969] 3 All ER 1627) at 948B:
- Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking; "I suspect but I cannot prove".
- 3.3 With this in mind the starting point to considering whether circumstances give rise to a suspicion would be when those circumstances raise questions or gives rise to discomfort, apprehension or mistrust.
- 3.4 A suspicious state of mind is subjective, which means that a court would have to draw inferences concerning a person's state of mind in relation to a particular set of circumstances from the evidence at its disposal concerning those circumstances. However, the FIC Act adds an element of objectivity to this with the phrase "*ought reasonably to have known or suspected*" in section 29(1). The application of this phrase is explained in section 1(3) of the FIC Act. Section 1(3) of the POCA provides that a person ought reasonably to have known or suspected a fact if a reasonably diligent and vigilant person with the same knowledge, skill, training and experience, as well as the knowledge, skill, training and experience that may reasonably be expected of a person in the same position, would have known or suspected that fact. This expands the scope of the obligation to identify circumstances which may indicate that a set of circumstances concerning a business, or the transactions involving the business, is of a suspicious nature.
- 3.5 When considering whether there is reason to be suspicious of a particular situation one should assess all the known circumstances relating to that situation. This includes the normal business practices and systems within the industry where the situation arises.
- 3.6 A suspicious situation may involve several factors that may on their own seem insignificant, but, taken together, may raise suspicion concerning that situation. The context, in which a situation arises, therefore, is a significant factor in assessing suspicion. This will vary from business to business and from one customer to another.
- 3.7 A person to whom section 29 of the FIC Act applies, should evaluate matters concerning the business in question and transactions involving the business, in relation to what

seems appropriate and is within normal practices in the particular line of business of that person, and bring to bear on these factors such as the knowledge the person may have of the customer. This should involve an application of person's knowledge of the customer's business, financial history, background and behaviour.

- 3.8 A particular category of transactions that are reportable under section 29(1) of the FIC Act is transactions which a person knows or suspects to have no apparent business or lawful purpose. This refers to situations where customers enter into transactions that appear unusual in a business context or where it is not clear that purpose of the transaction(s) is lawful. In order to identify situations where customers wish to engage in these unusual transactions a person would have to have some background information as to the purpose of a transaction and evaluate this against several factors such as the size and complexity of the transaction as well as the person's knowledge of the customer's business, financial history, background and behaviour.
- 3.9 In Part 4 of this Guidance Note more information is given as to factors that may indicate that a transaction is suspicious in a money laundering and terrorist financing context, respectively. These are indicators as to circumstances that may give rise to a suspicious state of mind or may be indicative of the fact that a reasonably diligent and vigilant person may have become suspicious of a particular transaction or series of transactions.

Part 4 - Indicators of Suspicious and Unusual Transactions

- 4.1 The indicators discussed in this Part apply specifically to those situations where a suspicion may relate to a transaction between a business and its customer. These indicators are offered in order to assist persons involved in business to identify those situations where transactions should raise questions or give rise to the sense of discomfort, apprehension or mistrust which was referred to in the previous Part. These indicators are therefore merely **examples** of factors that may be helpful when evaluating transactions. The list is not exhaustive and does not intend to cover every possible situation. The indicators suggested here should not to be viewed in isolation and should always be taken into consideration in conjunction with all other circumstances pertaining to a particular transaction.

Unusual business

- Deposits of funds with a request for their immediate transfer elsewhere;
 - Unwarranted and unexplained international transfers;
 - The payment of commissions or fees that appear excessive in relation to those normally payable;
 - Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type of transaction or particular method of transacting;
 - Transactions do not appear to be in keeping with normal industry practices;
 - Purchase of commodities at prices significantly above or below market prices;
 - Unnecessarily complex transactions;
 - Unwarranted involvement of structures such as trusts and corporate vehicles in transactions;
 - A transaction seems to be unusually large or otherwise inconsistent with the
-

customer's financial standing or usual pattern of activities;

- Buying or selling securities with no apparent concern for making a profit or avoiding a loss;
- Unwarranted desire to involve entities in foreign jurisdictions in transactions.

Knowledge of Reporting or Record Keeping Requirements

- A customer attempts to convince employee not to complete any documentation required for the transaction;
- A customer makes inquiries that would indicate a desire to avoid reporting;
- A customer has unusual knowledge of the law in relation to suspicious transaction reporting;
- A customer seems very conversant with money laundering or terrorist activity financing issues;
- A customer is quick to volunteer that funds are clean or not being laundered.

Identification

- The use of a seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar but different addresses and, in particular, the opening or operating of a false name account;
- Opening accounts using false or fictitious documents;
- A customer provides doubtful or vague identification information;
- A customer refuses to produce personal identification documents;
- A customer changes a transaction after learning that he must provide a form of identification;
- A customer only submits copies of personal identification documents;
- A customer wants to establish identity using something other than his or her personal identification documents;
- A customer's supporting documentation lacks important details such as contact particulars;
- A customer inordinately delays presenting corporate documents; or
- All identification presented is foreign or cannot be checked for some reason.

General

- A customer provides insufficient vague or suspicious information concerning a transaction;
- Accounts that show unexpectedly large cash deposits and immediate withdrawals;
- A frequent exchange of small denomination notes for larger denomination notes;
- Involvement of significant amounts of cash in circumstances that are difficult to explain.

Suspicious Transaction Reports - threshold

- 4.2 It is important to make it clear that there is no monetary threshold which applies to the reporting of suspicious or unusual transactions. Once the conclusion is reached that a situation exists which should give rise to a suspicion that a transaction relates to proceeds of unlawful activities, money laundering or terror financing, as explained above, the transaction must be reported irrespective of the amount involved.
-

- 4.3 This must not be confused with a situation where the amount involved in a transaction, or series of transactions, is the basis of a suspicion or forms part of the circumstances which gives rise to a suspicion pertaining to the transaction or series of transactions.

Should the closing of an account be regarded as suspicious?

- 4.4 The closing of an account with an institution is a transaction which forms part of the business relationship which will be terminated by the account closure. In these circumstances institutions should consider factors such as the history of the account, the circumstances that led to the customer's decision to close the account and the reasons given by the customer for the closure of the account. For example, where a customer's instruction to close an account was preceded by a request by the institution for additional or updated information pertaining to the customer, the decision to rather close the account than to provide the requested information may be regarded as suspicious.

Part 5 - What are the Implications of making a STR?

Can an institution continue transacting with a customer after a STR has been made?

- 5.1 Section 33 of the FIC Act provides that a reporter may continue with and carry out a transaction in respect of which a report is required to be made unless the Centre directs the reporter not to proceed with the transaction in terms of section 34.
- 5.2 The Centre may issue a directive ("an intervention order") in writing not to proceed with a transaction after consultation with the institution or person concerned. The Centre must have reasonable grounds to suspect that a transaction may involve the proceeds of unlawful activities or property which is connected to an offence relating to terrorist financing, or may in some other way constitute money laundering terrorist financing. The intervention order may require the institution or person not to proceed with the transaction which gave rise to the Centre's belief or any other transaction in respect of funds that are affected by the particular transaction. The intervention order is valid for a period not exceeding five days excluding weekends and public holidays.
- 5.3 One of the main purposes of an intervention order is to prevent the dissipation of funds or property which may be the proceeds of unlawful activity. A typical example of where this may be the case is where funds or assets are due to be transferred from one location to another or from one person to another, especially where the transfer will have the effect of moving the funds or assets out of South Africa. Reporters are encouraged to indicate to the Centre at the time of making a report under section 29 if they believe that the funds or assets involved in a transaction or series of transactions may be dissipated. The same also applies if a report has been filed with the Centre and the reporter subsequently becomes aware that the suspected proceeds may be dissipated. In such cases the reporter may contact the Centre quoting their reference number and informing the Centre of the activities within such account.

Confidentiality and Privilege

- 5.4 Section 37(1) of the FIC Act overrides secrecy and confidentiality obligations in South African law. No duty of secrecy or confidentiality prevents any institution or person from complying with an obligation to file a report under the FIC Act.
- 5.5 Section 37(2) protects the common law right to legal professional privilege as between an attorney and an attorney's client in respect of communications made in confidence between:
- the attorney and the attorney's client for the purposes of legal advice or litigation which is pending or contemplated or which has commenced; or
 - a third party and an attorney for the purposes of litigation which is pending or contemplated or has commenced.

The reporter enjoys legal protection concerning a report submitted to the Centre

- 5.6 Section 38 of the FIC Act protects persons who participate in making reports to the Centre. No legal action, whether criminal or civil, can be instituted against any natural or legal person who complies in good faith with the reporting obligations of the FIC Act.
- 5.7 In addition to protection against legal liability, the FIC Act also protects the identities of those involved in making a report to the Centre. A person involved in the making of a report cannot be forced to give evidence in criminal proceedings concerning such a report. However, such a person may choose to do so voluntarily. If a person elects not to testify, no evidence regarding that person's identity is admissible as evidence in criminal proceedings.

Tipping off

- 5.8 A person involved in the making of a report may not inform anyone, including the customer or any other person associated with a reported transaction, of the contents of a suspicious transaction report or even the fact that such a report has been made.
- 5.9 Section 29 of the FIC Act prohibits any reporter as well as any other person who knows or suspects that a report has been made from disclosing any information regarding that report except for information disclosed:
- within the scope of the powers and duties of that person in terms of any legislation,
 - for the purpose of carrying out the provisions of this Act,
 - for the purpose of legal proceedings, including any proceedings before a judge in chambers, or
 - in terms of an order of court.
- 5.10 Contravening these prohibitions constitutes offences in terms of the FIC Act that carry maximum penalties of imprisonment for a period up to 15 years or a fine up to R10 million.

Are there any defences associated with the reporting obligation?

- 5.11 In terms of Section 69 of the FIC Act if a person who is an employee, director or trustee of, or a partner in, an accountable institution, is charged with not reporting suspicious or unusual transactions, that person may raise as a defence that he reported the

matter internally to the person responsible for ensuring compliance by the accountable institution with its duties.

- 5.12 In certain cases an employee may simply report the matter to a superior and, if that can be proved, the person will have a valid defence if he or she is charged with not reporting the transaction to the Centre directly.
- 5.13 In many situations the fact that a suspicion is formed and a report made to the Centre implies that a business could possibly be dealing with the proceeds of unlawful activities in a way that would fall within the scope of the money laundering offences of section 4, 5 and 6 of the POCA. In order to allow persons to report their suspicions freely while carrying on their business without exposing them to criminal liability for their involvement in the reported transaction a defence is provided in section 7A of the POCA against racketeering charges under section 2(1)(a) or (b) of the POCA and money laundering charges under sections 4, 5 and 6 of that Act. This defence applies both where a person has made a report to the Centre or has made a report in terms of the internal rules or arrangements of the institutions by which the person is employed.

Reactive reporting

- 5.14 Reactive reporting refers to the submitting of a STR to the Centre following an external prompt without a prior suspicion having been formed on the basis of the circumstances in which a particular transaction or series of transactions have been conducted. Examples of the prompts that may give rise to reactive reporting are:
- receiving a subpoena in terms of section 205 of the Criminal Procedure Act, 1997 (Act No 51 of 1997) or a similar process to provide evidence concerning matters relating its business dealings with a particular customer;
 - receiving a request to confirm whether a person is a customer of an institution in terms of section 27 of the FIC Act in respect of a particular customer;
 - receiving an intervention order in terms of section 34 of the FIC Act in connection with a transaction involving a particular customer;
 - receiving a monitoring order in terms of section 35 of the FIC Act concerning the transactions of a particular customer;
 - receiving other types of enquiries from government agencies such as investigating authorities or the South African Revenue Service about a particular customer;
 - seeing information in the media that may adversely affect a particular customer.
- 5.15 With regard to these external factors it is important to bear in mind that the obligation to file a STR with the Centre arises where a person becomes aware of certain facts or in situations which should give rise to a suspicion, as discussed in Part 2, above. External factors such as those referred to here, may contribute to the forming of a suspicion, but in all cases these factors should be considered in conjunction with all other factors pertaining to a particular transaction or series of transactions. These factors should, not in and of themselves, form the reason for submitting a report to the Centre in absence of any suspicion formed.
-

Part 6 - Process for Submitting STRs to the Centre

What is the time period for reporting a suspicious transaction?

- 6.1 In terms of regulation 24 of the Regulations a report under section 29 of the FIC Act must be sent to the Centre **as soon as possible**. In terms of the regulation this period must not be longer than fifteen days, excluding Saturdays, Sundays and Public Holidays, after a person became aware of the facts which give rise to a suspicion.
- 6.2 It is important to note that, in terms of regulation 24, the period for the filing of a STR does start from the point where a person forms a suspicion. The fifteen-day period starts when a person becomes aware of the facts which will eventually give rise to a suspicion. This may be, and in the majority of cases will be, before a suspicion is formed.
- 6.3 The fifteen-day period is to be used to consider other information at the reporter's disposal and to evaluate the circumstances to determine whether a transaction, or series of transactions, is suspicious or not. In order to comply with regulation 24, as explained in paragraph 5.1 above, this should be done as quickly as possible and once a suspicion is formed, the relevant transaction or transactions must be reported without delay. This means that reporters should not take the view that they, as a matter of routine, have a fifteen day period for the filing of reports under section 29 of the FIC Act. Reporters will be in breach of regulation 24 if they delay the reporting of a transaction or series of transactions once a suspicion is formed, and reporters should therefore avoid routinely reporting transactions 15 days after a transaction takes place.
- 6.4 It is only in exceptional cases that the Centre may consider condoning a STR being sent after the expiry of the fifteen-day period. If a reporter believes that they will not be able to report within the fifteen-day period, the reporter may apply for condonation for the late filing of the STR from the Centre. Application for an extension must be made **before** the expiry of the fifteen-day period and must be in writing. In the application for an extension the reporter must provide reasons as to why the period will not be met. Furthermore, details as to when the STR will be submitted must be provided. This application can be faxed to the Centre's Manager: Monitoring and Analysis at 012 309 9496.

How should a STR be submitted?

- 6.5 A report under section 29 of the FIC Act must be made by means of **internet based reporting** provided by the Centre at: www.fic.gov.za. **A STR may not be posted**. Only in exceptional cases may a STR be sent by fax or delivered by hand to the Centre at the address provided. The reporting form is available from the Centre or its website.

The Centre's contact details are:

Physical Address: 240 Vermeulen Street, Pretoria. 0001.
Telephone: 012 309 9200
Facsimile: 0123099496
E-mail: fic_feedback@treasury.gov.za
Website: www.fic.gov.za

Batch reporting

Reporters also have the option of submitting STRs via batch reporting. Batch reporting issued in instances where high volumes of STRs are submitted to the Centre on a regular basis. To be able to access this facility, reporters can forward their requests to the following email address: fic01@fic.gov.za

Information to be provided in a STR

- 6.6 Regulation 23 of the Regulations sets out the prescribed particulars that should be contained in a STR. A copy of the reporting form can be accessed via the Centre's website or in the Regulations. The following is the basic information that should be contained in the STR:
- The person or entity making the report;
 - The transaction that is reported;
 - Any account involved in the transaction;
 - The person conducting the transaction or the entity on whose behalf it is conducted;
 - The representative, if any who is conducting the transaction on behalf of another;
 - General information concerning the transaction.

What happens to a STR after being submitted to the Centre?

- 6.7 Once the Centre receives the STR, further analytical work will be conducted on the information provided in the report. If the information provided in the report, together with the additional analysis, indicates a reasonable believe that the information may be required to investigate suspected unlawful activity, the information will be referred to the appropriate authority to carry out further investigation. In accordance with section 38(3) of the FIC Act the Centre is required to ensure that personal information of those involved in the making of an STR is protected from unauthorised disclosure.

Completion of the STR form

- 6.8 The following guidelines are based on electronic reporting as this is the preferred method of receiving reports. The report consists of eight parts numbered from Part A to Part H. It is important to complete all fields in each part that are applicable to the situation which is reported. It is also important that as much information as possible be included in the report as this will enable the Centre to take action in respect of a report immediately and assess whether to instruct the reporter not to proceed with the transaction under section 34 of the FIC Act.

Example of a field:

* 1. Person or entity's Name :

- 6.9 The "Next" button will only work if **ALL** the mandatory fields in the Part that have been completed.

User Name and Password

- 6.10 Reporters who regularly submit reports electronically to the Centre as well as appointed Money Laundering Control Officers or Money Laundering Reporting Officers are advised to register their details with the Centre using the form on the website at www.fic.gov.za. This form must be printed or downloaded from the website, completed and forwarded to the Centre via fax at 012 309 9496 or via email to fic_feedback@fic.gov.za.
- 6.11 Once a person has registered with the Centre they will receive a user name and password. In subsequent reports the person will only have to enter the user name and password and will immediately be routed to Part 2(A) of the form. If the reporter's details have changed, the reporter must forward the updated details to the Monitoring and Analysis Department via fax at 012 309 9496 or via email to fic_feedback@fic.gov.za.
- 6.12 The reporter will then immediately be able to proceed with the completion of the rest of the form. Persons who experience any difficulty with obtaining or using their passwords should please contact the Centre's help desk at 0123099300.

Username ::	<input type="text"/>	<input type="button" value="Check"/>
Password ::	<input type="password"/>	

- 6.13 Reporters who are **NOT** registered users and who do not wish to register must not enter any information in these fields. Such persons must proceed directly to Part A where **ALL** the fields must be completed.

Important to remember when completing the STR form

- Do not to leave any spaces in the information entered into the relevant fields.
- Do not use any punctuation marks such as dashes, colons or forward or back slashes when reporting account numbers, branch numbers or amounts.

<u>Examples</u>		
	<u>Incorrect</u>	<u>Correct</u>
Time	2pm	14:00
Currency	R	ZAR
Amount	R 2 000 000	2000000
Account No.	2359-34-67	23593467
Tel. No.	(012) 309 9200	0123099200
Date	2008/05/30	20080530

Completing Part A: Particulars of person or entity from which STR emanates

- 6.14 Part A of the reporting form is divided into two parts - Part A and Part A (2). Part A requires information identifying the **PERSON MAKING THE STR**. It is important that the

reporter fill in their **OWN** particulars here as the Centre uses this information to send an acknowledgement of receipt and reference number for the report. The reference number should be kept and utilised at all times when dealing with the Centre in relation to a report. This is confirmation that the Centre has received a report and proof that a report was submitted to the Centre.

Example for individual reporting:

* 1. Person or entity's Full Name :	Joe Soap
* 2. Person or entity's Identifying number	186513550039081
* 3. Street Address:	11 Tasneed Avenue Marlborough Gaugeng 1392
* 4. Postal Address :	P O Box 1097465 Marlborough 1392
* 5. City :	Johannesburg
* 6. Postal Code :	1392
* 7. Surname of contact person :	Soap
* 8. Initials of contact person :	J
* 9. Title of contact person :	Mr
* 10. Telephone Number of contact person	0913729888
* 11. Fax Number of contact person :	0913729889
* 12. E-mail address of contact person :	joe.soap@yahoo.com
Next	

- 6.15 Reporters who are reporting on behalf of their employer must fill in the employer's details (fields A1 to A6) and their own details (fields A7 to A12). Please take note of the employer's internal procedures in this regard.

Example for company report:

* 1. Person or entity's Full Name :	Soap's Plastics
* 2. Person or entity's Identifying number	99/56783/23
* 3. Street Address:	11 Tasneed Avenue Marlborough Gaugeng 1392
* 4. Postal Address :	P O Box 1097465 Marlborough 1392
* 5. City :	Johannesburg
* 6. Postal Code :	1392
* 7. Surname of contact person :	Soap

* 8. Initials of contact person :	J
* 9. Title of contact person :	Mr
* 10. Telephone Number of contact person	0913729888
* 11. Fax Number of contact person :	0913729889
* 12. E-mail address of contact person :	joe.soap@soapsplastics.com
Next	

- 6.16 Part A (2) deals with the type of report that is being made. If it is a new report, the reporter should provide their own unique internal reference number, if such a number has been allocated to the report, for ease of reference and future correspondence.
- 6.17 A reporter who wishes to make a correction of, or an addition to, a previous report, please remember to fill in the Centre's reference number and their own unique reference number in respect of the previous report so that the Centre can match the reports. The field requesting the date of the previous report relates to the date that the report was submitted to, and received by, the Centre. Please take note of the format for reporting the date of the transaction (YYYYMMDD).

Example of Part A(2):

This is :

☐ a new report

☐ a correction of a previous report

☒ additional information to a previous report

Your reference number for this report : SP27/2009

Number of previous report: 888/2009
(Recent reference number received from the FIC)

Date of previous report: 20090807 (yyyymmdd)

Part of previous report affected : A ☐ B ☐ C ☐ D ☒ E ☐ F ☐ G ☐ H ☐

Next

Completing Part B: Particulars of transaction reported

- 6.18 Part B of the STR form deals with the transaction/s which are being reported to the Centre.
- 6.19 It is very important to provide as much information as possible concerning the specific transaction or series of transactions which are the subject of the STR, in order to

enable the Centre to carry out a meaningful analysis of the reported information. All relevant fields must therefore be completed. An example of how to complete Part B is provided below.

Example of Part B:

1a. Date of Transaction	20090328	(yyyymmdd)
1b. Time of Transaction	1530	(hhmm)
1c. Period of transaction (in case of series of transactions):	From 20050203 To 20050205	(yyyymmdd)
2. Type of funds :	<input checked="" type="checkbox"/> Cash	
	<input type="checkbox"/> Cheque	
	<input type="checkbox"/> Credit	Card
	<input type="checkbox"/> Bank	Draft
	<input type="checkbox"/> Money	Order
	<input type="checkbox"/> EFT	
	<input type="checkbox"/> Travelers'	Cheque
	<input type="checkbox"/> Other	

3.	Amount of Transaction(s) in Rand Value:	<input type="text" value="200000"/>
4.	Currency :	<input type="text" value="South African Rand , ZAR"/>
5.	Description of property :	<input type="text"/>
6.	Value of Property :	<input type="text"/>
7.	Method Transaction Was Conducted :	<div><input checked="" type="checkbox"/> In-branch <input type="checkbox"/> Telephone <input type="checkbox"/> Mail <input type="checkbox"/> Courier <input type="checkbox"/> ATM <input type="checkbox"/> Internet <input type="checkbox"/> Inward foreign transfers <input type="checkbox"/> Other <input type="text"/></div>
8.	Stated Purpose of Transaction (where applicable) :	<input type="text" value="purchase of car"/>

		<input type="checkbox"/> Cash	
		<input type="checkbox"/> Cheque	
		<input type="checkbox"/> Deposit	
		<input type="checkbox"/> Bank	Draft
		<input type="checkbox"/> Money	Order
9. Method In Which Funds Were Disposed Of :	<input checked="" type="checkbox"/> EFT		
	<input type="checkbox"/> Trav		Cheque
	<input type="checkbox"/> Currency		Exchange
	<input type="checkbox"/> Internet		Transfer
	<input type="checkbox"/> Other	<input type="text"/>	
10. Amount of	<input type="text" value="150000"/>		
Disposition :			
11. Currency :	<input type="text" value="South African Rand . ZAR"/>		
		<input type="checkbox"/> Bought	
		<input type="checkbox"/> Sold	
		<input type="checkbox"/> Let	
12. Method In Which Property Was Disposed Of :	<input type="checkbox"/> Hired		
	<input type="checkbox"/> Exchanged		
	<input type="checkbox"/> Donated		
	<input type="checkbox"/> Other	<input type="text"/>	
13. Name of Other Institution or Person (where applicable) :	<input type="text" value="MPA BANK"/>		
14. Account Number at Other Institution (where applicable) :	<input type="text" value="012012"/>		

15.	Branch Where Transaction was Conducted (where applicable) :	CAPE TOWN
16.	Identifying Number of Branch (where applicable) :	1250604
17.	Remarks, Comments, Explanations etc. Person Conducting Transaction May Have Made or Given :	Mr Bloggs (/the client) indicated that he requires the funds to be transferred immediately. He claimed that he needed the funds to purchase a vehicle.
		Next

Transaction(s) (fields B1a to B1c)

- 6.20 A report can relate either to a single transaction or a series of transactions. Fields B1a and 1b relate to a single transaction and field B1c should be completed for a series of transactions. Field B1c should be filled in where the suspicion was detected after monitoring behaviour over a period of time.

Type of funds (field B2)

- 6.21 This relates to the format in which the transaction was carried out when the suspicion occurred. Type of funds could include cash, cheque, credit card or other. In the case of "other", please indicate the type of funds used in the transaction in the field provided.

Amount of Transaction(s) in Rand Value (field B3)

- 6.22 Amounts must be completed without any spaces or currency signs. If the transaction(s) were undertaken in a foreign currency please convert this to Rand and provide the amount in approximate Rand value, using the day of the report as a guide for the exchange rate.

Currency (field B4)

- 6.23 This field requires the reporter to indicate the currency in which the transaction was conducted for example, United States Dollar (USD) or Great British Pound (GBP). Please use the abbreviation ZAR for South African Rand.

Description of the property (field B5)

- 6.24 This field must be used if the transaction involved assets other than money, such as the purchase of fixed property or an investment policy for example. Property, other than money, can include movable (vehicle) or immovable (house), corporeal (things that are visible and tangible such as land, buildings, vehicles, jewellery) or incorporeal thing (trademarks, patents, copy right) and includes any rights, privileges, claims and securities and any interests. A description of the property must be provided in this field. Please do not use the TAB button or leave any unnecessary spaces.

Example

Incorrect

The property is:
Erf 1234
Marlborough
1610

Correct

Erf 1234 Marlborough 1610

Value of property (field B6)

- 6.25 In this field the reporter must indicate the approximate value of the property.

Method transaction was conducted (field B7)

- 6.26 The reporter must indicate how the transaction was conducted, for example: in a branch, by mail or via ATM which appears on the screen. If the transaction was not conducted using the listed methods of transaction then complete the "other" field and provide a description of the other method in which the transaction was conducted.

Stated purpose of the transaction (field B8)

- 6.27 The reporter must indicate the information which the customer may have provided as to the intended purpose of the transaction, for example that the transaction was conducted to purchase a new vehicle.

Method in which funds were disposed of (field B9)

- 6.28 This field requires the reporter to describe how the business disposed of the funds as a result of the transaction, in other words what happened to the funds involved in the transaction. There could be more than one use for a particular transaction. For example, the customer could initiate a transaction in cash, send an electronic fund transfer ("EFT"), order a bank draft and deposit the remainder.

Amount of disposition (field B10)

- 6.29 In this field the reporter must indicate the amount involved in the disposition. If the amount was not in Rand, the reporter must convert the amount and also provide the currency information such as USD/GBP/ZAR.

Currency (field B11)

- 6.30 This field requires the reporter to provide currency in which the disposition was carried out, even if it was in Rand. For example: enter CAD for Canadian dollars or USD

for United States Dollars.

Method in which property was disposed of (field B12)

- 6.31 If property, other than money was used in the transaction, this field must be used to indicate the manner in which the property was disposed of.

Name of other institution or person (field B13)

- 6.32 The reporter must indicate whether another person or institution was involved in the transaction, apart from the reporting business and the customer carrying out the transaction which is being reported. For example, if the reporter knows who the recipient of the funds were, or to which institution the funds were transferred, then those particulars must be provided.

Account number at other institution (field B14)

- 6.33 If the transaction which is being reported involved an account at the other institution referred to in field B13 and this number is available to the reporter, then the account number must be provided in this field. Please note that no spaces or punctuation marks should be used.

Branch where the transaction was conducted (field B15)

- 6.34 This field requires the reporter to indicate at which branch or office of the reporting business the transaction in question was conducted. For example, if the transaction occurred at an institution's branch or office in Cape Town, then the specific branch name, i.e. Cape Town, must be inserted. ***This is the case even though the transaction may have been identified as suspicious and be reported by the institution's head office in Johannesburg.*** It is very important that this information as to the geographical location where the transaction was carried out be provided in the report to the Centre as it contributes greatly to the Centre's ability to analyse the reported information.

Identifying number of branch (field B16)

- 6.35 If the branch or office where a transaction is carried out has a unique number to identify it generally or within the reporting institution, that must be provided in this field. For example: if an institution's branch in Cape Town has a branch number of 1250604 then the branch number 1250604 must be completed in the field.

Remarks, Comments, Explanations (field B17)

- 6.36 This field requires the reporter to provide any remarks, comments, or explanations the person conducting the transaction may have made or given in respect of the transaction. It is very important that this information be provided if it is available as it helps to contextualise the report and improves the Centre's ability to analyse the reported information.

Completing Part C: Particulars of accounts involved in transaction

- 6.37 Part C of the reporting form pertains to information about the account(s) involved in
-

the reported transaction(s), if an account was involved. In other words, in every case where an account is involved in a transaction Part C must be completed. This is not limited to bank accounts, and includes accounts of any nature which a reporting business may provide to its customers in accordance with the nature of that institution.

6.38 It is possible to have more than one transaction per report, and more than one disposition per transaction. It is also possible that more than one account may have been involved in a transaction or series of transactions.

6.39 As with the previous part, it is very important to provide as much information as possible. All relevant fields must be completed in order to provide the account information for each account that is included in the report.

Example of Part C:

1. Account number :	25212
2. Branch where account is held :	Cape town
3. Identifying number of branch (where applicable) :	1250604
4. Type of account :	cheque
5. Name of each account holder :	A : A. SMIT B : B. NEL C : K. KHOZA
6. Date Opened :	20050201

7. Date Closed :

8. Closed by : ☒ Not applicable
☐ Institution
☐ Client

9. Status of account : ☒ Not applicable
☐ Active
☐ Inactive
☐ Dormant

10. Previous Activity in Past 180 days concerning this account considered for reporting (whether in fact reported or not) :

11. Report Number if reported :

Account number (field C1)

- 6.40 This field requires the reporter to provide the relevant account number. Please do not leave any spaces.

Branch where account is held (field C2)

- 6.41 This field requires the reporter to provide the branch name(s) where the account(s) are held. Please note that this is not necessarily the same as the branch referred to in the previous section where the transaction(s) were conducted. As with the previous part of the form, it is very important that this information as to the geographical location where the relevant account is held be provided in the report to the Centre as it contributes greatly to the Centre's ability to analyse the reported information.

Identifying number of branch (field C3)

- 6.42 If the branch where an account is held has a unique number to identify that branch generally or within the reporting institution, that must be provided in this field. For example: if the account in question is held at an institution's branch in Cape Town and that branch has a branch number of 1250604 then the branch number 1250604 must be completed in the field.

Type of account (field C4)

- 6.43 The type of the account must be indicated in this field. For example: a cheque, savings, credit, or business account.

Name of each account holder (field C5)

- 6.44 The full name of each account holder (up to three) must be provided in this field. This relates to information on each individual or entity that holds the account. For example, in the case of a joint account of a husband and wife, include the names of each spouse. The account holder might be different from the individual(s) authorised to give instructions on the account. For example, an account for a corporation will have one or more individuals authorised to give instructions on that account. In such a case, the name of the corporation that holds the account must be provided in this field.

Date opened (field C6)

- 6.45 This field requires the reporter to provide the date when the account was opened.

Date closed and closed by (fields C7 and C8)

- 6.46 If the account in question had been closed before the report had been made, the date (yyyymmdd) when the account was closed must be provided here. If the account is still open at the time when the report is made this field must be completed at N/A. If the account had been closed the reporter must indicate on whose initiative this had been done by marking the relevant option in field C8.

Status of account (field C9)

- 6.47 In this field the reporter must indicate whether the account was active, inactive or dormant at the time the transaction or series of transactions, which is the subject of the report was initiated.

Previous activity on the account (field C10)

- 6.48 This field requires the reporter to indicate any activity on the account in the 180 days preceding the date of the report which had been identified and considered for reporting to the Centre (whether in fact reported or not). In other words the reporter is required to indicate past activity relating to the account which had raised attention as possibly being suspicious and in respect of which there had been some consideration given to whether the activity should be reported to the Centre. For example: three large round deposits and withdrawals shortly after deposits.

Report number (field C11)

- 6.49 If the activity referred to in field C10 had been reported to the Centre, the reference number of the previous report must be provided here.

Completing Part D: Particulars of person or entity concerning whom report is made

- 6.50 This Part of the STR form requires the reporter to provide the details of the person or
-

entity concerning whom the report is made. In the majority of cases where the report is based on a transaction, or series of transactions, to which the business was a party, the information provided in this Part will relate to the customer of the business who carried out the transaction(s). If the report concerns more than one individual or entity, this information should be completed under this Part F, together with any other information that was not completed in the form.

Example of Part D:

1. This Report Concerns :

☒ an individual
(i. please complete sections 2 to 10 and 16 to 18 of this part
ii. complete as many sections as possible)

☐ an entity
(i. please complete sections 11 to 18 of this part
ii. complete as many sections as possible)

2. Surname :

Blogs

3. First Name :

Joe

4. Other Initials :

j

5. Identifying number :

45856292211485

6. Type of Identifier :



ID

Book



Passport



Other

7. Country of Residence :

South Africa

8. Contact Telephone Number :

012309652825

9. Person's Occupation :

law yer

10. Is there a photograph or other image of the person available?



Yes



No

11. Name of entity :

12. Identifying number (where applicable) :

13. Type of business :

14. Country of origin :

The form is titled 'Part D' and contains the following fields:

- 15. Persons with Signing Authority :** This field is divided into three sub-sections:
 - A :** A text input field.
 - B :** A text input field.
 - C :** A text input field.
- 16. Street Address :** A text input field.
- 17. City :** A text input field.
- 18. Postal Code :** A text input field.

At the bottom left of the form is a button labeled 'Next'.

This report concerns: (field D1)

- 6.51 If the report relates to a natural person then fields 2-10 and 16-18 of Part D must be completed. If the report concerns an entity then fields 11 to 18 of Part D must be completed.

Surname, first names and other initials (fields D2 to D4)

- 6.52 These fields require the reporter to provide the person's full surname, full first name and other initials, respectively.

Identifying number (field D5)

- 6.53 This field requires the reporter to provide the person's identity or passport number. For example: 72525652266215 (please do not leave any spaces).

Type of identifier (field D6)

- 6.54 In this field the reporter must indicate the type of document that had been used to confirm the person's identity. For example: indicate if a passport, green bar coded identity book or drivers licence was used.

Country of residence (field D7)

- 6.55 This field requires the reporter to provide the person's country of permanent residence. Please insert the full name of the country, for example, South Africa and not RSA or SA.

Contact phone number (field D8)

- 6.56 This field requires the reporter to list all available contact numbers with an indicator (w-work) (h-home) (c-mobile) (f-fax). For example:
 012526256226w,
 0112528525h,
 012 52525225f

Person's occupation (field D9)

- 6.57 This field requires the reporter to provide person's occupation. For example: accountant, lawyer, government employee etc.

Photograph (field D10)

- 6.58 This field requires the reporter to indicate whether the reporting business has a photograph or other image of the person available. This may be an image obtained from video surveillance of the business' premises or from a copy or an electronic scan of a person's identity document, drivers licence or passport, for example.

Name of entity (field D11)

- 6.59 This field requires the reporter to provide the name of the entity to which the report relates.

Identifier number (field D12)

- 6.60 This field requires the reporter to provide the company or close corporation registration number or other unique identifying number that may apply to the entity in question.

Type of business (field D13)

- 6.61 This field requires the reporter to indicate the nature of the business activity in which the entity in question is involved, for example, the financial services industry, farming etc.

Country of origin (field D14)

- 6.62 This field requires the reporter to indicate the country from which the entity originates. Please insert the full name of the country, for example, South Africa and not RSA or SA.

Person with authority to transact (field D15)

- 6.63 In this field the reporter must provide the full name(s) and surname(s) of the person(s) who have authority to transact with the reporting business on behalf of the entity. Please do not use punctuation or tabs as separators.

Street Address (field D16 to D18)

- 6.64 These fields require the reporter to provide the street address (street number, name of building and suburb, for example: 12 Striven Street, Westbuild building 934, Sunnyside) as well as the city and postal code of the entity.

Completing Part E: Particulars of person conducting transaction

- 6.65 Part E only applies if the transaction was conducted by a person on behalf of the person or entity referred to in Part D. The details pertaining to that individual who
-

carried out the transaction on behalf of the person identified in Part D should be provided in full.

Example of Part E:

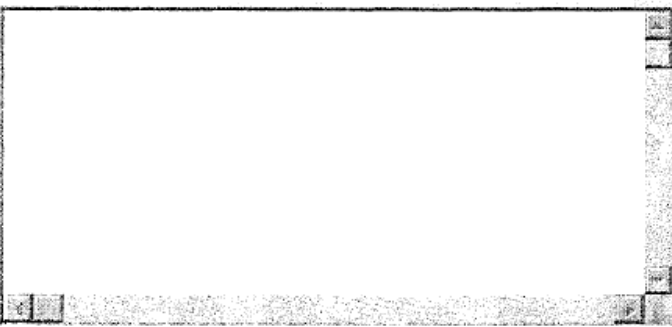
1. Transaction was conducted by :	
<input type="radio"/> the person referred to in Part D (do not proceed to complete this part)	<input checked="" type="radio"/> a person on behalf of the person or entity referred to in Part D (please complete as many of the sections as possible)

2. Surname :	<input type="text" value="Blogs"/>
3. First Name :	<input type="text" value="Joe"/>
4. Other Initials :	<input type="text" value="R"/>
5. Identifying number :	<input type="text" value="56252526255625"/>
6. Type of Identifier :	<input checked="" type="checkbox"/> ID <input type="checkbox"/> Passport <input type="checkbox"/> Other <input type="text" value="Book"/>
7. Is there a photograph or other image of the person available?	<input checked="" type="radio"/> Yes <input type="radio"/> No
8. Street Address :	<input type="text" value="91 Cain Street"/>
9. City :	<input type="text" value="Pretoria"/>
10. Postal Code :	<input type="text" value="0001"/>
11. Country of Residence :	<input type="text" value="South Africa"/>
12. Contact Telephone Number :	<input type="text" value="01155252526"/>
13. Person's Occupation :	<input type="text" value="Law yer"/>

Completing Part F: Particulars of suspicious activity

- 6.66 Part F requires the reporter to explain what had led them to believe that there was something suspicious about the transaction. In this Part the reporter must describe the events which led to the forming of the conclusion that the situation which is reported is suspicious. The reporter must also provide the reasons for forming this conclusion. The more information the reporter provides to explain the basis of the suspicion, the more it will enhance the Centre's ability to analyse the reported information. The ideal response would clearly and completely describe all of the factors or unusual circumstances which led the reporter to a suspicion of proceeds of an unlawful activity, and would provide as many relevant details as possible to support this determination.
- 6.67 Please do not leave out information about the description of a suspicious situation or try to incorporate information by referring to any other files, documents, etc. The Centre may not be able to access that information unless the reporter provides the details in the STR.

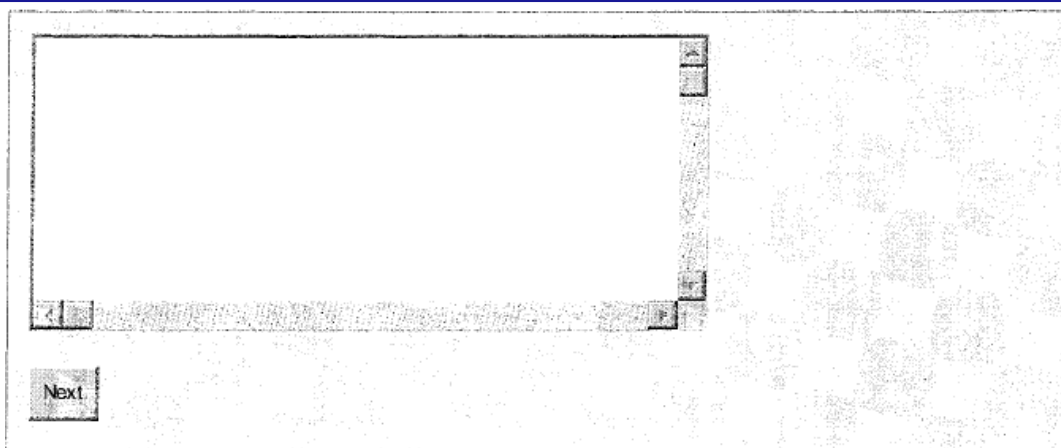
(Please describe clearly and completely the events which led to the forming of the conclusion that the relevant activity is suspicious and state the reasons for this conclusion being formed)



Next

Completing Part G: Particulars of action taken

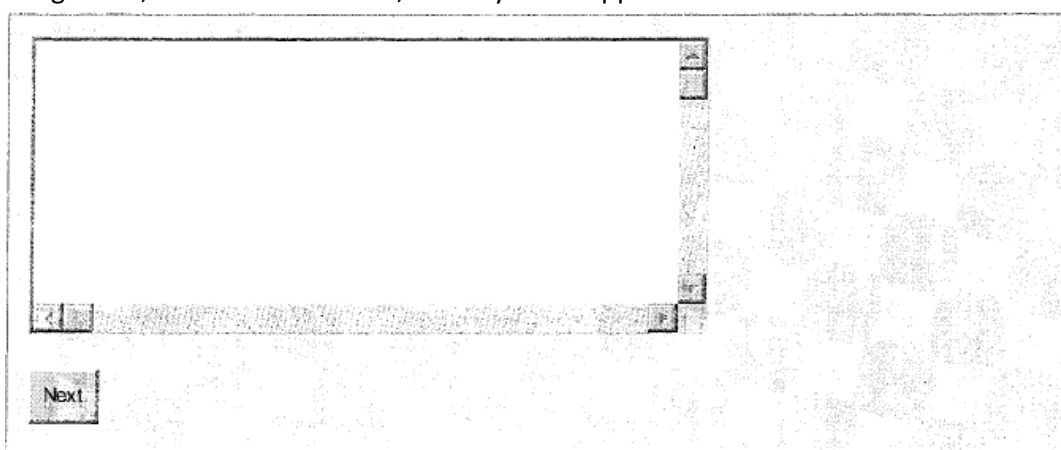
- 6.68 Part G requires the reporter to indicate what action, if any, was taken resulting relation to the suspicious situation. In this part the reporter must indicate they did, apart from reporting to the Centre, concerning the suspicious situation, for example:
- carrying out the transaction in accordance with the customer's instructions;
 - submitting a report or complaint to a law enforcement agency;
 - conducting an internal enquiry;
 - suspending a transaction pending an internal enquiry;
 - subjecting the account been to further monitoring;
 - ending the business relationship with the customer.



Next

Completing Part H: list of available documents

- 6.44 Part H requires the reporter to list all available documents that the reporter used to arrive at the suspicion which is being reported. For example all account opening documentation; information required by the institution as part of its transactional obligations, account statements, and any other applicable documentation.



Next

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

Notice No. R. 454 of 2010

1. Definitions
2. Exemption from Regulations made under Act 38 of 2001

Notice No. R. 454 of 2010

Notice No. R. 454
28 May 2010

National Treasury

By virtue of the powers vested in me by section 74 of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001), I, Pravin J Gordhan, Minister of Finance, hereby make the exemptions set out in the Schedule:

Pravin J Gordhan
Minister of Finance

1. Definitions

In this Schedule "the Act" means the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), and any expression to which a meaning has been assigned in the Act shall have that meaning, and—

"prepaid Instrument"

means an instrument that functions as an electronic surrogate for coins and banknotes, representing a claim on the issuer, which is stored on an electronic device such as a chip card or computer memory and which is accepted as a means of payment by persons other than the issuer;

"the Regulations"

means the Money Laundering and Terrorist Financing Control Regulations, 2002, promulgated by Government Notice No. R. 1595 of 20 December 2002 as amended by GN R456 in *Government Gazette* 27580 of 20 May 2005.

2. Exemption from Regulations made under Act 38 of 2001

- (1) This exemption applies to every accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act.
 - (2) Every accountable institution referred to in paragraph (1), above, is exempted, subject to the conditions set out in paragraph (4) below, from compliance with the provisions of—
 - (a) regulations 3 and 4 of the Regulations, concerning the particulars to be obtained and verified in establishing and verifying persons' identities, and
 - (b) section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(h) and 22(1)(i) of the Act in so far as the records referred to in these sections would apply to information relating to the particulars referred to in paragraph (a),in respect of the issuing of a prepaid instrument which meets the characteristics referred to in paragraph (3) by, or on behalf of, the accountable institution, to a client.
 - (3) A prepaid instrument referred to in paragraph (2) in respect of which this exemption applies, is a prepaid Instrument in respect of which—
-

-
- (a) the value of every individual transaction initiated through the use of the prepaid payment instrument cannot exceed R200,00;
 - (b) the available balance cannot exceed R1500,00 at any time;
 - (c) the monthly turn-over of value loaded onto the prepaid instrument cannot exceed R3000,00;
 - (d) can only be used to purchase goods or services in the Republic;
 - (e) the reloading of value to the prepaid instrument to enable use or further use of the prepaid instrument can only be done by means of an online system requiring the client to enter a personal identification number;
 - (f) the use of the prepaid instrument cannot not enable the remittance of funds, the withdrawal of cash or the receipt of cash as part of a transaction for the payment of goods or services or in any other form whatsoever.
 - (4) This exemption is subject to the condition that—
 - (a) an accountable institution which issues a prepaid instrument directly to a client, or on whose behalf a prepaid instrument is issued to a client, applies enhanced measures, over and above its normal procedures, to scrutinise the transaction activity in relation to the use of the prepaid instrument on an ongoing basis with a view to identify and report suspicious and unusual transactions,
 - (b) where prepaid instruments are issued to a clients on behalf of the accountable institution, the accountable institution—
 - (i) establishes and verifies the identities of the persons issuing the prepaid instruments on its behalf as it would for a client in terms of section 22 of the Act, and
 - (ii) applies enhanced measures, over and above its normal procedures, to scrutinise the transaction activity of the person issuing the prepaid instrument in relation the issuing of the prepaid instruments on an ongoing basis with a view to identify and report suspicious and unusual transactions.
 - (5) This exemption shall come into operation on 14 May 2010.

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

Notice No. 471 of 2010

1. Definitions

2. Exemption from Regulations made under Act 38 of 2001

Notice No. 471 of 2010

Notice No. R. 471

4 June 2010

National Treasury

By virtue of the powers vested in me by section 74 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), I, Pravin J Gordhan, Minister of Finance, hereby make the exemptions set out in the Schedule:

Pravin J Gordhan
Minister of Finance

1. Definitions

In this Schedule "the Act" means the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), and any expression to which a meaning has been assigned in the Act shall have that meaning, and—

"prepaid Instrument"

means an instrument that functions as an electronic surrogate for coins and banknotes, representing a claim on the issuer, which is stored on an electronic device such as a chip card or computer memory and which is accepted as a means of payment by persons other than the issuer;

"the Regulations"

means the Money Laundering and Terrorist Financing Control Regulations, 2002, promulgated by Government Notice No. R. 1595 of 20 December 2002 as amended by GN R456 in *Government Gazette* 27580 of 20 May 2005.

2. Exemption from Regulations made under Act 38 of 2001

- (1) This exemption applies to every accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act.
- (2) Every accountable institution referred to in paragraph (1), above, is exempted in respect of the issuing of a prepaid card which meets the characteristics referred to in paragraph (3) by, or on behalf of, the accountable institution to a client, subject to the conditions set out in paragraph (4) below, from compliance with the provisions of—
 - (a) regulations 3, 4, 5 and 6 of the Regulations, concerning the particulars to be obtained and verified in establishing and verifying persons' identities, and
 - (b) section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(h) and 22(1)(i) of the Act in so far as the records referred to in these sections would apply to information relating to the particulars referred to in paragraph (a), and
 - (c) section 22(1)(f)(ii) of the Act in so far as it relates to the party who offers the prepaid card as a means of payment.
- (3) A prepaid card referred to in paragraph (2) in respect of which this exemption applies, is a prepaid card—

-
- (a) in respect of which the value loaded onto the prepaid card cannot exceed R5 000,00;
 - (b) which cannot be reloaded for value to enable use or further use of the prepaid card;
 - (c) which can only be used as a means of payment at a point of sales device in the Republic;
 - (d) in respect of which the loading of value to the prepaid card to enable its use can only be done by means of an electronic transfer of funds from an existing personal identification number based debit or credit card;
 - (e) which cannot be used in any manner to enable the remittance of funds, the withdrawal of cash or the receipt of cash as part of a transaction for the payment of goods or services or in any other form whatsoever, and
 - (f) which will only be valid until 31 August 2010.
- (4) This exemption is subject to the conditions that—
- (a) an accountable institution which issues a prepaid card which meets the characteristics referred to in paragraph (3) directly to a client, or on whose behalf a prepaid instrument is issued to a client, applies enhanced measures, over and above its normal procedures, to scrutinise the transaction activity in relation to the use of the prepaid card on an ongoing basis with a view to identify and report suspicious and unusual transactions;
 - (b) the locations where the prepaid cards which meet the characteristics referred to in paragraph (3) are issued, are only within areas created for this purpose inside the stadia where matches for the 2010 FIFA World Cup are taking place and are accessible only to valid ticket holders and other persons authorised to enter such stadia, and
 - (c) the number of prepaid cards issued per debit or credit card on any particular day are limited to no more than three.
- (5) This exemption shall come into operation on 30 May 2010 and shall expire on 12 July 2010.

Exemption in Terms of Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

Notice No. 560 of 2010

1. Definitions

2. Exemption from Regulations made under Act 38 of 2001

Notice No. 560 of 2010

Notice No. 560

25 June 2010

National Treasury

By virtue of the powers vested in me by section 74 of the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001), I, Pravin J Gordhan, Minister of Finance, hereby make the exemptions set out in the Schedule:

Pravin J Gordhan
Minister of Finance

1. Definitions

In this Schedule "the Act" means the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), and any expression to which a meaning has been assigned in the Act shall have that meaning, and—

"prepaid Instrument"

means an instrument that functions as an electronic surrogate for coins and banknotes, representing a claim on the issuer, which is stored on an electronic device such as a chip card or computer memory and which is accepted as a means of payment by persons other than the issuer;

"the Regulations"

means the Money Laundering and Terrorist Financing Control Regulations, 2002, promulgated by Government Notice No. R. 1595 of 20 December 2002 as amended by GN R456 in *Government Gazette* 27580 of 20 May 2005.

2. Exemption from Regulations made under Act 38 of 2001

- (1) This exemption applies to every accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act.
- (2) Every accountable institution referred to in paragraph (1), above, is exempted, subject to the conditions set out in paragraph (4) below, from compliance with the provisions of—
 - (a) regulations 3 and 4 of the Regulations, concerning the particulars to be obtained and verified in establishing and verifying persons' identities, and
 - (b) section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(h) and 22(1)(i) of the Act in so far as the records referred to in these sections would apply to information relating to the particulars referred to in paragraph (a),in respect of the issuing of a prepaid instrument which meets the characteristics referred to in paragraph (3) by, or on behalf of, the accountable institution, to a client.
- (3) A prepaid instrument referred to in paragraph (2) in respect of which this exemption applies, is a prepaid Instrument In respect of which—
 - (a) the value of every individual transaction initiated through the use of the

-
- (b) prepaid payment instrument cannot exceed R200,00;
 - (b) the available balance cannot exceed R1 500,00 at any time;
 - (c) the monthly turn-over of value loaded onto the prepaid instrument cannot exceed R3 000,00;
 - (d) can only be used to purchase goods or services in the Republic;
 - (e) the reloading of value to the prepaid instrument to enable use or further use of the prepaid instrument can only be done by means of an online system requiring the client to enter a personal identification number;
 - (f) the use of the prepaid instrument cannot enable the remittance of funds, the withdrawal of cash or the receipt of cash as part of a transaction for the payment of goods or services or in any other form whatsoever.
 - (4) This exemption is subject to the condition that—
 - (a) an accountable institution which issues a prepaid instrument directly to a client, or on whose behalf a prepaid instrument is issued to a client, applies enhanced measures, over and above its normal procedures, to scrutinise the transaction activity in relation to the use of the prepaid instrument on an ongoing basis with a view to identify and report suspicious and unusual transactions,
 - (b) where prepaid instruments are issued to a clients on behalf of the accountable institution, the accountable institution—
 - (i) establishes and verifies the identities of the persons issuing the prepaid instruments on its behalf as it would for a client in terms of section 22 of the Act, and
 - (ii) applies enhanced measures, over and above its normal procedures, to scrutinise the transaction activity of the person issuing the prepaid instrument in relation the issuing of the prepaid instruments on an ongoing basis with a view to identify and report suspicious and unusual transactions.
 - (5) This exemption shall come into operation on 28 May 2010.
-



Regulations

www.acts.co.za

Regulations

Money Laundering and Terrorist Financing Control Regulations : Notice No. R. 1595 of 2002

Money Laundering and Terrorist Financing Control Regulations

[Name of regulations substituted by regulation 6 of Notice No. R. 456 of 2005]

Notice No. R. 1595 of 2002

1. Definitions

1A. Prescribed amount of a single transaction

[Repealed] Chapter 1 : Establishment and verification of identity

Chapter 2 : Record-Keeping

Chapter 3 : Client Profile

Chapter 4 : Reporting of suspicious and unusual transactions

Chapter 5 : Measures to Promote Compliance and Appeals

Chapter 6 : Miscellaneous

Annexure

Exemptions

Notice No. R. 1595 of 2002

Notice No. R. 1595

20 December 2002

National Treasury

The Minister of Finance has, in terms of section 77 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), made the regulations set out in the Schedule.

1. Definitions

In these regulations "**the Act**" means the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001), and, unless the context otherwise indicates, any word or expression to which a meaning has been assigned in the Act has that meaning, and –

"cash threshold report"

means a report which must be submitted by accountable and reporting institutions in terms of section 28 of the Act;

[Definition inserted by regulation 2(a) of Notice No. R. 1062 of 2017]

"close corporation"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

"days"

for the purpose of regulation 24, means all days of the week excluding Saturdays, Sundays and public holidays;

[Definition inserted by regulation 2(a) of Notice No. R. 456 of 2005]

"foreign company"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

"guidance"

means guidance issued by the Centre in terms of regulation 28;

[Definition substituted by regulation 2(c) of Notice No. R. 1062 of 2017]

"identification document"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

"manager"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

"property associated with terrorist and related activities"

means property referred to in section 28A(a) and (b) of the Act;

[Definition inserted by regulation 2(b) of Notice No. R. 456 of 2005]

"reporter"

- (a) an accountable institution or reporting institution making a cash threshold report under section 28 of the Act as contemplated in regulation 22C;
- (b) an accountable institution making a terrorist property report under section 28A of the Act as contemplated in regulation 22A; and
- (c) a natural or legal person making a suspicious or unusual transaction report, suspicious or unusual activity report, terrorist financing transaction report of terrorist financing activity report, under section 29 of the Act as contemplated in regulations 23, 23A, 23B or 23C, or other entity on whose behalf such a report is made;

[Definition inserted by regulation 2(d) of Notice No. R. 1062 of 2017]

"South African company"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

"suspicious or unusual transaction or series of transactions"

[Definition deleted by regulation 2(e) of Notice No. R. 1062 of 2017]

"suspicious or unusual activity report"

means a report which must be submitted—

- (a) in terms of section 29(1) of the Act in respect of the proceeds of unlawful activities or money laundering where the report relates to an activity which does not involve a transaction between two or more parties; or
- (b) in terms of section 29(2) of the Act in respect of a transaction or a series of transactions about which inquiries are made, but which has not been concluded;

[Definition inserted by regulation 2(e) of Notice No. R. 1062 of 2017]

"suspicious or unusual transaction report"

means a report which must be submitted in terms of section 29(1) of the Act in respect of the proceeds of unlawful activities or money laundering where the report relates to a transaction or series of transactions between two or more parties;

[Definition inserted by regulation 2(e) of Notice No. R. 1062 of 2017]

"terrorist financing activity report"

- (a) in terms of section 29(1) of the Act in respect of the financing of terrorism and related activities where the report relates to an activity which does not involve a transaction between two or more parties, or
- (b) in terms of section 29(2) of the Act in respect of a transaction or a series of transactions about which inquiries are made, but which has not been concluded;

[Definition inserted by regulation 2(e) of Notice No. R. 1062 of 2017]

"terrorist financing transaction report"

means a report which must be submitted in terms of section 29(1) of the Act in relation to the financing of terrorism and related activities where the report relates to a transaction or series of transactions between two or more parties;

[Definition inserted by regulation 2(e) of Notice No. R. 1062 of 2017]

"terrorist property report"

means a report which must be submitted in terms of section 28A of the Act;

[Definition inserted by regulation 2(e) of Notice No. R. 1062 of 2017]

"the Amendment Act"

means the Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008);

[Definition inserted by regulation 2 of Notice No. 1107 of 2010]

"trust"

[Definition deleted by regulation 2(b) of Notice No. R. 1062 of 2017]

1A. Prescribed amount of a single transaction

- (1) For the purposes of the definition of a single transaction as contemplated in the Act, the prescribed value of a transaction is an amount not less than R5 000,00.

[Section 1A inserted by regulation 3 of Notice No. R. 1062 of 2017]

[Repealed] Chapter 1 : Establishment and verification of identity

[Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 1 : Introduction

[Repealed] Part 2 : Natural Persons

[Repealed] Part 3 : Legal Persons

[Repealed] Part 4 : Partnerships

[Repealed] Part 5 : Trusts
[Repealed] Part 6 : General

[Repealed] Part 1 : Introduction

[Part 1 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

2. [Repealed] Introductory

2. [Repealed] Introductory

[Regulation 2 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 2 : Natural Persons

[Part 2 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

3. [Repealed] Information concerning South African citizens and residents
4. [Repealed] Verification of information concerning South-African citizens and residents
5. [Repealed] Information concerning foreign nationals
6. [Repealed] Verification of information concerning foreign nationals

3. [Repealed] Information concerning South African citizens and residents

[Regulation 3 repealed by regulation 4 of Notice No. R. 1062 of 2017]

4. [Repealed] Verification of information concerning South-African citizens and residents

[Regulation 4 repealed by regulation 4 of Notice No. R. 1062 of 2017]

5. [Repealed] Information concerning foreign nationals

[Regulation 5 repealed by regulation 4 of Notice No. R. 1062 of 2017]

6. [Repealed] Verification of information concerning foreign nationals

[Regulation 6 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 3 : Legal Persons

[Part 3 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

- 7. [Repealed] Information concerning close corporations and South African companies
- 8. [Repealed] Verification of information concerning close corporations and South African compa
- 9. [Repealed] Information concerning foreign companies
- 10. [Repealed] Verification of information concerning foreign companies
- 11. [Repealed] Information concerning other legal persons
- 12. [Repealed] Verification of information concerning other legal persons

7. [Repealed] Information concerning close corporations and South African companies

[Regulation 7 repealed by regulation 4 of Notice No. R. 1062 of 2017]

8. [Repealed] Verification of information concerning close corporations and South African compa

[Regulation 8 repealed by regulation 4 of Notice No. R. 1062 of 2017]

9. [Repealed] Information concerning foreign companies

[Regulation 9 repealed by regulation 4 of Notice No. R. 1062 of 2017]

10. [Repealed] Verification of information concerning foreign companies

[Regulation 10 repealed by regulation 4 of Notice No. R. 1062 of 2017]

11. [Repealed] Information concerning other legal persons

[Regulation 11 repealed by regulation 4 of Notice No. R. 1062 of 2017]

12. [Repealed] Verification of information concerning other legal persons

[Regulation 12 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 4 : Partnerships

[Part 4 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

13. [Repealed] Information concerning partnerships

14. [Repealed] Verification of information concerning partnerships

13. [Repealed] Information concerning partnerships

[Regulation 13 repealed by regulation 4 of Notice No. R. 1062 of 2017]

14. [Repealed] Verification of information concerning partnerships

[Regulation 14 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 5 : Trusts

[Part 5 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]

15. [Repealed] Information concerning trusts

16. [Repealed] Verification of information concerning trusts

15. [Repealed] Information concerning trusts

[Regulation 15 repealed by regulation 4 of Notice No. R. 1062 of 2017]

16. [Repealed] Verification of information concerning trusts

[Regulation 16 repealed by regulation 4 of Notice No. R. 1062 of 2017]

[Repealed] Part 6 : General***[Part 6 of Chapter 1 repealed by regulation 4 of Notice No. R. 1062 of 2017]***

- 17. [Repealed] Additional requirements when person acts on authority of another
- 18. [Repealed] Verification in absence of contact person
- 19. [Repealed] Accountable institution maintain correctness of particulars

17. [Repealed] Additional requirements when person acts on authority of another

[Regulation 17 repealed by regulation 4 of Notice No. R. 1062 of 2017]

18. [Repealed] Verification in absence of contact person

[Regulation 18 repealed by regulation 4 of Notice No. R. 1062 of 2017]

19. [Repealed] Accountable institution maintain correctness of particulars

[Regulation 19 repealed by regulation 4 of Notice No. R. 1062 of 2017]**Chapter 2 : Record-Keeping**

20. Particulars of third parties keeping records

20. Particulars of third parties keeping records

If an accountable institution appoints a third party to keep on its behalf any records which that institution must retain in terms of the Act, that institution must without delay provide the Centre and the relevant supervisory body with—

[Words preceding regulation 20(a) substituted by regulation 5 of Notice No. R. 1062 of 2017]

- (a) the third party's—
 - (i) full name, if the third party is a natural person; or
 - (ii) registered name, if the third party is a close corporation or company;
 - (b) the name under which the third party conducts business;
 - (c) the full name and contact particulars of the individual who exercises control over access to those records;
 - (d) the address where the records are kept;
 - (e) the address from where the third party exercises control over the records; and
 - (f) 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.

[Repealed] Chapter 3 : Client Profile

[Chapter 3 repealed by regulation 6 of Notice No. R. 1062 of 2017]

21. [Repealed] Information to identify proceeds of unlawful activities or money laundering activities

21. [Repealed] Information to identify proceeds of unlawful activities or money laundering acti

[Regulation 21 repealed by regulation 6 of Notice No. R. 1062 of 2017]

Chapter 4 : Reporting

[Chapter 4 heading substituted by regulation 7 of Notice No. R. 1062 of 2017]

22. Manner of reporting

22A. Information to be reported concerning a terrorist property report

22B. Prescribed amount for cash transaction reporting

22C. Information to be reported concerning a cash threshold report

23. Information to be reported

23A. Information to be reported concerning a suspicious or unusual activity report

23B. Information to be reported concerning a terrorist financing transaction report

23C. Information to be reported concerning a terrorist financing activity report

24. Period for reporting

24A. Manner in which and period within additional information to be furnished

22. Manner of reporting

- (1) Subject to subregulation (2), a report made under Part 3 of Chapter 3 of the Act must be made in accordance with the format specified by the Centre, and sent to the Centre electronically by means of—
 - (a) the internet-based reporting portal provided by the Centre for this purpose at the following internet address: <http://www.fic.gov.za>, or
 - (b) a method developed by the Centre for this purpose and made available to a person who is required to make such reports.
 - (2) If a person who is required to make a report under Part 3 of Chapter 3 of the Act—
 - (a) does not have the technical capability to make a report in accordance with the subregulation (1), or
 - (b) is for another reason indefinitely unable to make a report in accordance with subregulation (1),
-

that person shall make the report on a form specified by the Centre from time to time for this purpose and provide it to the Centre at the contact particulars specified by the Centre from time to time for this purpose.

[Regulation 22 substituted by regulation 8 of Notice No. R. 1062 of 2017]

22A. Information to be reported concerning a terrorist property report

[Regulation 22A heading substituted by regulation 9 of Notice No. R. 1062 of 2017]

- (1) When a reporter makes a terrorist property report, the report must contain full particulars of—
 - (a) the name of the accountable institution making the report;
 - (b) the identifying particulars of the accountable institution on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the accountable institution on whose behalf the report is made;
 - (d) the type of business or economic sector of the accountable institution on whose behalf the report is made;
 - (e) the surname, first name and date of birth of a contact person;
 - (f) the contact particulars of a contact person; and
 - (g) if the contact person mentioned in paragraph (e) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
- (2) In respect of the property concerning which a terrorist property report is made, the report must contain—
 - (a) full particulars of—
 - (i) the type of property concerned; and
 - (ii) a description of the property; and
 - (b) as much of the following information as is readily available—
 - (i) any identifying particulars concerning the property;
 - (ii) the estimated value of the property;
 - (iii) the physical address where the property is located; and
 - (iv) if the property was disposed of, the value of the disposition.
- (3) In respect of a person or entity exercising control over the property on behalf of the accountable institution making a terrorist report, the report must contain full particulars of—
 - (a) the name of the person or entity;
 - (b) the identifying particulars of the person or entity including an identity number or a registration or license number;
 - (c) the contact address of the person or entity;
 - (d) in the case of a natural person, the person's contact particulars;
 - (e) in the case of a legal person or an entity, the surname, first name and contact

-
- particulars of a contact person; and
 - (f) if the contact person mentioned in paragraph (d) or (e) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
 - (4) In respect of every person who, according to the knowledge of the accountable institution making a terrorist property report, may have an interest in the property, the report must contain as much of the following information as is readily available—
 - (a) in the case of a natural person—
 - (i) the person's title, gender, names and surname;
 - (ii) the person's identifying number, nationality and date of birth;
 - (iii) the source of identifying information from which the particulars referred to in subparagraphs (i) and (ii) were obtained;
 - (iiiA) the person's alias, if any;
 - (iv) the person's contact address in the Republic;
 - (v) the person's country of residence;
 - (vi) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (vii) the person's contact number;
 - (viii) the person's occupation;
 - (ix) the source of the funds with which the person acquired the interest in the property;
 - (x) the person's income tax number; and
 - (xi) the employer's name, contact address and contact particulars; and
 - (b) in the case of an legal person or other entity, full particulars of—
 - (i) the person's or entity's name;
 - (ii) the person's or entity's identifying number, if it has such a number;
 - (iii) the person's or entity's contact address in the Republic;
 - (iv) the type of business conducted by the person or entity;
 - (v) the person's or entity's country of origin;
 - (vi) if the country of origin is other than the Republic, the person or entity's contact address in the country of origin;
 - (vii) the source of the funds with which the person or entity acquired the interest in the property; and
 - (viii) in the case of a company, the information referred to in 4(a)(i) to (xi) in respect of at least one director of that company and the role of such person in that company.
 - (5) A terrorist property report must contain a description of the grounds on which the accountable institution making the report has reached the conclusion that the entity which owns or controls the property in question, or on whose behalf, or at whose direction, the property in question is owned or controlled, is an entity referred to in subsection (1)(a) or (b) of section 28A of the Act and the action taken by such accountable institution in respect thereof.
 - (6) A terrorist property report must contain an indicator or indicators in respect of the
-

circumstances that gave rise to the submission of the report.

[Regulation 22A substituted by regulation 9 of Notice No. R. 1062 of 2017]

22B. Prescribed amount for cash transaction reporting

The prescribed amount of cash above which a transaction must be reported to the Centre under section 28 of the Act is R24 999,99 or an aggregate of smaller amounts which combine to come to this amount if it appears to the accountable institution or reporting institution concerned that the transactions involving those smaller amounts are linked to be considered fractions of one transaction.

[Regulation 22B inserted by regulation 2 of Notice No. R. 867 of 2010]

22C. Information to be reported concerning a cash threshold report

[Regulation 22C heading substituted by regulation 10 of Notice No. R. 1062 of 2017]

- (1) When a reporter makes a cash threshold report, the report must contain full particulars of—
 - (a) the name of the accountable or reporting institution making the report;
 - (b) the identifying particulars of the accountable or reporting institution on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the accountable or reporting institution on whose behalf the report is made;
 - (d) the type of business or economic sector of the accountable or reporting institution on whose behalf the report is made;
 - (e) ***[Regulation 22C(1)(e) deleted by Notice No. R. 1062 of 2017]***
 - (f) in the case of a legal or entity, the surname, first name, date of birth and contact particulars of a contact person; and
 - (g) if the person mentioned in paragraph (f) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
 - (2) In respect of the transaction or series of aggregated transactions for which a cash threshold report is made, the report must contain—
 - (a) full particulars of—
 - (i) the location where—
 - (aa) the transaction, or
 - (bb) in the case of a series of aggregated transactions, each of the aggregated transactions, took place;
-

-
- (ii)
 - (aa) the date of the transaction; or
 - (bb) in the case of a series of aggregated transactions, date of the first and last transactions in the series;
 - (iii) the value of—
 - (aa) the transaction; or
 - (bb) in the case of a series of aggregated transactions, each of the aggregated transactions, in local currency; and
 - (iv) a description of how the transaction or series of aggregated transactions was conducted; and
 - (b) as much information as is readily available concerning the currency in which the funds were disposed of.
- (3) In respect of each natural person conducting the transaction or series of aggregated transactions or legal person or other entity on whose behalf the transaction or series of transactions is conducted, for which a cash threshold report is made, the report must contain as much of the following information as is readily available—
- (a) in the case of a natural person—
 - (i) the person's title, gender, names and surname;
 - (ii) the date of birth of the person, nationality and identification number;
 - (iii) the source of identifying information from which the particulars referred to subparagraphs (i) and (ii) were obtained;
 - (iv) the person's alias, if any;
 - (v) the person's contact address in the Republic;
 - (vi) the person's country of residence;
 - (vii) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (viii) the person's contact number;
 - (ix) the person's occupation;
 - (x) the person's source of funds;
 - (xi) the person's income tax number; and
 - (xii) the employer's name, contact address and contact particulars;
 - (b) in the case of a legal person or other entity—
 - (i) the person's or entity's name;
 - (ii) the person's or entity's identifying number, if it has such a number;
 - (iii) information in paragraph (a) of the natural person with authority to conduct the transaction on behalf of the person or entity; and
 - (iv) in the case of a company, the information referred to in paragraph (a), in respect of at least one director of that company and the role of such person in that company; or
 - (c) in the case another entity, any information which is readily available.
- (4) A cash threshold report must contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report.

[Regulation 22C substituted by Notice No. R. 1062 of 2017]

23. Information to be reported

- (1) When a reporter makes a suspicious or unusual transaction report, the report must contain full particulars of—
 - (a) the name of the natural or legal person making the report or entity on whose behalf the report is made;
 - (b) the identifying particulars of the person or entity on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the person or entity on whose behalf the report is made;
 - (d) the type of business or economic sector of the entity on whose behalf the report is made;
 - (e) in the case of a natural person making the report, the person's surname, first name, date of birth and contact particulars;
 - (f) in the case of a legal person or an entity making the report, the person's surname, first name, date of birth and contact particulars of a contact person who may be contacted in relation to the report; and
 - (g) if the person mentioned in paragraph (e) or (f) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
 - (2) In respect of the transaction or series of transactions concerning which a suspicious or unusual transaction report is made, the report must contain—
 - (a) full particulars of—
 - (i) the location where—
 - (aa) the transaction, or
 - (bb) in the case of a series of transactions, each of the transactions in that series,took place;
 - (ii) the date of the transaction, or, in the case of a series of transactions, the period over which the transactions were conducted;
 - (iii) a description of how the transaction or series of transactions were conducted;
 - (iv) if the transaction or series of transactions involved property comprising money, the amount in local currency; and
 - (v) if the transaction or series of transactions involved property other than money, a description of the type of property and all identifying characteristics of the property; and
 - (b) as much of the following information as is readily available—
 - (i) if the transaction or series of transactions involved property the estimated value of the property;
 - (ii) if the property involved in the transaction or series of transactions was disposed of—
 - (aa) the manner in which it was disposed of;
 - (bb) the amount of the disposition, in the case of property comprising money;
-

-
- (cc) the currency of the disposition, in the case of property comprising money;
 - (dd) the value for which the property was disposed of, in the case of property other than money; and
 - (ee) the currency used in the disposition of the property, in the case of property other than money;
 - (iii) if another institution or person was involved in the transaction or series of transactions—
 - (aa) the name of the other institution or person; and
 - (bb) the number of any account at the other institution involved in the transaction or series of transactions;
 - (iv) the name and identifying particulars of the branch or office where the transaction or series of transactions was conducted; and
 - (v) any remarks, comments, reasons or explanations which the person conducting the transaction or series of transactions may have made or given.
 - (3) If any account held at the reporter was involved in the transaction or series of transactions concerning which a suspicious or unusual transaction report is made, the report must contain—
 - (a) full particulars in respect of each account, of—
 - (i) the account number;
 - (ii) the name and identifying particulars of the branch or office where each account is held;
 - (iii) the type of account;
 - (iv) the currency in which this account is denominated;
 - (v) the date on which the account was opened;
 - (vi) the reference numbers allocated by the Centre and the reporter to any previous reports made in connection with the account;
 - (vii) the balance in the account on the date on which the report is made; and
 - (viii) the status of the account immediately before the reported transaction or series of transactions was carried out; and
 - (b) as much of the following information as is readily available in respect of each such account—
 - (i) if the account was closed the date on which the account was closed;
 - (ii) the balance in the account immediately before the transaction or series of transactions was carried out; and
 - (iii) in respect of each signatory on the account—
 - (aa) the person's title, gender, names and surname;
 - (bb) the person's identifying number, nationality and date of birth;
 - (cc) the source of identifying information from which the particulars referred to in subparagraphs (aa) and (bb) were obtained;
 - (dd) the person's alias, if any;
 - (ee) the person's contact address in the Republic;
 - (ff) the person's country of residence;
 - (gg) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (hh) the person's contact number;
 - (jj) the person's occupation;
-

-
- (kk) the source of funds of the person;
 - (ll) the person's income tax number;
 - (mm) the person's employer's name, contact address and contact particulars; and
 - (nn) the role of such signatory.
 - (3A) In respect of each holder of each account referred to in subregulation (3), the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title, gender, nationality and alias, if any;
 - (bb) the person's contact address in the Republic;
 - (cc) the person's country of residence;
 - (dd) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ee) the person's contact number;
 - (ff) the person's occupation;
 - (gg) the person's source of funds;
 - (hh) the person's income tax number; and
 - (ii) the person's employer's name, contact address and contact particulars; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person's or entity's contact address in the country of incorporation or origin;
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date when it was closed; and
 - (gg) the tax number of the person or entity.
 - (4) In respect of each client of the reporter, concerning whom a suspicious or unusual transaction report is made, the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available
 - (aa) the person's alias, if any;
-

-
- (bb) the person's country of residence;
 - (cc) if the person's country of residence is the Republic, the person's contact address in the Republic;
 - (dd) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ee) the person's contact number;
 - (ff) the person's occupation;
 - (gg) the person's source of funds;
 - (hh) the person's income tax number; and
 - (ii) the person's employer's name, contact address and contact particulars; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the type of business conducted by the person or entity;
 - (bb) the names of the natural person's with authority to conduct the transaction on behalf of the person or entity;
 - (cc) the person's or entity's country of incorporation or origin and contact address;
 - (dd) if the country of incorporation or origin is other than the Republic, the person or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company.
 - (5) In respect of a natural person conducting a transaction or series of transactions concerning which a suspicious or unusual transaction report is made, on behalf of another natural person or a legal person or other entity, the report must contain as much of the following information as is readily available—
 - (a) the person's title, gender, names and surname;
 - (b) the person's identifying number, nationality and date of birth;
 - (c) the source of identifying information from which the particulars referred to in subparagraphs (a) and (b) were obtained;
 - (d) the person's contact address in the Republic;
 - (e) the person's contact number;
 - (f) the person's occupation;
 - (g) the person's country of residence;
 - (h) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (i) the person's alias, if any;
 - (j) the person's source of funds;
 - (k) the person's income tax number; and
 - (l) the person's employer's name, contact address and contact particulars.
 - (6) A suspicious or unusual transaction report must—
 - (a) contain a full description of the suspicious or unusual transaction or series of transactions, including the reason why it is deemed to be suspicious or
-

- unusual as contemplated in section 29;
- (b) indicate what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the transaction or series of transactions concerning which the report is made; and
- (c) contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report.

[Regulation 23 substituted by regulation 11 of Notice No. R. 1062 of 2017]

23A. Information to be reported concerning a suspicious or unusual activity report

- (1) When a reporter makes a suspicious or unusual activity report, the report must contain full particulars of—
 - (a) the name of the natural or legal person making the report or entity on whose behalf the report is made;
 - (b) the identifying particulars of the person or entity on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the person or entity on whose behalf the report is made;
 - (d) the type of business or economic sector of the entity on whose behalf the report is made;
 - (e) in the case of a natural person who is making the report, the person's surname, first name, date of birth and contact particulars;
 - (f) in the case of a legal person or an entity making the report, the surname, first name, date of birth and contact particulars of a contact person who may be contacted in relation to the report; and
 - (g) if the person mentioned in paragraph (e) or (f) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
- (2) In respect of the activity concerning which a suspicious or unusual activity report is made, the report must contain as much of the following information as is readily available—
 - (a) the location where the suspicious or unusual activity took place;
 - (b) the date on which the suspicious or unusual activity took place;
 - (c) a description of how the suspicious or unusual activity was conducted;
 - (d) if the suspicious or unusual activity involved property comprising money, the amount in local currency;
 - (e) if the suspicious or unusual activity involved property other than money, a description of the type of property, all identifying characteristics of the property and the estimated value of the property;
 - (f) if the property involved in the suspicious or unusual activity were disposed of—
 - (i) the manner in which it was disposed of;

-
- (ii) the amount of the disposition, in the case of property comprising money;
 - (iii) the currency of the disposition, in the case of property comprising money;
 - (iv) the value for which the property was disposed of, in the case of property other than money; and
 - (v) the currency used in the disposition, in the case of property other than money;
 - (g) if another institution or person was involved in the suspicious or unusual activity—
 - (i) the name of the other institution or person; and
 - (ii) the number of any account at the other institution involved in the suspicious or unusual activity;
 - (h) the name and identifying particulars of the branch or office where the suspicious or unusual activity was conducted; and
 - (i) any remarks, comments, reasons or explanations which the person conducting the suspicious or unusual activity may have made or given.
- (3) If any account held at the reporter was involved in the suspicious or unusual activity concerning which a suspicious or unusual activity report is made, then the report must contain as much of the following information as is readily available in respect of each such account—
- (a) the account number;
 - (b) the name and identifying particulars of the branch or office where each account is held;
 - (c) the type of account;
 - (d) the currency in which this account is denominated;
 - (e) the date on which the account was opened;
 - (f) the balance in the account on the date on which the report is made;
 - (g) the status of the account immediately before the reported activity was carried out;
 - (h) if the account was closed the date on which the account was closed; and
 - (i) in respect of each signatory on the account—
 - (i) the person's title, gender, names and surname;
 - (ii) the person's identifying number, nationality and date of birth;
 - (iii) the source of identifying information from which the particulars referred to in subparagraphs (i) and (ii) were obtained;
 - (iv) the person's alias, if any;
 - (v) the person's contact address in the Republic;
 - (vi) the person's country of residence;
 - (vii) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (viii) the person's contact number;
 - (ix) the person's occupation;
 - (x) the source of funds of the person;
 - (xi) the person's income tax number;
 - (xii) the person's employer's name, contact address and contact particulars; and
 - (xiii) the role of such signatory.
- (4) In respect of each account referred to in subregulation (3), the report must contain—
-

-
- (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title and gender;
 - (bb) the person's alias, if any;
 - (cc) the person's contact address in the Republic;
 - (dd) the person's country of residence;
 - (ee) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ff) the person's contact number;
 - (gg) the person's occupation;
 - (hh) the source of funds of the person;
 - (ii) the person's income tax number;
 - (jj) the person's employer's name, contact address and contact particulars; and
 - (kk) the source of identifying information from which the particulars referred to in subparagraphs (aa) and (bb) were obtained and the issuing country; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person's or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date on which it was closed; and
 - (gg) the tax number of the person or entity.
 - (5) In respect of each client of the reporter concerning whom a suspicious or unusual activity report is made, the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number, and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title and gender;
 - (bb) the person's alias, if any;
 - (cc) the person's country of residence;
 - (dd) if the person's country of residence is the Republic, the person's contact address in the Republic;
-

- (ee) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ff) the person's contact number;
 - (gg) the person's occupation;
 - (hh) the source of funds of the person;
 - (ii) the person's income tax number;
 - (jj) the person's employer's name, contact address and contact particulars;
 - (kk) the source of identifying information from which the particulars referred to in subparagraph (a)(i)(aa) and (a)(i)(bb) were obtained; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date when it was closed; and
 - (gg) the tax number of the person or entity.
- (6) In respect of a natural person conducting a suspicious or unusual activity concerning which a suspicious or unusual activity report is made, on behalf of another natural person or a legal person or other entity, the report must contain as much of the following information as is readily available—
 - (a) the person's title, gender, names and surname;
 - (b) the person's identifying number, nationality and date of birth;
 - (c) the source of identifying information from which the particulars referred to in subparagraph (a) and (b) were obtained;
 - (d) the person's alias, if any;
 - (e) the person's contact address in the Republic;
 - (f) the person's country of residence;
 - (g) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (h) the person's contact number;
 - (i) the person's occupation;
 - (j) the source of funds of the person;
 - (k) the person's income tax number; and
 - (l) the person's employer's name, contact address and contact particulars.
- (7) A suspicious or unusual activity report must—
 - (a) contain a full description of the suspicious or unusual activity, including the

- reason why it is deemed to be suspicious or unusual as contemplated in section 29;
- (b) indicate what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the suspicious or unusual activity concerning which the report is made;
 - (c) contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report; and
 - (d) contain the reference numbers allocated by the Centre and the reporter to any previous reports made.

[Regulation 23A inserted by regulation 12 of Notice No. R. 1062 of 2017]

23B. Information to be reported concerning a terrorist financing transaction report

- (1) When a reporter makes a terrorist financing transaction report, the report must contain full particulars of—
 - (a) the name of the natural or legal person making the report or entity on whose behalf the report is made;
 - (b) the identifying particulars of the person or entity on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the person or entity on whose behalf the report is made;
 - (d) the type of business or economic sector of the entity on whose behalf the report is made;
 - (e) in the case of a natural person making the report, the person's surname, first name, date of birth and contact particulars;
 - (f) in the case of a legal person or an entity making the report, the surname, first name, date of birth and contact particulars of a contact person who may be contacted in relation to the report;
 - (g) if the person mentioned in paragraph (e) or (f) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the source of identifying information from which the particulars referred to were obtained and the issuing country thereof.
- (2) In respect of the transaction or series of transactions concerning which a terrorist financing transaction report is made, the report must contain—
 - (a) full particulars of—
 - (i) the location where—
 - (aa) the transaction; or
 - (bb) in the case of a series of transactions, each of the transactions in that series, took place;
 - (ii) the date of the transaction, or, in the case of a series of transactions, the period over which the transactions were conducted;
 - (iii) a description of how the transaction or series of transactions were

-
- conducted;
 - (iv) if the transaction or series of transactions involved property comprising money, the amount in local currency; and
 - (v) if the transaction or series of transactions involved property other than money, a description of the type of property and all identifying characteristics of the property; and
 - (b) as much of the following information as is readily available—
 - (i) if the transaction or series of transactions involved property, the estimated value of the property;
 - (ii) if the property involved in the transaction or series of transactions were disposed of—
 - (aa) the manner in which it was disposed of;
 - (bb) the amount of the disposition, in the case of property comprising money;
 - (cc) the currency of the disposition, in the case of property comprising money;
 - (dd) the value for which the property was disposed of, in the case of property other than money; and
 - (ee) the currency used in the disposition, in the case of property other than money;
 - (iii) if another institution or person was involved in the transaction or series of transactions—
 - (aa) the name of the other institution or person; and
 - (bb) the number of any account at the other institution involved in the transaction or series of transactions;
 - (iv) the name and identifying particulars of the branch or office where the transaction or series of transaction was conducted; and
 - (v) any remarks, comments, reasons or explanations which the person conducting the transaction or series of transactions may have made or given.
 - (3) If any account held at the reporter was involved in the transaction or series of transactions concerning which a terrorist financing transaction report is made, the report must contain—
 - (a) full particulars in respect of each such account, of—
 - (i) the account number;
 - (ii) the name and identifying particulars of the branch or office where each account is held;
 - (iii) the type of account;
 - (iv) the currency in which this account is denominated;
 - (v) the date on which the account was opened;
 - (vi) the reference numbers allocated by the Centre and the reporter to any previous reports made in connection with the account;
 - (vii) the balance in the account on the date on which the report is made; and
 - (viii) the status of the account immediately before the reported transaction or series of transactions was carried out; and
 - (b) as much of the following information as is readily available in respect of each such account—
 - (i) if the account was closed the date on which the account was closed;
 - (ii) the balance in the account immediately before the transaction or
-

-
- series of transactions was carried out; and
 - (iii) in respect of each signatory on the account—
 - (aa) the person's title, gender, names and surname;
 - (bb) the person's identifying number, nationality and date of birth;
 - (cc) the source of identifying information from which the particulars referred to in subparagraphs (aa) and (bb) were obtained;
 - (dd) the person's alias, if any;
 - (ee) the person's contact address in the Republic;
 - (ff) the person's country of residence;
 - (gg) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (hh) the person's contact number;
 - (ii) the person's occupation;
 - (jj) the source of funds of the person;
 - (kk) the person's income tax number;
 - (ll) the person's employer's name, contact address and contact particulars; and
 - (mm) the role of such signatory.
 - (4) In respect of each holder of each account referred to in subregulation (3), the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title, gender, nationality and alias, if any;
 - (bb) the person's contact address in the Republic;
 - (cc) the person's country of residence;
 - (dd) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ee) the person's contact number;
 - (ff) the person's occupation;
 - (gg) the person's source of funds;
 - (hh) the person's income tax number; and
 - (ii) the person's employer's name, contact address and contact particulars; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person's or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in
-

-
- paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date on which it was closed; and
 - (gg) the tax number of the person or entity.
 - (5) In respect of each client of the reporter concerning whom a terrorist financing report is made, the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number, and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's alias, if any;
 - (bb) the person's country of residence;
 - (cc) if the person's country of residence is the Republic, the person's contact address in the Republic;
 - (dd) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ee) the person's contact number;
 - (ff) the person's occupation;
 - (gg) the source of funds of the person;
 - (hh) the person's income tax number; and
 - (ii) the person's employer's name, contact address and contact particulars; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the type of business conducted by the person or entity;
 - (bb) the names of the natural person with authority to conduct the transaction on behalf of the person or entity;
 - (cc) the person's or entity's country of incorporation or origin and contact address;
 - (dd) if the country of incorporation or origin is other than the Republic, the person's or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (6) In respect of a natural person conducting a transaction or series of transactions concerning which a terrorist financing transaction report is made, on behalf of another natural person or a legal person or other entity, the report must contain as much of the following information as is readily available—
 - (a) the person's title, gender, names and surname;
 - (b) the person's identifying number, nationality and date of birth;
 - (c) the source of identifying information from which the particulars referred to in subparagraph (a) and (b) were obtained;
-

-
- (d) the person's alias, if any;
 - (e) the person's contact address in the Republic;
 - (f) the person's country of residence;
 - (g) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (h) the person's contact number;
 - (i) the person's occupation;
 - (j) the person's source of funds;
 - (k) the person's income tax number; and
 - (l) the person's employer's name, contact address and contact particulars.
- (7) A terrorist financing transaction report must—
- (a) contain a full description of the terrorist financing transaction or series of transactions, including the reason why it is deemed to be suspicious or unusual as contemplated in section 29;
 - (b) indicate what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the transaction or series of transactions concerning which the report is made; and
 - (c) contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report.

[Regulation 23B inserted by regulation 12 of Notice No. R. 1062 of 2017]

23C. Information to be reported concerning a terrorist financing activity report

- (1) When a reporter makes a terrorist financing activity report, the report must contain full particulars of—
- (a) the name of the natural or legal person making the report or entity on whose behalf the report is made;
 - (b) the identifying particulars of the person or entity on whose behalf the report is made including a registration or license number;
 - (c) the contact address of the person or entity on whose behalf the report is made;
 - (d) the type of business or economic sector of the entity on whose behalf the report is made;
 - (e) in the case of a natural person who is making the report, the person's surname, first name, date of birth and contact particulars;
 - (f) in the case of a legal person or an entity making the report, the surname, first name, date of birth and contact particulars of a contact person who may be contacted in relation to the report; and
 - (g) if the person mentioned in paragraph (e) or (f) is—
 - (i) a South African citizen or resident, the identifying particulars of that person and the source of identifying information from which the particulars were obtained; or
 - (ii) not a South African citizen or resident, the identifying particulars of that contact person and the of identifying information from which the particulars referred to were obtained and the issuing country thereof.
- (2) In respect of the activity concerning which a terrorist financing activity report is made,
-

-
- the report must contain as much of the following information as is readily available—
- (a) the location where the activity took place;
 - (b) the date on which the activity took place;
 - (c) a description of how the activity was conducted;
 - (d) if the activity involved property comprising money, the amount in local currency;
 - (e) if the activity involved property other than money, a description of the type of property, all identifying characteristics of the property and the estimated value of the property;
 - (f) if the property involved in the activity were disposed of—
 - (i) the manner in which it was disposed of;
 - (ii) the amount of the disposition, in the case of property comprising money;
 - (iii) the currency of the disposition, in the case of property comprising money;
 - (iv) the value for which the property was disposed of, in the case of property other than money; and
 - (v) the currency used in the disposition, in the case of property other than money;
 - (g) if another institution or person was involved in the activity—
 - (i) the name of the other institution or person; and
 - (ii) the number of any account at the other institution involved in the activity;
 - (h) the name and identifying particulars of the branch or office where the activity was conducted; and
 - (i) any remarks, comments, reasons or explanations which the person conducting the activity may have made or given.
- (3) If any account held at the reporter was involved in the activity concerning which a terrorist financing activity report is made, then the report must contain as much of the following information as is readily available in respect of each such account—
- (a) the account number;
 - (b) the name and identifying particulars of the branch or office where each account is held;
 - (c) the type of account;
 - (d) the currency in which this account is denominated;
 - (e) the date on which the account was opened;
 - (f) the balance in the account on the date on which the report is made;
 - (g) the status of the account immediately before the reported activity was carried out;
 - (h) if the account was closed the date on which the account was closed; and
 - (i) in respect of each signatory on the account—
 - (i) the person's title, gender, names and surname;
 - (ii) the person's identifying number, nationality and date of birth;
 - (iii) the source of identifying information from which the particulars referred to in subparagraphs (i) and (ii) were obtained;
 - (iv) the person's alias, if any;
 - (v) the person's contact address in the Republic;
 - (vi) the person's country of residence;
 - (vii) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
-

-
- (viii) the person's contact number;
 - (ix) the person's occupation;
 - (x) the source of funds of the person;
 - (xi) the person's income tax number;
 - (xii) the person's employer's name, contact address and contact particulars; and
 - (xiii) the role of such signatory.
 - (4) In respect of each holder of each account referred to in subregulation (3), the report must contain—
 - (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title and gender;
 - (bb) the person's alias, if any;
 - (cc) the person's contact address in the Republic;
 - (dd) the person's country of residence;
 - (ee) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ff) the person's contact number;
 - (gg) the person's occupation;
 - (hh) the person's source of funds;
 - (ii) the person's income tax number; and
 - (jj) the person's employer's name; contact address and contact particulars; and
 - (kk) the source of identifying information from which the particulars referred to in subparagraphs (a)(i)(aa) and (a)(i)(bb) were obtained and the issuing country; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person's or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date on which it was closed; and
 - (gg) the tax number of the person or entity.
 - (5) In respect of each client of the reporter concerning whom a terrorist financing activity report is made, the report must contain—
-

-
- (a) in the case of a natural person—
 - (i) full particulars of—
 - (aa) the person's names and surname;
 - (bb) the person's identifying number and date of birth; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's title and gender;
 - (bb) the person's alias, if any;
 - (cc) the person's country of residence;
 - (dd) if the person's country of residence is the Republic, the person's contact address in the Republic;
 - (ee) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (ff) the person's contact number;
 - (gg) the person's occupation;
 - (hh) the person's source of funds;
 - (ii) the person's income tax number;
 - (jj) the person's employer's name, contact address and contact particulars; and
 - (kk) the source of identifying information from which the particulars referred to in subparagraph (a)(i)(aa) and (a)(i)(bb) were obtained; or
 - (b) in the case of a legal person or other entity—
 - (i) full particulars of—
 - (aa) the person's or entity's name; and
 - (bb) the person's or entity's identifying number, if it has such a number; and
 - (ii) as much of the following information as is readily available—
 - (aa) the person's or entity's contact address in the Republic;
 - (bb) the type of business conducted by the person or entity;
 - (cc) the person's or entity's country of incorporation or origin;
 - (dd) if the country of incorporation or origin is other than the Republic, the person or entity's contact address in the country of incorporation or origin; and
 - (ee) in the case of a company, the information referred to in paragraph (a)(i) and (ii), in respect of at least one director of that company and the role of such person in that company;
 - (ff) if the person or entity has been closed, the date when it was closed; and
 - (gg) the tax number of the person or entity.
- (6) in respect of a natural person conducting an activity concerning which a terrorist financing activity report is made, on behalf of another natural person or a legal person or other entity, the report must contain as much of the following information as is readily available—
- (a) the person's title, gender, names and surname;
 - (b) the person's identifying number, nationality and date of birth;
 - (c) the source of identifying information from which the particulars referred to in subparagraphs (a) and (b) were obtained;
 - (d) the person's alias, if any;
 - (e) the person's contact address in the Republic;
 - (f) the person's country of residence;
-

-
- (g) if the person's country of residence is other than the Republic, the person's contact address in the country of residence;
 - (h) the person's contact number;
 - (i) the person's occupation;
 - (j) the person's source of funds;
 - (k) the person's income tax number; and
 - (l) the person's employer's name, contact address and contact particulars.
- (7) A terrorist financing activity report must—
- (a) contain a full description of the activity which is the subject of the terrorist financing activity report, including the reason why it is deemed to be suspicious or unusual as contemplated in section 29;
 - (b) indicate what action the natural or legal person making the report, or other entity on whose behalf the report is made, has taken in connection with the activity concerning which the report is made;
 - (c) contain an indicator or indicators in respect of the circumstances that gave rise to the submission of the report; and
 - (d) contain the reference numbers allocated by the Centre and the reporter to any previous reports made.

[Regulation 23C inserted by regulation 12 of Notice No. R. 1062 of 2017]

24. Period for reporting

- (1) A report under section 28A of the Act must be sent to the Centre as soon as possible but not later than 5 days after a natural person who is an accountable institution or is in charge of, manages or is employed by an accountable institution, had established that the accountable institution has property associated with terrorist and related activities in its possession or under its control, unless the Centre has approved of the report being sent after the expiry of this period.
- (2) A request for a report referred to in subregulation (1) to be sent to the Centre after the period referred to in that subregulation must reach the Centre before the expiry of that period.
- (3) A report under section 29 of the Act must be sent to the Centre as soon as possible but not later than fifteen days after a natural person or any of his or her employees, or any of the employees or officers of a legal person or other entity, has become aware of a fact concerning a transaction on the basis of which knowledge or a suspicion concerning the transaction must be reported, unless the Centre has approved of the report being sent after the expiry of this period.
- (4) A report under section 28 of the Act must be sent to the Centre as soon as possible but not later than 2 days after a natural person or any of his or her employees, or any of the employees or officers of a legal person or other entity, has become aware of a fact of a cash transaction or series of cash transactions that has exceeded the prescribed limit.

[Regulation (4) inserted by regulation 3 of Notice No. R. 867 of 2010]

[Regulation 24 substituted by regulation 5 of Notice No. R. 456 of 2005]

24A. Manner in which and period within additional information to be furnished

An accountable institution, a reporting institution or any other person that receives a request for additional information from the Centre in terms of section 32 of the Act must, after receiving such request from the Centre and within the number of days specified in the request furnish to the centre the additional information—

- (a) in accordance with the format and content specified by the Centre; and
- (b) electronically by means of the internet-based reporting portal provided by the Centre at the internet address, <http://www.fic.gov.za>, or by any other means specified by the Centre.

[Regulation 24A inserted by regulation 13 of Notice No. R. 1062 of 2017]

Chapter 5 : Measures to Promote Compliance and Appeals

[Chapter 5 heading substituted by regulation 14 of Notice No. R. 1062 of 2017]

25. [Repealed] Internal rules concerning establishment and verification of identities

26. [Repealed] Internal rules concerning the keeping of records

27. [Repealed] Internal rules concerning reporting of information

27A. Period for and manner of registration by accountable institutions and reporting institutions

27B. Period within and manner in which supervisory body must submit written report to Centre

27C. Manner in which appeal is to be lodged and payment of fee

27D. Criteria for supervisory body to request information relating to a report made in terms of section 29

25. [Repealed] Internal rules concerning establishment and verification of identities

[Regulation 25 repealed by regulation 15 of Notice No. R. 1062 of 2017]

26. [Repealed] Internal rules concerning the keeping of records

[Regulation 26 repealed by regulation 15 of Notice No. R. 1062 of 2017]

27. [Repealed] Internal rules concerning reporting of information

[Regulation 27 repealed by regulation 15 of Notice No. R. 1062 of 2017]

27A. Period for and manner of registration by accountable institutions and reporting institutions

- (1) Every accountable institution referred to in Schedule 1 of the Act and every reporting institution referred to in Schedule 3 of the Act must within the period commencing 1 December 2010 until 1 March 2011, register with the Centre in terms of section 43B of the Act.
- (2) Any person or category of persons added to the list in Schedule 1 or Schedule 3 of the Act after the commencement of this regulation must register with the Centre within 90 days after the amended Schedule 1 or Schedule 3 is published by notice in the *Gazette*.
- (3) Any person or category of persons who, on commencing a new business, fall within the list of accountable institutions or reporting institutions in Schedule 1 and Schedule 3 respectively must, within 90 days of the day the business opened, register with the Centre.
- (4) The registration of an accountable institution and a reporting institution contemplated in subregulation (1), (2) and (3) must be in accordance with the format specified by the Centre and must be submitted to the Centre electronically by means of the internet-based reporting portal provided by the Centre for this purpose at the following internet address: <http://www.fic.gov.za>.
- (5) If a person does not have the technical capability to register in accordance with subregulation (4) that person must submit the registration on a form specified by the Centre at the contact particulars specified by the Centre from time to time for this purpose.
- (6) The registration of an accountable institution or a reporting institution is not a licensing process and no license will be issued on the completion of a registration contemplated in subregulation (1), (2) and (3).
- (7) No fee is payable for a registration contemplated in subregulation (1), (2) or (3).

[Regulation 27A inserted by regulation 3 of Notice No. 1107 of 2010]

27B. Period within and manner in which supervisory body must submit written report to Centre

- (1) A supervisory body must, as contemplated in section 45(1C) of the Act, within 30 days after taking a decision to institute an action against an accountable institution in terms of the Act or any order, determination or directive made in terms of the Act submit a written report to the Centre on any action taken or intended to be taken against that
-

accountable institution.

- (2) A supervisory body must submit the written report contemplated in subregulation (1) in accordance with the format specified by the Centre at the contact particulars specified by the Centre for this purpose.

[Regulation 27A inserted by regulation 4 of Notice No. 1107 of 2010]

27C. Manner In which appeal is to be lodged and payment of fee

With regard to an appeal contemplated in section 45D(1) of the Act—

- (a) the appellant must lodge an appeal against a decision of the Centre or supervisory body with the chairperson of the appeal board within 30 days from the date when notice of such decision was received in writing by the appellant;
- (b) the notice of appeal, contemplated in paragraph (a), must be accompanied by an affidavit containing in full the particulars of the appellant, the decision appealed against, the grounds for the appeal and must also state the physical address where the appellant will accept delivery of all documents relevant to the appeal;
- (c) the appellant must deliver the notice of appeal to the address specified on the notice to impose the administrative sanction;
- (d) the appellant must, with the appeal, pay a fee of R10 000-00 to the Centre.

[Regulation 27A inserted by regulation 4 of Notice No. 1107 of 2010]

27D. Criteria for supervisory body to request information relating to a report made in terms of section 29

- (1) For the purposes of section 45B(2A) of the Act, a supervisory body referred to in section 45B(2A)(c) of the Act may only order from an accountable institution under inspection, the production of a copy of a report, or the furnishing of a fact or information related to the report contemplated in section 29 if, to the satisfaction of the Centre—
 - (a) appropriate measures are taken by the supervisory body to ensure that the information obtained from the report is processed only for the purposes of determining compliance with the Act;
 - (b) appropriate measures are taken by the supervisory body to prevent unlawful access to the information contained in the report; and
 - (c) appropriate security safeguards are in place for the protection of information contained in the report.
- (2) The Centre must advise the accountable institution concerned in writing of its decision whether a supervisory body meets the criteria contemplated in subregulation (1).

[Regulation 27D inserted by regulation 16 of Notice No. R. 1062 of 2017]

Chapter 6 : Miscellaneous

- 28. Guidance
- 29. Offences and penalties and administrative sanctions for non-compliance
- 30. Title and commencement

28. Guidance

- (1) The Centre may issue guidance concerning—
 - (a) the application of a risk-based approach to establish and verify the identity of a client;
 - (aA) customer due diligence measures;
 - (aB) the duty to keep records;
 - (aC) financial sanctions;
 - (b) reporting duties;
 - (bA) registration;
 - (bB) any obligations imposed on supervisory bodies under the Act; and
 - (c) any other obligations imposed on accountable institutions under the Act.
- (2) Guidance referred to in subregulation (1) may differ for different accountable institutions or persons, or categories of accountable institutions or persons and different categories of transactions.

[Regulation 28 substituted by regulation 17 of Notice No. R. 1062 of 2017]

29. Offences and penalties and administrative sanctions for non-compliance

- (1) ***[Regulation 29(1) deleted by regulation 29 of Notice No. R. 1062 of 2017]***
 - (2) ***[Regulation 29(2) deleted by regulation 29 of Notice No. R. 1062 of 2017]***
 - (3) ***[Regulation 29(3) deleted by regulation 29 of Notice No. R. 1062 of 2017]***
 - (4) ***[Regulation 29(4) deleted by regulation 29 of Notice No. R. 1062 of 2017]***
 - (5) ***[Regulation 29(5) deleted by regulation 29 of Notice No. R. 1062 of 2017]***
 - (6) Any accountable institution, which fails to inform the Centre or the relevant supervisory body of particulars concerning third parties keeping records in accordance with regulation 20 is non-compliant and is subject to an administrative sanction.
 - (6A) Any person or institution which fails to provide the information to be reported concerning a terrorist property report in accordance with regulation 22A is guilty of an offence.
 - (6B) Any person or institution which fails to provide the information to be reported
-

concerning a terrorist property report in accordance with regulation 22A is non-compliant and is subject to an administrative sanction.

- (6C) Any person or institution which fails to provide the information to be reported concerning a cash threshold report in accordance with regulation 22C is guilty of an offence.
 - (6D) Any person or institution which fails to provide the information to be reported concerning a cash threshold report in accordance with regulation 22C is non-compliant and is subject to an administrative sanction.
 - (6E) Any person or institution which fails to provide the information to be reported concerning a suspicious or unusual transaction report in accordance with regulation 23 is guilty of an offence.
 - (6F) Any person or institution which fails to provide the information to be reported concerning a suspicious or unusual transaction report in accordance with regulation 23 is non-compliant and is subject to an administrative sanction.
 - (6G) Any person or institution which fails to provide the information to be reported concerning a suspicious or unusual activity report in accordance with regulation 23A is guilty of an offence.
 - (6H) Any person or institution which fails to provide the information to be reported concerning a suspicious or unusual activity report in accordance with regulation 23A is non-compliant and is subject to an administrative sanction.
 - (6I) Any person or institution which fails to provide the information to be reported concerning a terrorist financing transaction report in accordance with regulation 23B is guilty of an offence.
 - (6J) Any person or institution which fails to provide the information to be reported concerning a terrorist financing transaction report in accordance with regulation 23B is non-compliant and is subject to an administrative sanction.
 - (6K) Any person or institution which fails to provide the information to be reported concerning a terrorist financing activity report in accordance with regulation 23C is guilty of an offence.
 - (6L) Any person or institution which fails to provide the information to be reported concerning a terrorist financing activity report in accordance with regulation 23C is non-compliant and is subject to an administrative sanction.
 - (7) Any person or institution, which fails to send a report to the Centre within the period referred to in regulation 24 or 24A is non-compliant and is subject to an administrative sanction.
 - (8) ***[Regulation 29(8) deleted by regulation 18 of Notice No. R. 1062 of 2017]***
 - (9) Any person or institution convicted of an offence under this regulation is liable to imprisonment for a period not exceeding three years or a fine not exceeding R1
-

million.

[Regulation 29 substituted by regulation 18 of Notice No. R. 1062 of 2017]

30. Title and commencement

- (1) These regulations are called the Money Laundering and Terrorist Financing Control Regulations.
[Subregulation (1) substituted by regulation 6 of Notice No. R. 456 of 2005]
- (2) Chapter 4 and regulations 29(7) and (9) shall come into operation on 3 February 2003.
- (3) Regulation 1, Chapters 1, 2, 3, and 5 and regulations 28 and 29(1), (2), (3), (4), (5), (6) and (8) shall come into operation on 30 June 2003.

Annexure

Form 1 - Suspicious or Unusual Transaction Report [Deleted]

Form 1 - Suspicious or Unusual Transaction Report [Deleted]

[Form 1 deleted by regulation 7 of Notice No. R. 456 of 2005]

Exemptions

Interpretation

Part 1 : General Exemptions

Part 2 : Exemptions for insurance and investment providers

Part 3 : Exemptions for members of Exchanges

Part 4 : Exemptions for attorneys and administrators of property

Part 5 : Exemptions for estate agents

Part 6 : Exemptions for gambling institutions

Part 7 : Exemptions for banks

Part 8 : Miscellaneous

Exchanges recognised for purposes of the exemption in respect of public companies the securities of which are listed on a stock exchange

Interpretation - Definitions

In this Schedule "the Act" means the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001), and any expression to which a meaning has been assigned in the Act shall have that meaning, and –

"the Regulations"

means the Regulations promulgated by Government Notice R. ... of ... under section 77 of the Act.

Part 1 : General Exemptions**(2) Timing of verification**

Every accountable institution may by, way of exemption from section 21 of the Act, accept a mandate from a prospective client to establish a business relationship or to conclude a single transaction, or take any similar preparatory steps with a view to establishing a business relationship or concluding a single transaction, before the accountable institution verified the identity of that prospective client in accordance with section 21 of the Act, subject to the condition that the accountable institution will have completed all steps which are necessary in order to verify the identity of that client in accordance with section 21 of the Act before the institution—

- (a) concludes a transaction in the course of the resultant business relationship, or
- (b) performs any act to give effect to the resultant single transaction.

(3) Exemption from Parts 1, 2 and 4 of Chapter 3 of Act 38 of 2001

Every natural person who performs the functions of an accountable institution referred to in Schedule 1 to the Act in a partnership with another natural person, or in a company or close corporation is exempted from the provisions of Parts 1, 2 and 4 of Chapter 3 of the Act subject to the condition that those provisions are complied with by another person employed by the partnership, company or close corporation in which he or she practices.

(4) Exemption from section 21 and 22 of the Act 38 of 2001

Every accountable institution is exempted from compliance with the provisions of section 21 and 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act, in respect of a business relationship or single transaction which is established or concluded with that institution (the second accountable institution) by another accountable institution (the primary accountable institution) acting on behalf of a client of that primary accountable institution, subject to the condition that the primary accountable institution confirms in writing to the satisfaction of the second accountable institution that—

- (a) it has established and verified the identity of the client in accordance with section 21 of the Act, or
 - (b) in terms of its internal rules and the procedures ordinarily applied in the course of establishing business relationships or concluding single transactions
-

the primary accountable institution will have established and verified, in accordance with section 21 of the Act, the identity of every client on whose behalf it will be establishing business relationships or conducting concluding single transactions with the second accountable institution.

(5) Exemption from verification obligations under section 21 of the Act

Every accountable institution is exempted from compliance with the provisions of section 21 of the Act which require the verification of the identity of a client of that institution if –

- (a) that client is situated in a country where, to the satisfaction of the relevant supervisory body, anti-money laundering regulation and supervision of compliance with such anti-money laundering regulation, which is equivalent to that which applies to the accountable institution is in force,
- (b) a person or institution in that country, which is subject to the anti-money laundering regulation referred to in paragraph (a) confirms in writing to the satisfaction of the accountable institution that the person or institution has verified the particulars concerning that client which the accountable institution had obtained in accordance with section 21 of the Act, and
- (c) the person or institution referred to in paragraph (b) undertakes to forward all documents obtained in the course of verifying such particulars to the accountable institution.

(6) Exemption from regulations made under Act 38 of 2001

- (1) Every accountable institution is exempted from compliance with regulation 7(c), 7(d), 7(f), 7(g), 7(h), 7(i), 7(j), 8, 9(c), 9(d), 9(e), 9(f), 9(g), 9(h), 9(i), 9(j), 9(k) and 10 of the Regulations, and of section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars referred to in those regulations, in respect of a business relationship established or single transaction concluded with a public company the securities of which are listed on a stock exchange recognised for this purpose and listed in the Schedule to these exemptions.
- (2) Every accountable institution is exempted from compliance with regulation 3(1)(d), 4(2), 5(1)(e), 6(2), 7(h), 8(d), 9(h), 10(c), 11(d), 12(b), 15(c) and 16(b) of the Regulations, and of section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars referred to in those regulations.

Part 2 : Exemptions for insurance and investment providers

7) Exemption from Parts 1 and 2 of Chapter 3 of Act 38 of 2001

- 1) Every accountable institution which performs the functions of an accountable institution referred to in items 5, 8, 12, 17 and 18 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 of the Act in respect of every business relationship or single transaction concerning –

-
- a) any long term insurance policy which is a fund policy or a fund member policy as defined in the Long-term Insurance Act, 1998 and the regulations thereto and in respect of which the policyholder is a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962;
 - b) any unit trust or linked product investment effected by a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962, including an investment made to fund in whole or in part the liability of the fund to provide benefits to members or surviving spouses, children, dependants or nominees of members of the fund in terms of its rules;
 - c) any annuity purchased as a compulsory annuity in terms of the rules of a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962;
 - d) any reinsurance policy issued to another accountable institution;
 - e) any long-term insurance policy classified in terms of the Long-term Insurance Act, 1998 as an assistance policy;
 - f) any long term insurance policy which provides benefits only upon the death, disability, sickness or injury of the life insured under the policy;
 - g) any long-term insurance policy in respect of which recurring premiums are paid which will amount to an annual total not exceeding R25 000,00, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client –
 - i) who increases the recurring premiums so that the amount of R25 000,00 is exceeded;
 - ii) who surrenders such a policy within three years after its commencement; or
 - iii) to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;
 - h) any long term insurance policy in respect of which a single premium not exceeding R 50 000,00 is payable, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client –
 - i) who surrenders such a policy within three years after its commencement; or
 - ii) to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;
 - i) any contractual agreement to invest in unit trust or linked product investments in respect of which recurring payments are payable amounting to an annual total not exceeding R 25 000,00, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client who liquidates the whole or part of such an investment within one year after the making of the first payment;
 - j) any unit trust or linked product investment in respect of which a once-off consideration not exceeding R 50 000,00 is payable, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client who liquidates the whole or part of such an investment within one year after the making of the first payment;
 - k) any other long term insurance policy on condition that within the first three
-

years after the commencement of the policy the surrender value of the policy does not exceed twenty per cent of the value of the premiums paid in respect of that policy.

- 2) Every accountable institution which performs the functions of an accountable institution referred to in items 4, 15, 17 and 18 is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 of the Act in respect of transactions in securities listed on a stock exchange (as defined in the Stock Exchanges Control Act, 1985) or a financial market (as defined in the Financial Markets Control Act, 1989) for a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962, including investments in such securities made to fund in whole or in part the ability of the fund to provide benefits for members, surviving spouses, children, dependants or nominees of members of the fund in terms of its rules.

Part 3 : Exemptions for members of Exchanges

8) Exemption from sections 21 and 22 of Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in items 4 and 15 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Sections 21 and 22 of the Act in respect of the clients on whose behalf a person or an institution is acting when entering into a business relationship with the accountable institution, if —

- a) that person or institution is situated in a country where, to the satisfaction of the relevant supervisory body, it is subject to anti-money laundering regulation and supervision of compliance with such anti-money laundering regulation, which is equivalent to that which applies to the accountable institution, and
- b) that person or institution confirms in writing to the satisfaction of the accountable institution that the person or institution will have obtained and recorded the identities of all such clients in the manner required by that country's anti-money laundering legislation.

9) Exemption from regulations made under Act 38 of 2001

- 1) Every accountable institution which performs the functions of an accountable institution referred to in items 4 and 15 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of regulation 7(f), 7(g), 7(h), 7(i), 7(j), 8(c), 9(h), 9(i), 9(j), 10(c) and 10(e) of the Regulations, and of section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars referred to in those regulations, in respect of a business relationship established, or single transaction concluded, with a client which is —
 - a) a legal person, and
 - b) a non-controlled client as defined in the Rules of the JSE Securities Exchange South Africa, as amended.
- 2) Every accountable institution which performs the functions of an accountable institution referred to in items 4 and 15 of Schedule 1 to the Act is exempted, in

respect of those functions, from compliance with the provisions of regulation 9(h), 9(i), 9(j), 9(k), 10(c) 10(d) and 10(e) of the Regulations, and of section 22(1) (a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars referred to in those regulations, in respect of a person or an institution with whom the accountable institution enters into a business relationship, if that person or institution is situated in a country where, to the satisfaction of the relevant supervisory body, it is subject to anti-money laundering regulation and supervision of compliance with such anti money laundering regulation, which is equivalent to that which applies to the accountable institution.

Part 4 : Exemptions for attorneys and administrators of property

10) Exemption from Parts 1 and 2 of Chapter 3 of Act 38 of 2001

- 1) Every accountable institution which performs the functions of an accountable institution referred to in item 1 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 of the Act in respect of every business relationship or single transaction except for a business relationship or single transaction in terms of which –
 - a) a client is assisted in the planning or execution of –
 - i) the buying or selling of immovable property;
 - ii) the buying or selling of any business undertaking;
 - iii) the opening or management of a bank, investment or securities account;
 - iv) the organisation of contributions necessary for the creation, operation or management of a company or close corporation or of a similar structure outside the Republic;
 - v) the creation, operation or management of a company or close corporation or of a similar structure outside the Republic;
 - vi) the creation, operation or management of a trust or of a similar structure outside the Republic, except for a trust established by virtue of a testamentary writing or court order;
 - b) a client is assisted in disposing of, transferring, receiving, retaining, maintaining control of or in any way managing any property;
 - c) a client is assisted in the management of any investment;
 - d) a client is represented in any financial or real estate transaction; or
 - e) a client deposits, over a period of twelve months, an amount of R100 000 or more with the institution in respect of attorney's fees which may be incurred in the course of litigation.
- 2) Every accountable institution which performs the functions of an accountable institution referred to in item 2 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 of the Act in respect of every business relationship or single transaction concerning –
 - a) the preparation of a testamentary writing;
 - b) the administration of a deceased estate, as executor of that estate;
 - c) the administration of trust property as trustee of a trust established by

- virtue of a testamentary writing or court order; or
- d) the administration of trust property as trustee of a trust established to administer funds payable from an employees' benefit fund for the benefit of a nominated beneficiary or dependant of a deceased member of such an employees' benefit fund.

Part 5 : Exemptions for estate agents

11) Exemption from Parts 1, 2 and 4 of Chapter 3 of Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in item 3 of the Schedule to the Act and which renders the services referred to in paragraphs 2 (a) and (b) of the regulations made under section 33 of the Estate Agency Affairs Act, 1976 (Act No. 112 of 1976) in Government Notice R 1485 of 17 July 1981, is exempted from compliance with the provisions of Parts 1, 2 and 4 of Chapter 3 of the Act in respect of that part of its business to which those services relates.

Part 6 : Exemptions for gambling institutions

12) Exemption from Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in item 9 of Schedule 1 to the Act and which is required to hold a license to operate a casino is exempted from compliance with the provisions of the Act in respect of all activities of such an institution which may be performed without the institution being required to hold such a license.

13) Exemption from Parts 1 and 2 of Chapter 3 of Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in item 9 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of the Act in respect of every single transaction concluded with a client, in terms of which –

- a) credit or any representation of value which is issued or sold by the institution to be used for gambling, is provided directly or indirectly to the client for a consideration not exceeding R25 000,00 or more, or
- b) an amount not exceeding R25 000,00 is provided directly or indirectly to the client in exchange for any representation of value which is issued or sold by the institution to be used for gambling; or
- c) an amount not exceeding R25 000,00 is received from the client –
 - i) as a deposit for gaming;
 - ii) as a repayment of credit previously extended;
 - iii) as a wager at any gaming activity at which a representation of value which is issued or sold by the institution to be used for gambling is not customarily

- used for wagering; or
- iv) for safekeeping;
- d) an amount not exceeding R5 000,00 is received from the client as a wager at any gaming activity at which a representation of value which is issued or sold by the institution to be used for gambling is customarily used for wagering;
- e) cash, a cheque or other negotiable instrument or funds are exchanged by, or on behalf of the client, for cash, a cheque or other negotiable instrument or funds which are to be transferred, to the amount not exceeding R25 000,00.

14) Exemption from regulations made under Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in item 9 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of regulation 3(1)(d), 3(1)(e), 4(2), 4(3), 5(1)(e) and 5(1)(f) of the Regulations, and of section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars referred to in those regulations, in respect of every single transaction which is not subject to the exemption referred to in paragraph 11 of this Schedule.

Part 7 : Exemptions for banks

15) Exemption from Parts 1 and 2 of Chapter 3 of Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 of the Act in respect of every business relationship with a natural person in terms of which an unsecured loan of an amount not exceeding R15 000,00 is made to that person.

16) Exemption from sections 21 and 22 of Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of section 21 and 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act in respect of an institution providing similar services with which the accountable institution has entered into a business relationship and which situated in a country where, to the satisfaction of the relevant supervisory body, it is subject to anti-money laundering regulation and supervision of compliance with such anti money laundering regulation, which is equivalent to that which applies to the accountable institution.

17) Exemption from regulations made under Act 38 of 2001

Every accountable institution, which performs the functions of an accountable institution referred to in items 6, 7, 14 and 16 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of regulations 3(1)(d), 3(1)(e), 3(2)(d), 3(2)(e), 4(2) and 4(3) of the Regulations, and of section 22(1)(a), 22(1)(b), 22(1)(c), 22(1)(d), 22(1)(e), 22(1)(h) and 22(1)(i) of the Act concerning the particulars

referred to in those regulations, in respect of every business relationship with a natural person who is a citizen of, or resident in, the Republic, in terms of which that person holds an account which —

- a) enables the account holder to withdraw or transfer or make electronic payments from that account to an amount not exceeding R15 000,00 over a 24 hour period;
- b) enables the account holder to receive a deposit, or a series of deposits over a period of 24 hours, into that account not exceeding —
 - i) on more than one occasion in a calendar month, an amount of R5 000,00; and
 - ii) at any time, an amount of R20 000,00;
- c) enables the account holder to maintain a balance in that account not exceeding R25 000,00; and
- d) does not enable the holder of that account to transfer funds out of that account to any destination outside the Republic, subject to the conditions that such an account does not remain dormant for a period exceeding 180 days and that the same person does not hold more than one such account with the same institution at any time.

Part 8 : Miscellaneous

18) Exemptions do not apply in case of suspicious and unusual transactions

No exemption referred to in paragraph 4(1), 5(1), 6(1), 9 and 13 of this Schedule shall apply in any circumstances where consideration is given to the making of a report under section 29 of the Act unless the accountable institution concerned may, by carrying out the required steps to which the exemptions referred to in those paragraphs apply, directly or indirectly alert, or bring information to the attention of another person which will, or is likely to, prejudice an investigation.

19) Commencement

These regulations shall come into operation on 20 May 2005.

Exchanges recognised for purposes of the exemption in respect of public companies the securities of which are listed on a stock exchange

(Exemption 6)

- American Stock Exchange
- Amsterdam Exchanges N.V.
- Athens Stock Exchange
- Australian Stock Exchange Ltd
- Barcelona Stock Exchange
- Bolsa de Comercio de Buenos Aires
- Bolsa de Madrid
- Bolsa de Comercio de Santiago
- Bolsa de Valores de Bilbao

-
- Bolsa de Valores de Lima
 - Bolsa de Valores de Lisboa
 - Bolsa de Valores do Rio de Janeiro
 - Bolsa de Valores do Sao Paulo
 - Bolsa Mexicana de Valores
 - Bourse de Montréal
 - Brussels Exchanges Ltd
 - Canadian Venture Exchange
 - Chicago Board Options Exchange, Inc.
 - Colombo Stock Exchange
 - Copenhagen Stock Exchange
 - Deutsche Börse AG
 - Helsinki Exchanges Group Ltd Oy
 - Irish Stock Exchange
 - Istanbul Stock Exchange
 - Italian Exchange
 - Jakarta Stock Exchange
 - Johannesburg Stock Exchange
 - Korea Stock Exchange
 - Kuala Lumpur Stock Exchange
 - Ljubljana Stock Exchange, Inc.
 - London Stock Exchange
 - Malta Stock Exchange
 - National Association of Securities Dealers Inc.
 - New York Stock Exchange, Inc
 - New Zealand Stock Exchange
 - OM Stock Exchange
 - Osaka Securities Exchange
 - Oslo Bors
 - Paris Bourse SBF SA
 - Philippine Stock Exchange Inc.
 - Singapore Exchange
 - Société de la Bourse de Luxembourg SA
 - Swiss Exchange
 - Taiwan Stock Exchange
 - Tehran Stock Exchange
 - The Bermuda Stock Exchange Ltd
 - The Chicago Stock Exchange, Inc.
 - The Stock Exchange of Hong Kong Ltd
 - The Stock Exchange of Thailand
 - The Tel Aviv Stock Exchange Ltd
 - The Toronto Stock Exchange
 - Tokyo Stock Exchange
 - Warsaw Stock Exchange
 - Wiener Börse AG
-

Keyword Index

- 1 -

16 120

- A -

above 37
 absence 170
 acceptable documentation 109
 Acceptable documents 110
 access 33, 44, 75
 access to information 36
 Accountable 80, 170
 accountable institution 52
 accountable institutions 36, 47, 194
 Act 10
 Act No. 1 of 2017 92
 Acting 20
 activity report 180, 188
 acts 170
 additional 40
 Additional due diligence measures 27
 additional information 193
 Additional requirements 170
 address slip 108
 adequate proof 108
 administrative sanctions 60, 196
 administrators 203
 Admissibility 32, 44
 advise 68
 advise Centre of clients 36
 affected 43
 African 43
 all partners in a partnership 114
 Alternate means of verification 108
 Amendment 80, 83
 Amendment of list 83, 84
 Amendment of sections 89
 Annexure 198
 Anonymous clients 25
 anti-money laundering 50, 104
 Appeal 62
 appeal board 65, 74
 appeal is to be lodged 195
 Appeals 193
 application 75
 Application of Act 16
 Application to court 66
 appointment 19, 20
 Appointment of inspectors 56

arrangements 84
 Arrangements for consultations 83
 assistance 68
 attorneys 203
 Audit 23
 authorised representative 37
 authorities 80
 authority 170
 avoid 75

- B -

bank 120
 banks 205
 bearer negotiable instrument 70
 best banking practice 116
 Board approval 104
 bodies 43, 81
 business 31
 business relationship 26

- C -

cash 37, 40, 69, 70
 cash threshold report 174
 cash transaction reporting 174
 Centre 22, 33, 41, 68, 73, 136, 194
 Chapter 1 16, 166
 Chapter 2 24, 170
 Chapter 3 25, 171
 Chapter 4 55, 171
 Chapter 5 79, 193
 Chapter 6 196
 citizens 167
 Clarification 107, 108, 120
 Clarification of partnership agreements 114
 client 68, 98, 120
 Client acceptance policies 107
 Client Profile 171
 Client profiling procedures 105
 clients 105
 clients acting under false 25
 close corporations 168
 commencement 85, 92, 198
 companies 113, 168
 Compliance 50, 55
 comply 71
 Composition 24
 computer system 75
 Conducting 75
 confidential 46
 confidentiality 43
 conflict with other laws 16

-
- Consultation process 50
 - contact person 170
 - Continuation 41
 - Contravention of prohibitions 68
 - Control Measures 25
 - conveyance 40, 70
 - Core Principles 116
 - correctness 170
 - correspondent banking relationships 118
 - Correspondent Banks 118
 - counter terrorist financing compliance 50
 - Counter-Money laundering advisory Council 24
 - courts 79
 - Criteria for 195
 - customer due diligence 29, 67
 - D -**
 - dealing with property 35
 - Defences 77
 - Definition 113, 117
 - Definitions 11, 76, 157, 159, 161, 164
 - Delegation 23
 - Deleted 198
 - Department of Home Affairs 108
 - Destroying 68
 - direction 71
 - Directives 51
 - directives of Centre 75
 - Director 19, 20, 22
 - disclosure 70
 - Domestic Prominent Influential Person 30, 87
 - domestic prominent influential persons 83
 - Doubts about veracity 29
 - duties 75, 98
 - duty 43
 - Duty to identify clients 25
 - Duty to keep record 30
 - E -**
 - electronic 40, 71
 - Enforcement 55
 - entities identified 68
 - entities identified by 34
 - Establishing 107
 - establishment 17, 24, 65, 166, 193
 - estate agents 204
 - evidence 44
 - Examples 98
 - Exchanges 202, 206
 - exemption 156, 157, 158, 159, 160, 161, 206
 - Exemption 5 120
 - Exemptions 80, 120, 200, 202, 203, 204, 205
 - Exemptions 5 120
 - F -**
 - Failure 67, 68, 69, 70, 71, 72, 73
 - Failure to answer 74
 - Failure to attend 74
 - Failure to comply 67, 75
 - Failure to comply with duty 73
 - Failure to register 73
 - Failure to report property 69
 - Family members 30
 - FATF Recommendations 116
 - faxed copies 109
 - fictitious names 25
 - financial 23
 - Financial Intelligence Centre 16
 - Financial Intelligence Centre Act 156, 158, 160
 - Financial Intelligence Centre Act, 2001 123
 - Financial Intelligence Centre Amendment Act 92
 - Financial sanctions 25, 33
 - Financial Services Board 96
 - Financing of Terrorist 25
 - footnotes 84
 - foreign 167
 - foreign clients 120
 - foreign companies 168
 - foreign country 120
 - foreign nationals 112, 168
 - Foreign Prominent Public Official 29, 88
 - foreign prominent public officials 84
 - forfeiture 77
 - Form 1 198
 - formulate 72
 - Formulation 47
 - fully or truthfully 74
 - Functions 18, 24
 - Funds 23
 - furnished 193
 - furnishing 40
 - G -**
 - gambling institutions 204
 - General 170
 - General Exemptions 199
 - General powers 19
 - give 68
 - Glossary 121, 126
 - governance 50, 73
 - Government departments 115
 - Guidance 102, 196
-

-
- Guidance Note 2 96
 - Guidance Note 3 102
 - Guidance Note 4 124
 - Guidance to Financial Services Industries 96
 - H -**
 - held 43
 - high risk clients 105
 - high-risk clients 117
 - Hindering or obstructing 74
 - I -**
 - Identification 98, 112, 113, 115
 - Identification of clients 25
 - Identification of trusts 114
 - identify 67, 171
 - identify proceeds 171
 - identities 193
 - identity document 108
 - identity documents 108
 - implement 72
 - implementation 47
 - Implementation of Guidance Note 1 104
 - Implications 133
 - Inability to conduct 29
 - Indemnity 83
 - Indicators 131
 - information 40, 43, 44, 46, 72, 167, 168, 169, 171, 172, 176, 194
 - information relating to a report 195
 - Information to be reported 174, 180, 188
 - inspection 74
 - Inspections 57
 - institution 120, 170
 - institutions 80, 81
 - insurance 200
 - internal 72
 - Internal rules 193, 194
 - international standards 116
 - Interpretation 199
 - Intervention 41
 - Introduction 97, 127, 167
 - Introductory 167
 - investigating 80
 - investment 200
 - issuing guidance 50
 - J -**
 - Jurisdiction 79
 - K -**
 - keep 67
 - keeping 193
 - kept 31, 32
 - known close associates 30
 - KYC procedures 108
 - L -**
 - laws 83
 - Legal Entities 112
 - Legal incapacity 111
 - Legal Persons 27, 168
 - limit 37
 - List of Accountable Institutions 85
 - List of Reporting Institutions 87
 - List of Supervisory Bodies 86
 - listed companies 112
 - lost or stolen 108
 - M -**
 - Manner 171, 193
 - Manner in 195
 - manner of 194
 - Measures 47, 118, 193
 - Meetings 24
 - members 202
 - Miscellaneous 79, 196, 206
 - Misuse 72
 - modification 76
 - Money Laundering 25, 164
 - money laundering activities 171
 - monitoring 42, 50, 71
 - N -**
 - nationals 167
 - Nations Security Council 69
 - natural person 109
 - Natural Persons 107, 112, 167
 - Nature 130
 - non face-to-face verification 108
 - non-compliance 196
 - not 43
 - Notice No. 1035 of 2006 123
 - Notice No. 1262 of 2001 10
 - Notice No. 301 of 2008 125
 - Notice No. 471 of 2010 158
 - Notice No. 560 of 2010 160
 - Notice No. 563 of 2017 92
 - Notice No. 715 of 2005 102
 - Notice No. 735 of 2004 96
 - Notice No. R. 1354 of 2004 100
 - Notice No. R. 1595 of 2002 164
 - Notice No. R. 454 of 2010 156
-

Notices 96
 Notification of persons 33
- O -
 Objectives 17
 Obligation to keep 31
 Obligation to Report 128
 obligations 43
 Obstructing 75
 obtaining information 26
 off the shelf 113
 Offences 53, 74, 196
 office 20
 official 75
 official identity document 107
 Ongoing client detail maintenance 111
 Ongoing due diligence 28
 order 71
 orders 42
 organs of state 115
 other 22
 other legal persons 169
 other persons 25
- P -
 Part 1 25, 167
 Part 2 30, 167
 Part 2A 33
 Part 3 36, 168
 Part 4 47, 169
 Part 5 52, 169
 Part 6 170
 Particulars 170
 parties 32
 partnership 113
 partnerships 27, 113, 169
 payment of fee 195
 penalties 76, 196
 pension 113
 PEP 117
 PEPs 117, 118
 Period 31, 192
 Period for 194
 Period within 193, 194
 Permitted financial services 35
 person 170
 personal information 47
 persons 67, 68
 Policies 118
 politically exposed person 117
 Politically Exposed Persons 117

powers 80
 Powers of access 37
 Preface 102, 125
 Prescribed amount 166, 174
 previously obtained information 29
 procedure 24
 procedures 40, 104
 Process 136
 Prohibitions relating to persons 34
 Promote Compliance 47, 193
 Proof 20
 property 203
 Property associated with 38
 Protection 44, 46
 Protection of 47
 provide 43, 73
 provident funds 113
 providers 200
 public companies 206
- R -
 Record 31
 Record-Keeping 170
 records 31, 32, 33, 67, 68, 170, 193
 Referral 52, 53
 Registration 52
 registration by 194
 regulated by 96
 Regulations 82, 157, 159, 161, 164
 Related Activities 25
 relationships 31
 Removal 20
 Repealed 24, 33, 166, 167, 168, 169, 170, 171, 193, 194
 report 69, 70, 71
 reported 172, 176
 reporting 40, 43, 81, 171, 192, 194
 Reporting duties 36
 reporting institution 52
 reporting institutions 36, 194
 reporting obligations 36
 reports 44
 reports required 37
 Republic 70
 request 71
 residential address 108, 109
 residents 107, 167
 Resolutions 69
 Resolutions of United 69
 Resolutions of United Nations Security Council 38

-
- Responsibilities 20
 - Responsibility 53
 - Revenue 43
 - Risk indicators 105
 - risk-based approach 104
 - rules 72
 - S -**
 - Schedule 199
 - Schedule 1 85
 - Schedule 2 86
 - Schedule 3 87
 - Schedule 3A 87
 - Schedule 3B 88
 - Schedule 4 89
 - Schedules 85, 198
 - screening 22
 - Search 77
 - Second Reporting Exemption 100
 - section 29 195
 - securities 206
 - Security 22
 - Security Council 68
 - Security Council of the United Nations 33, 34
 - seizure 77
 - send 70
 - Service 43
 - Short title 85
 - should be identified 114
 - single transaction 166
 - South 43
 - South African banks 116
 - South African Citizens 107
 - South African companies 168
 - South-African citizens 167
 - staff 21, 22
 - stakeholders 83
 - Status 84, 109
 - stock exchange 206
 - STR 133
 - submitted to Centre 37
 - Submitting 136
 - subsidiaries 112
 - summoned 74
 - supervision 52, 53
 - supervisory 43, 81
 - supervisory body 75, 194, 195
 - suspected 53
 - Suspicion 130
 - suspicious 39, 70, 131, 176
 - suspicious or unusual 180
 - Suspicious or Unusual Transaction Report 198
 - Suspicious Transaction Reporting 124
 - T -**
 - tampering 68
 - terrorist and related activities 38, 69
 - terrorist financing 184, 188
 - Terrorist Financing Control 164
 - terrorist financing policies 104
 - terrorist property report 172
 - the Wolfsberg Principles 116
 - third 32
 - third parties 170
 - third party verification 110
 - Third Reporting Exemption 123
 - Title 198
 - training 50, 73
 - transaction 96, 98
 - transaction records 31
 - transaction report 176, 184
 - transactions 31, 37, 39, 41, 69, 70, 75, 98
 - transfers 40, 71
 - Transitional 84
 - Treatment of PEPs 117
 - trust 115
 - trustee 115
 - trusts 27, 114, 169
 - U -**
 - Unauthorised 70, 75, 76
 - Understanding 26
 - United Nations 68
 - United Nations Security Council 69
 - unlawful activities 171
 - unusual 39, 176
 - Unusual Transactions 131
 - V -**
 - verification 102, 108, 112, 113, 115, 168, 169, 170, 193
 - verification of identity 166
 - Verification of information 167, 168, 169
 - verify 109
 - Verifying Identities 107
 - W -**
 - What is the Nature 130
 - Who Must Report 128
 - Y -**
 - year 23
-