www.fsca.co.za

MONEY LAUNDERING, FINANCING OF TERRORISM AND PROLIFERATION OF FINANCING SECTOR RISK ASSESSMENT

COLLECTIVE INVESTMENT SCHEMES AND FINANCIAL ADVISORY AND INTERMEDIARY SERVICES SECTORS

ISSUED BY THE FINANCIAL SECTOR CONDUCT AUTHORITY

APRIL 2022

FSCA
Financial Sector Conduct Authority

Key statistics

*** As at 31 December 2020**

**** Information for the period 1 April 2018 – 31 December 2020**

***** Information for the 2019 and 2020 calendar years**

The number of Collective Investment Scheme (CIS) Managers* **65**	The number of Financial Services Providers (FSPs)* **9179** (excluding FSPs with Cat 1.2 and/or 1.6 and/or 1.16 authorisation)	Total value of assets under management by CIS Managers* **R3,188 trillion**	Total value of assets under management by FSPs* **R10,175 trillion**
Number of STRs filed by CIS Managers** **360** **to the value of** **R182 million**	The number of STRs filed by FSPs** **10 553** **to the value of** **R3 450 million**	Number of TPRs filed by CIS managers and FSPs** **0**	Total inflow and outflow of money in the CIS sector*** **R211 billion inflow** **R190 billion outflow**
Number of CTRs filed by CIS managers** **2 030** **to the value of** **R125 million**	Number of CTRs filed by FSPs** **38 900** **to the value of** **R4 billion**	Matters referred by the FSCA to SAPS to investigate** **104**	Total inflow and outflow in the Financial Advisory and Intermediary Services sector*** **R175 billion inflow** **R154 billion outflow**

TABLE OF CONTENTS

Glossary		**4**
A.	**Executive Summary**	**6**
B.	**Background**	**14**
C.	**Risk Assessment Methodology**	**16**
D.	**Sectoral Threat Analysis**	**19**
E.	**Sector Vulnerability Analysis**	**30**
F.	**Consequences**	**40**

GLOSSARY

AFU	Asset Forfeiture Unit of the National Prosecuting Authority
AI	Accountable Institutions *referred to in items 4, 5 and 12 of Schedule 1 to the FIC Act.*
AUs	Authorised Users *of an exchange as defined in the Financial Markets Act, 19 of 2012*
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and/or the Combatting of Financing of Terrorism
CIS	Collective Investment Scheme
CISCA	Collective Investment Schemes Control Act, 45 of 2002
CIS Manager	Collective Investment Schemes Manager *registered in terms of the Collective Investment Schemes Control Act, 45 of 2002*
CTR	Cash Threshold Report(ing)
CTRA	Cash Threshold Report *submitted in terms of section 28 of the FIC Act, whereby the transaction values have been aggregated (added up) to total the threshold value*
DPI	Directive to Provide Information *issued by the FSCA during 2021 to understand the ML/TF/PF risks of individual institutions*
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FAIS Act	Financial Advisory and Intermediary Services Act, No. 37 of 2002
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FIC Act	Financial Intelligence Centre Act, *No. 38 of 2001*
FSCA	Financial Sector Conduct Authority
FSP	Financial Services Provider *requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, No. 37 of 2002, to provide advice or intermediary services in respect of the investment of any financial product (but excluding a non-life insurance policy as defined in the Insurance Act, No. 18 of 2017 and a health service benefit provided by*

	a medical scheme as defined in section 1(1) of the Medical Schemes Act, No. 131 of 1998.
FSR Act	Financial Sector Regulation Act, *Act 9 of 2017*
LISP	Linked Investment Service Provider
ML/TF	Money laundering and/or terrorist financing
NPA	National Prosecuting Authority
PF	Proliferation of Finance *for weapons of mass destruction*
RUSI	Royal United Services Institute
SAPS	South African Police Service
SRA	Sector Risk Assessment
SSA	State Security Agency
STR	Suspicious Transaction Report(ing) and suspicious activity report(ing)
STR	Terrorist Financing Report *in terms of section 28A of the FIC Act*
TF	Terrorist Financing

A. EXECUTIVE SUMMARY

The FSCA was established in terms of the FSR Act as a dedicated Market Conduct Regulator in South Africa. The FSCA's mandate includes all financial institutions that provide a financial product and/or a financial service as defined in the FSR Act and licensed in terms of a financial sector law, including CIS Managers and FSPs.

Financial products such as a participatory interest in a CIS, other investments or a life insurance product may be abused by money launders to wash their illicitly acquired gains. Many CISs, other investment or life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial products, there is a risk that the funds used to invest in CISs, other investments or to purchase life insurance products may be the proceeds of crime. There is also a risk, albeit limited, that funds withdrawn from a CIS, other investments or life insurance products could be used to fund terrorism.

CIS Managers and FSPs can use this risk assessment as an important resource for feedback on ML/TF/PF risks in the sector and to assess their institutional risks. Based on this assessment, the FSCA expects AIs to refine their institutional compliance controls and mitigation strategies. In addition to identifying and monitoring risk factors that may apply to their individual businesses. This risk assessment also seeks to assist AIs in reporting suspicious transactions or AML/CFT related matters to the FIC and the FSCA respectively.

Below is a summary of the findings of the risk assessment conducted on the above-mentioned sectors to understand the ML/TF/PF risks in those sectors. The FSCA assessed the ML/TF/PF risks for the period **1 April 2018 – 31 December 2020**. The assessment focused on money laundering (ML), terrorist financing (TF) and the financing of proliferation (PF).

Overall Risk Rating of the sectors under review:

	Money laundering			Terrorist financing			Proliferation fina	
	Threats	**Vulnerabilities**	**Consequences**	**Threats**	**Vulnerabilities**	**Consequences**	**Threats**	**Vulnerabilities**
CIS	Low	Medium	Medium	Low	Medium	Medium	Low	Medium
Financial Advisory and Intermediary Services	Low	Medium	Medium	Low	Medium	Medium	Low	Medium

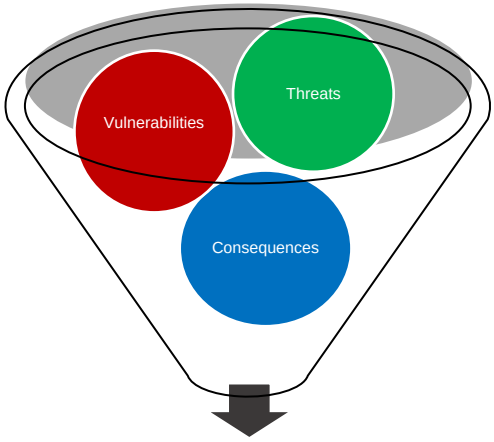
The FSCA assessed the overall ML/TF/PF risks in the CIS sector and category II, IIA and III financial services providers[1] in the non-bank financial services sector as **MEDIUM**. Category I and IV financial services providers[2] remain **LOW** risk for ML/TF/PF as indicated the original assessment conducted.

In conducting the sector risk assessment, the FSCA evaluated three areas namely **criminal threats**, **vulnerabilities** and **consequences** as recommended by the FATF[3]. The primary objective is to identify and understand ML/TF/PF risks and other criminal offences targeting the non-bank financial sector in South Africa.

[1] Category II FSP means a discretionary FSP. A discretionary FSP renders intermediary services of a discretionary nature as regards the choice of a particular financial product. Category IIA FSP means a Hedge Fund FSP. Category III FSP means an administrative FSP. An administrative FSP renders intermediary services in respect of financial products referred to in paragraphs (a), (b), (c) (excluding any short-term insurance contract or policy), (d) and (e), read with paragraphs (h),(i) and (j) of the definition of 'financial product' in section 1(1) of the FAIS Act, on the instructions of a client or another FSP.

[2] Category I FSP renders financial services other than the financial services mentioned in Categories II, IIA, III and IV. Category IV - 'Assistance Business FSP' means an FSP that renders intermediary services in relation to the administration of assistance policies on behalf of the Insurer to the extent agreed to in terms of a written mandate between the insurer and the Assistance Business FSP.

[3] FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment, February 2013



Sector Risk Assessment Results

1. Criminal Threat Environment

Threats are predicate offences and ML/TF/PF risks to which the CIS and Financial Advisory and Intermediary Services sectors may be exposed.

The CIS and Financial Advisory and Intermediary Services sectors are relatively big considering the assets under management by the sectors. Investigations and prosecutions of ML/TF matters in the sectors appears to be low. From a predicate offence perspective, the main concerns in these sectors relate to fraudulent claims, Ponzi schemes and unauthorized/unlicensed businesses. This is further supported by the suspicious transactions and activities reported by the sectors to the FIC. The most common offences reported to the FIC by CIS Managers relate to fraud and forgery while the most common offences reported to the FIC by FSPs relate to fraud and tax evasion.

The results of the DPI which was issued by FSCA to CIS Managers and FSPs for completion indicated that criminal threats and ML/TF/PF risks in the sectors related to the following:

Theft

2% of CIS Managers and 0.29% in the case of FSPs have experienced theft from the business by clients during the period of review. CIS Managers did not report any incidents of theft from the business by employees, however, 0.78% of FSPs reported incidents of theft by employees.

Fraud

The CIS and Financial Advisory and Intermediary Services sectors experienced low numbers in incidents of fraud by clients and employees respectively.

Money Laundering (ML)

The results related to the Financial Advisory and Intermediary Services sector pointed to a very low proportion of FSPs suspecting their business was being abused for ML purposes. The CIS sector did not provide information indicative of suspicious ML activity in respect of their business for the period of review.

Terrorist Financing (TF)/Proliferation Financing (PF)

The level of reporting on TF and PF was very low to non-existent for both sectors.

Law enforcement and intelligence agencies indicated that they have not observed that these sectors were abused for TF or PF during the period under review.

The CIS and Financial Advisory and Intermediary Services sectors have been assessed as follows from a threat perspective:

	Money laundering	Terrorist financing	Proliferation financing
CIS	Low	Low	Low
Financial Advisory and Intermediary Services	Low	Low	Low

The overall criminal threat environment is assessed as **LOW**.

2. Vulnerabilities

Vulnerabilities (inherent risks) are features of the industry/sectors that make it attractive for ML/TF/PF purposes.

The vulnerabilities (inherent risk) features of the sectors relate to the following:

Clients

Financial institutions operating in the CIS and Financial Advisory and Intermediary Services sectors are exposed to a wide array of client types. It was noted that the prevalence of foreign based clients, foreign prominent public officials and domestic prominent influential persons are low in these sectors. Though, the large presence of legal persons makes the CIS and Financial Advisory and Intermediary Services sectors vulnerable to ML/TF/PF.

Products and services

A high percentage of CIS Managers render financial services in respect of investment products to clients while the percentage is relatively low in the case of FSPs. The DPI results showed that rendering financial services in respect of unlisted securities, forex, private equity and products with exposure to crypto assets is not widespread.

It was taken into consideration that while both sectors provide products or render services in respect of products with offshore exposure, results in relation to the CIS sector depict that a significant number of CIS Manager render financial services in respect of products with offshore exposure. Large exposure to investment products with offshore exposure may make the CIS sector vulnerable to ML/TF/PF risk.

Distribution channels

Engagements with clients via persons acting on behalf of clients are not predominant in the CIS and Financial Advisory and Intermediary Services sectors.

Non-face-to-face transacting using telephone or the internet as a main distribution channel is relatively high in both sectors[4]; however, relatively low in the case of mobile applications and clients transacting using gift vouchers.

Geographies

Most FSPs do not engage in dealings with clients residing in sanctioned jurisdictions and none concerning CIS Managers. It is not common for FSPs to render financial services to clients that reside in sanctioned jurisdictions. The use of intermediaries outside South Africa is relatively moderate in the case of the Financial Advisory and Intermediary Services sector.

Use of Cash

The use of cash is still prevalent in the sectors, especially in the Financial Advisory and Intermediary Services sector.

Mitigation of ML/TF/PF risks

Results for both sectors have indicated that a high number of ML/TF risk assessments to identify ML/TF risks faced by AIs have been conducted. Moreover, both sectors have a high number of AIs that have developed and implemented RMCPs, and which make provision for client identification and verification of beneficial owners. Similarly, there is a very high rate of client due diligence conducted in the CIS and Financial Advisory and Intermediary Services sectors.

There were low levels of reporting of suspicious transactions.

[4] The statistics from the DPI are reflective of the fact that the directive to provide information was issued during the height of the COVID-19 pandemic in South Africa. There is a distinction between direct marketers (who use telephones as their only distribution channel and FSPs in general who would, under normal circumstances, always onboard using face to face and then maintain the relationship by adding the use of phones. Similarly, the use of internet platforms is predominantly used in the insurance sector as well as forex trading industry and is not embedded to a large extent in the majority of FSPs' distribution channels.

The CIS and Financial Advisory and Intermediary Services sectors have been assessed as follows from a vulnerability perspective:

	Money laundering	Terrorist financing	Proliferation financing
CIS	Medium	Medium	Medium
Financial Advisory and Intermediary Services	Medium	Medium	Medium

The overall vulnerability environment is assessed as **MEDIUM**.

3. Consequences

Consequence refers to the impact or harm that ML/TF risks may cause or have on clients, financial institutions, the financial sector and the broader South African economy. The controls put in place by financial institutions in the various sectors regulated by the FSCA will minimise any harm or damage caused by ML/TF/PF risks. The controls largely refer to measures for compliance with the FIC Act.

The consequences for clients because of the criminal misuse of the sector relate to financial losses and emotional distress. Financial institutions will suffer reputational damage, increased costs, and possibly decreased dividend distributions to shareholders. ML/TF/PF risks have the potential to impact the broader South African economy through reduction in taxation revenue and reduced financial investments in the sector which may impact on the economic growth of the country.

The consequences of ML/TF/PF in these sectors are also assessed as **MEDIUM**. The broader public may also lose confidence in the non-bank financial sector. There also may be an impact on the broader South African economy as investors will be hesitant to invest where there are indicators of ML/TF/PF.

Overall ML/TF/PF Risk Rating

The overall ML/TF/PF threat, vulnerability and consequence of the CIS and Financial Advisory and Intermediary Services sectors have been assessed as follows:

	Money laundering	Terrorist financing	Proliferation financing
CIS	Medium	Medium	Medium
Financial Advisory and Intermediary Services	Medium	Medium	Medium

B. BACKGROUND

The FSCA conducted a SRA on AUs, CIS Managers and FSPs in 2018/19 which results were published on the FSCA's website on 31 May 2019. As good practice, the SRA must be reviewed and updated on a regular basis to stay relevant. Since the information and statistics considered in the original SRA are more than two years old, a review of the facts, information and conclusions was necessary. The FSCA also addressed the concerns raised by the assessors of the Financial Action Task Force mutual evaluation of South Africa in this review. This report sets out the findings of the risk assessment conducted by the FSCA on the CIS and Financial Advisory and Intermediary Services sectors.

1. What has changed from the previous report?

- ✓ The previous report[5] set out the risk assessment of three sectors being AUs, CIS Managers and FSPs. The FSCA is now publishing two separate reports, firstly for the Securities sector and, secondly for the CIS and Financial Advisory and Intermediary Services sectors, respectively. This report addresses the risk assessment in respect of the CIS and Financial Advisory and Intermediary Services sectors. A separate report on the securities sector has been prepared.
- ✓ The FSCA received updated information on ML threats and vulnerabilities for the period 1 April 2018 – 31 December 2020.
- ✓ This report also considered the TF and PF threats, vulnerabilities and consequences in the CIS and Financial Advisory and Intermediary Services sectors.
- ✓ The ML/TF/PF risks in the CIS sector is rated as medium in this assessment. The previous risk assessment rated this sector as low. The current risk rating is mainly

[5] Anti-Money Laundering and Counter Financing of Terrorism Sector Risk Assessment Report of Authorised Users of an Exchange, Collective Investment Schemes Managers, Financial Services Providers, Issued by The Financial Sector Conduct Authority, May 2019
https://www.fsca.co.za/Regulatory%20Frameworks/Temp/4.4.1%20%20Sector%20Risk%20Assessment%20-%20Short%20Version%2031%20May%202019.pdf

attributed because of its inherent risks and more specifically the international exposure of the sector.

2. Why has the FSCA conducted the SRA?

- ✓ The SRA assists the FSCA to identify, assess and understand the ML/TF risks as well as proliferation financing risks in the sectors regulated by it. When we understand the ML/TF/PF risks, it helps to plan our activities in a risk-sensitive manner by determining how much attention to give relevant sectors and entities within those sectors, and to identify which risks should be prioritised.
- ✓ SRAs should be reviewed and updated regularly to remain relevant by:
    - o Setting out the frequency and triggers for updates to sectoral and entity risk assessments under the supervisory risk assessment methodology;
    - o Identifying and assessing emerging risks and trends within our supervised population, then **revising** the risk assessment on an ongoing basis; and
    - o Regular dialogue and information sharing with the public and private sector to understand the latest trends and risks.
- ✓ It assists with entity-level risk assessments. CIS Managers and FSPs should consider the risks identified by the SRA and align their own risk assessments, where applicable.
- ✓ The FSCA can provide guidance and clarify the supervisory expectations for entity risk assessments.

3. How should CIS Managers and FSPs use this SRA?

- ✓ CIS Managers and FSPs should consider the risks identified in this SRA with specific reference to red flags, trends and typologies and vulnerabilities.
- ✓ CIS Managers and FSPs should review and update their own risk assessment based on the results of this SRA.
- ✓ CIS Managers and FSPs should manage and mitigate the potential ML/TF/PF risk exposed to their business.

C. RISK ASSESSMENT METHODOLOGY

The FSCA followed the methodology as recommended by the FATF[6]. In terms of the methodology, three areas need to be evaluated namely **threats**, **vulnerabilities** and **consequences**.

Threats refer to criminal threats, including ML/TF risks that face the industry. In assessing threats, the following information was considered:

- Materiality;
- ML/TF/PF cases investigated and prosecuted in the CIS and Financial Advisors and Intermediary Services sectors during 1 April 2018 – 31 December 2020;
- Predicate offences investigated and prosecuted in the CIS and Financial Advisors and Intermediary Services sectors during 1 April 2018 – 31 December 2020;
- Proceeds of crime seized in the CIS and Financial Advisors and Intermediary Services sectors during 1 April 2018 – 31 December 2020;
- Number of STRs and TPRs submitted, the types of offences reported and reasons for submitting STRs by the sectors; and
- ML/TF trends in the sectors.

Vulnerabilities (inherent risks) refer to the features and characteristics of the industry that make it attractive for ML/TF purposes. The following information was considered:

- **Clients**
  - Types of clients;
  - Prevalence of foreign based clients;
  - Prevalence of high-risk clients such as foreign prominent public officials or domestic prominent influential persons; and
  - Clients that are part of a complex or multi layered structure of ownership or control.

[6] https://www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

- **Products and services**
  - Exposure to crypto assets;
  - Unlisted Securities;
  - Foreign Exchange (Forex);
  - Private Equity; and
  - Cross-border transactions (offshore exposure).

- **Distribution channels**
  - Distribution of products through other FSPs, group entities or third parties; and
  - Non-face-to-face transacting using telephone or internet.

- **Geographies**
  - Residence of clients in sanctioned jurisdictions; and
  - Use of intermediaries outside South Africa.

- **The use of cash**
  - The number and value of CTRs submitted to the FIC by the sectors.

- **Mitigation of ML/TF risks**
  - Risk assessment conducted by CIS Managers and FSPs;
  - Client due diligence conducted by CIS Managers and FSPs; and
  - Reporting of suspicious transactions by CIS Managers and FSPs.

Consequence refers to the impact or harm that ML/TF risks may cause or have on clients, financial institutions, the financial sector and the broader South African economy. The following criteria have been considered to determine consequences:

- Harm or loss to clients;
- Harm or loss to financial institutions;
- Harm or loss to the financial sector; and
- Harm or loss to the South African economy.

The ML/TF/PF risks were assessed for the period 1 April 2018 – 31 December 2020. Various sources were used to collect data from several agencies and industry bodies e.g., consultation with the FIC, NPA, SAPS, SARS, SSA, RUSI, industry experts as well as the results from the DPI, review of internal records and databases, including onsite & off-site inspections.

Each sector was then assessed as **Low**, **Medium** or **High** risk in each area assessed i.e., threats, vulnerabilities and consequences. All three risk areas were then combined to give a holistic rating of the CIS and Financial Advisory and Intermediary Services sectors respectively. It must be noted that a rating of low-risk does not mean that there is no risk within the sector. ML may still take place in low risk sectors. Similarly, a high-risk rating is not indicative of a lack of compliance in the sector. Some sectors, by their nature, always have a higher level of inherent risk.

D. SECTORAL THREAT ANALYSIS

1. Materiality

1.1. CIS Managers

The CIS industry is regulated in terms of CISCA. A CIS is an investment vehicle that allows investors to pool funds and invest in assets which they might not otherwise be able to access in their individual capacities. Investors are allocated a participatory interest or units, in proportion to the value of their contribution to the portfolio. Investors do not have control over assets purchased with their funds. Instead, they enjoy the benefits of a diversified portfolio managed by a registered CIS Manager, but in many cases this function is delegated to the Investment manager authorised under the FAIS Act through a delegation agreement.

The size of the CIS sector as at 31 December 2020 was as follows:

Type of Scheme	Number of CIS Managers	Assets under management
CIS in Securities	48	R3.10 trillion
CIS in Property	1	R1.40 billion
CIS in Participation Bonds	2	R4.11 billion
CIS in Hedge Funds	14	R83 billion

1.2. FSPs

An FSP is any person, other than a representative, who as a regular feature of the business of such a person, furnishes advice, renders an intermediary service, or provides both in respect of a financial product. FSPs are regulated under the FAIS Act. Financial advisers & intermediaries are considered a key segment of the financial services sector because they are the contact point between product suppliers and clients. Most financial advisers & intermediaries simply provide advice, do financial planning, sell products or help clients to select appropriate products for

their financial needs. Most financial advisers & intermediaries do not handle client funds and are not allowed use discretion on behalf of clients.

The different types of FSPs authorised by the FSCA as at 31 December 2020 are as follows:

Number and Types of FSPs as at end of 2020	
Category I FSPs (Financial advisers & Intermediaries)	8190
Category II FSPs (Discretionary Investment managers)	730
Category IIA FSPs (Hedge fund managers)	122
Category III FSPs (Linked Investment Service Providers & Platforms)	30
Category IV FSPs (Assistance business administrators)	107

The assets under management in the Financial Advisors and Intermediary Services sector was **R10,175 trillion** as at 31 December 2020.

2. ML/TF/PF cases investigated and prosecuted in the CIS and Financial Advisory and Intermediary Services sectors during 1 April 2018 – 31 December 2020

2.1. Money laundering and terrorist financing (ML/TF)

There were no ML/TF cases investigated or prosecuted involving the CIS and Financial Advisors and Intermediary Services sectors during the period under review by the NPA. SARS, however investigated a matter where entities fraudulently claimed VAT refunds. The accused in that case laundered the proceeds of crime by *inter alia* investing in financial products The FIC has analysed matters where ML was investigated in both sectors under review. See the ML/TF trends section below for more details.

None of the CIS Managers reported incidents of money being laundered through their business. However, 0.24% of FSPs indicated that money has been laundered through their business.

2.2. Proliferation of financing (PF) risks

PF risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions (TFS) obligations referred to in sections 26A-26C of the FIC Act. The source of PF risks would depend upon several factors as follows[7]:

- **Risk of a potential breach or non-implementation of targeted financial sanctions:** This risk may materialise when designated entities and individuals access financial services, and/or funds or other assets, as a result, for example:
  (a) delay in communication of designations at the national level,
  (b) lack of clear obligations on financial institutions, failure on the part of financial institutions to adopt adequate policies and procedures to address their PF risks (e.g., weak Client onboarding procedures and ongoing monitoring processes,
  (c) lack of staff training, ineffective risk management procedures, lack of a proper sanctions screening system or irregular or inflexible screening procedures, and a general lack of compliance culture);
- **Risk of evasion of targeted financial sanctions:** This risk may materialise due to concerted efforts of designated persons and entities to circumvent targeted financial sanctions (e.g., by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries).

TFS obligations apply to two country-specific regimes for DPRK (North Korea) and Iran, requires countries to freeze without delay the funds or other assets, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of:

(a) any person or entity designated by the United Nations (UN),
(b) persons and entities acting on their behalf or at their direction,
(c) those owned or controlled by them.

[7] http://www.fatf-gafi.org/publications/fatfgeneral/documents/public-consultation-proliferation-financing-risk.html

RUSI indicates that the maritime insurance sector may be at risk for PF.

There is currently no evidence of PF in the CIS and Financial Advisors and Intermediary Services sectors. PF uses the formal banking sector as it is a trade-based activity.

3. Predicate offences investigated and prosecuted in the CIS and Financial Advisory and Intermediary Services sectors during 1 April 2018 – 31 December 2020

ML is defined in the FIC Act as 'any activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of proceeds of unlawful activity or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of section 64 of the FIC Act or section 4, 5 or 6 of POCA'. Unlawful activity in the term 'proceeds of unlawful activity' refers to any criminal conduct. The unlawful activity is also referred to as a predicated offence. To prove ML, the NPA would have to prove that the proceeds emanated from a predicate offence. It is, therefore, important to understand what predicate offences are being committed that leads to ML.

During the period June 2020 – March 2021, the NPA prosecuted 45 matters involving ML. In most of the matters (42%), the predicate offence is indicated as fraud. Other predicate offences relate to dealing in drugs, abalone smuggling, racketeering and theft. These prosecutions were, however, in sectors other than CIS Managers and FSPs.

The FIC has indicated that most of crimes reported in STRs filed by CIS Managers and FSPs relate to fraud. Other crimes reported by CIS Managers and FSPs relate to forgery and tax evasion.

The FSCA referred 104 matters to the SAPS to investigate during the period under review. Most referrals related to the contravention of section 7(1) of the FAIS Act (rendering

unauthorised financial services). Although the referrals relate to contraventions of the FAIS Act, the SAPS also investigates common law offences i.e., fraud or theft.

The results of the DPI reflected that 2% of CIS Managers have been subject to investigation by SAPS and 0.25% in the case of FSPs. It was noted that a total of 0.9% of FSPs were defrauded by clients and 1.04% reported that their business was defrauded by employees. In the case of CIS Managers, 6% indicated that their business was defrauded by a client and no accounts of employees defrauding the business.

To the degree indicated in the DPI, corrupt deals are not prevalent in the CIS and Financial Advisory and Intermediary Services sectors. 2% of CIS Managers reported that their business was approached with a corrupt deal and 0.46% in relation to FSPs.

4. Proceeds of crimes seized in the CIS and Financial Advisory and Intermediary Services sectors during 1 April 2018 – 31 December 2020

According to the Asset Forfeiture Unit of the NPA, there were a few cases where employees of insurance brokers collaborated with clients to submit fraudulent claims. They also dealt with several cases where persons fraudulently misrepresented themselves as insurance brokers. There are also numerous matters where insured persons submitted fraudulent claims.

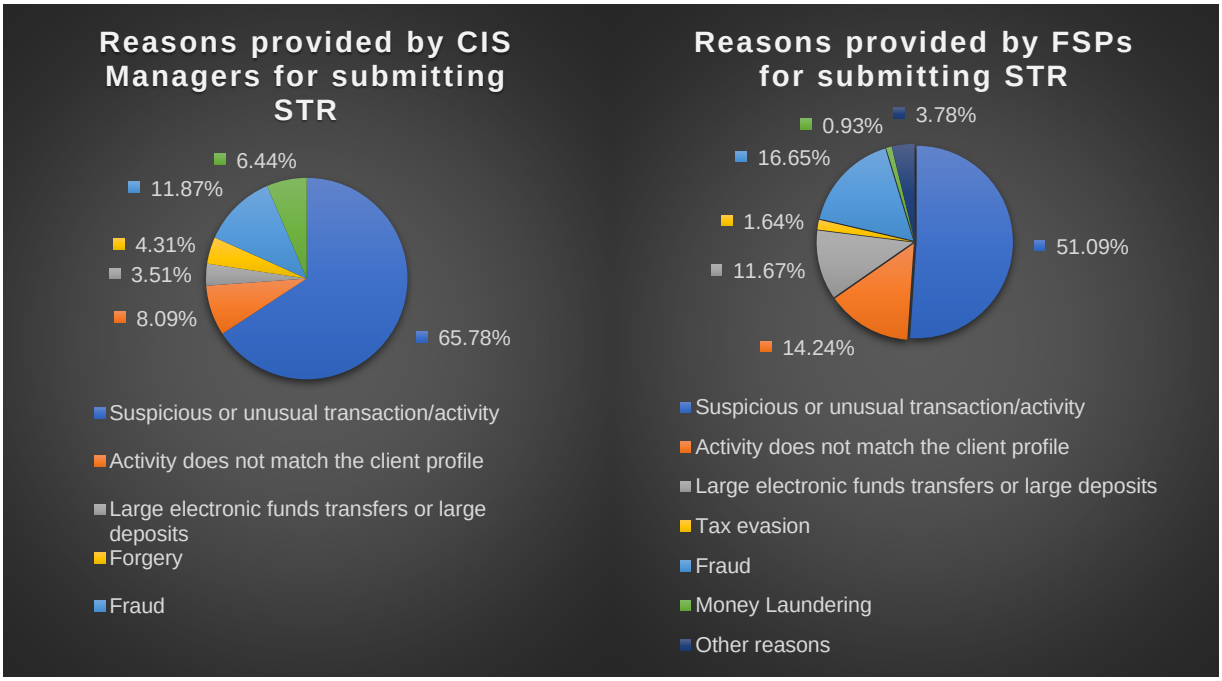
5. STRs and TPRs submitted by the industry

5.1. STRs

During the period under review CIS Managers and FSPs submitted 360 and 10 553 STRs respectively, to the FIC. This is an increase of from the previous period under review (2016/17 - 2017/18 financial years). The increase could be attributed to a better understanding of their reporting obligations. Some institutions have also automated STRs.

The value of the STRs submitted to the FIC by CIS Managers and FSPs amounted to R182 million and R3 450 million, respectively.

Compared to all other sectors, the number of STRs submitted by CIS Managers and FSPs are relatively low as it only accounts for 0,03% and 0,9%, respectively, of all STRs submitted.



- As at 31 December 2020 a total of 60 CIS Managers and 8409 FSPs were registered with the FIC.
- During the 2019/20 financial year, 10 CIS Managers submitted at least one STR to the FIC and 23 CIS Managers similarly submitted at least one STR in the 2020/21 financial year. A total of 6 out of the 10 CIS managers that submitted STRs to the FIC during 2019/20 submitted 5 or more STRs. A total of 5 out of the 23 CIS managers that submitted STRs to the FIC during 2020/21 submitted 5 or more STRs.
- During the 2019/20 financial year, 81 FSPs submitted at least one STR to the FIC and 94 FSPs similarly submitted at least one STR to the FIC in the 2020/21 financial year. A total of 29 out of the 81 FSPs that submitted STRs

to the FIC during 2019/20 submitted 5 or more STRs. A total of 23 out of the 94 FSPs that submitted STRs to the FIC during 2020/21 submitted 5 or more STRs.

- Both CIS Managers and FSPs indicate that the main reason for submitting STRs related to suspicious and/or unusual transactions/activities mentioned in section 29 of the FIC Act (66% and 51%, respectively). Section 29 of the FIC Act requires AIs to report transactions if:
    - The business has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
    - A transaction or series of transactions to which the business is a party –
        - Facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
        - Has no apparent business or lawful purpose;
        - Is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act;
        - May be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax, duty or levy imposed by legislation administered by the Commissioner of the South African Revenue Service;
        - Relates to an offence relating to the TF and related activities; or
        - Relates to the contravention of a prohibition under section 26B; or
    - The business has been used or is about to be used in any way for ML purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.
- The other reasons submitted by CIS Managers for submitting STRs to the FIC relate to (in order of most reported):
    - Fraud (12%);
    - The activity does not meet the profile of the client (8%);
    - Forgery (4%); and

- Large electronic transfers or deposits (3,5%).

- The other reasons submitted by FSPs for submitting STRs to the FIC relate to (in order of most reported):
  - Fraud (17%);
  - The activity does not meet the profile of the client (14%);
  - Large electronic transfers or deposits (12%); and
  - Tax evasion (1%).

No TPRs were submitted by CIS Managers or FSPs during the period under review.

The FSCA also gave consideration to STRs submitted by other AIs (Banks, Insurers, AUs, motor vehicle dealers etc.) where the subject matter was a CIS Manager or FSP.

- A bank reported a CIS Manager for receiving a large sum of money electronically;
- A total of 84 STRs were reported where the FSP was a payor (source party) and 51 STRs were reported where the FSP was a payee (destination party). The majority (64%) of the STRs related to suspicious or unusual transactions as mentioned in section 29 of the FIC Act. Other reasons related to:
  - Large electronic transfers;
  - The activity does not meet the client profile;
  - Reactive reporting where the institution received a subpoena from the SAPS or a request from the FIC; and
  - Fraud.

With regards to **PF**, CIS Managers and FSPs incorrectly reported clients appearing on a sanction/ watch list and contravention of the duty to freeze property, financial services or support of clients appearing on the resolution of the Security Council of the United Nations.

6. ML/TF trends in the industry

“Profit is fundamental to the goals of most crime, and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds” (FATF, 2010). Launderers generate proceeds in a myriad of various ways. But the primary stages of ML remain the same for all crimes:

(a) placement of the criminal proceeds into the financial or other transfer system;
(b) layering the funds so as to conceal their original source; and
(c) integration into the legitimate financial markets such as authorised users of an exchange, collective investment schemes and financial service providers.

6.1. CIS Managers

The following ML techniques are observed in the sector:

- The customer purchases a participatory interest in a CIS product using a single large sum of money particularly with an unusual payment method such as large cash lumpsums or cash equivalent like cheques.
- Paying a large sum of money into a CIS product and then disinvesting the money from the product by requesting the money to be paid to fictitious beneficiaries.
- Payments for participatory interest via third parties.
- Change of beneficiaries of a trust which cannot be satisfactorily explained.
- Unusual and frequent redemptions from the portfolio, especially when pay-out is made to a third party.
- Pre-signed application forms.
- Anonymous clients or clients with false or fictitious names.
- Reluctance to provide customer due diligence information.

Case scenario

The subject received a loan to purportedly purchase a house. He invested around 25% of the loan by putting a lump sum into a unit trust. He later withdrew the investment early to pay back the loan (capital and interest), making up the shortfall through other funds whose source is unknown. The use of proportion of the loan to purchase a policy combined with the unexpectedly early repayment of the loan led to the accountable institution filing a suspicious transaction report with the FIC. The FIC's investigation revealed that the unit trust holder was recently featured in the investigation of a cash in transit heist, and he had used fraudulent documents to prove the sources of his income and wealth.

6.2. FSPs

The following ML techniques are observed in the sector:

- Purchase of a product inconsistent with the customer's need.
- Purchase (or funding) of a product that appears to exceed a customer's known income or liquid net worth.
- Unusual payment methods, such as large cash lumpsums or cash equivalents such as cheques.
- Large payments made via several smaller payment amounts.
- Little or no concern by a customer for the performance of a product.
- Great concern about early termination features.
- Pre-signed application forms.
- Unusual and frequent claims against a financial product, especially when pay-out is made to a third party.
- Change of beneficiaries which cannot be satisfactorily explained.
- Payment for products via third parties.

- Unusual overpayment of premiums followed by a request to return overpaid amounts.
- Early redemption of policies which cannot be satisfactorily explained.

Case scenario

A law enforcement operation identified an accountant, Mr X, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drug trafficking led by Mr Y. Mr X's role was mainly that of a "legal and financial consultant". His task was to analyse the technical and legal aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these investments appear lawful from a fiscal stance. He was also trying as much as possible to make these investments profitable. Mr X was an expert in banking procedures and sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to Mr Y.
Mr X operated by subdividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by letters of credit as a warrant for commercial contracts which were later invested in other commercial activities.

The ML trends in the CIS and Financial Advisory and Intermediary Services sectors appears to be isolated and not widespread in these sectors.

There are currently no TF or PF trends in the CIS and Financial Advisory and Intermediary Services sectors in South Africa.

E. SECTOR VULNERABILITY ANALYSIS

The ML vulnerabilities in the CIS sector increase when clients in this sector are primarily international and there are high currency values generally managed in the sector. Moreover, the ML vulnerabilities are derived from the marketing of funds in foreign jurisdictions by foreign brokers. Although, many foreign based funds are managed by local fund administrators, the risks of ML to such funds appear to come mainly from foreign investors. The attractiveness of offshore funds as an investment vehicle for the proceeds of foreign tax crimes, international fraud or international corruption is believed to be well-established. The clients are often high-net worth individuals and/or Prominent Important Persons, who are considered an elevated vulnerability for ML.

A significant proportion of investment products and life insurance policies are sold through FSPs where the product provider will have limited or no direct contact with the client. In several cases, the FSP has the initial interaction with the customer. Accordingly, FSPs are more likely to be exposed to the layering and integration stages of ML and TF, rather than placement stage. The highest risk facing FSPs is aiding and abetting clients in committing ML and TF offences, including tax evasion.

The DPI results illustrated that ML vulnerabilities were informed by the following:

1. Clients

1.1. Types of clients

Amongst different types of clients for CIS Managers, 78% had a client base which consisted of a majority of natural persons and 57% in respect of FSPs' clients. 56% of CIS Managers reported that their client base includes a majority of legal persons, with only 14% reporting that trusts make up a majority of their clients.

A total of 19% of FSPs indicated that legal persons comprised the majority of their clients and 7.93% in respect of trusts making up a majority of the client base. In

relation to partnerships, a total of 2% of CIS Managers reported that they have partnerships as a majority of their client base and 5.52% in the case of FSPs' clients.

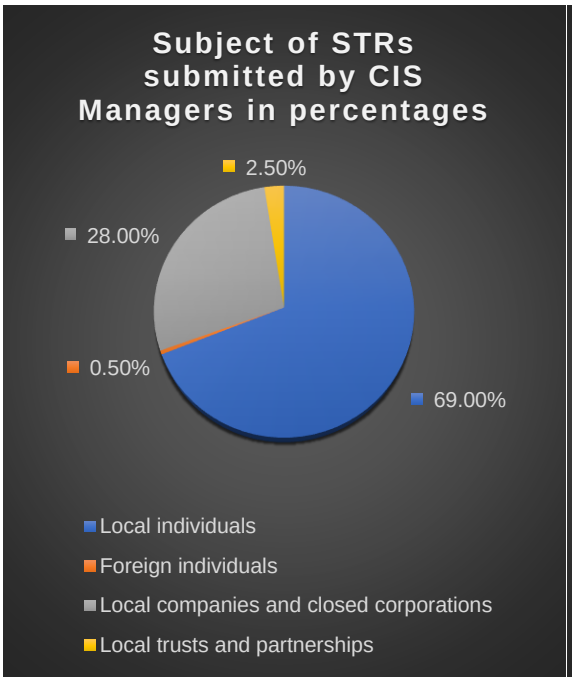
1.2. Prevalence of foreign based clients

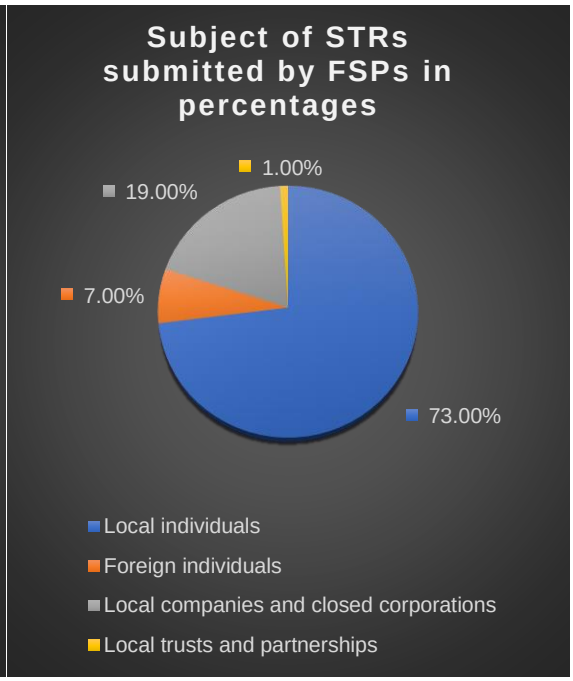
Most clients in respect of which financial services are rendered are local clients. A total of 2% of CIS Managers described that the majority type of their clients is foreign based and 2.21% FSPs render financial services to a client base that comprises of a majority of foreign based clients.

1.3. Prevalence of high-risk clients such as foreign prominent public officials or domestic prominent influential persons

A total of 0.24% of FSPs indicated that foreign prominent public officials form a majority of their client and 0.84% in respect of domestic prominent influential persons as a majority of the client base. A total of 4% of CIS Managers reported that they have domestic prominent influential persons as a majority of clients in respect of whom financial services are rendered and 2% indicated that foreign prominent public officials comprise a majority of their client base.

In terms of STRs submitted, the majority of STRs were reported on South African individuals by both CIS managers and FSPs.


Subject of STRs submitted by CIS Managers in percentages
2.50%
28.00%
0.50%
69.00%
Local individuals
Foreign individuals
Local companies and closed corporations
Local trusts and partnerships


Subject of STRs submitted by FSPs in percentages
1.00%
19.00%
7.00%
73.00%
Local individuals
Foreign individuals
Local companies and closed corporations
Local trusts and partnerships

Products and Services

CIS Managers[8] and FSPs offer clients a wide range of financial products and render services in respect of financial products to a wide range of clients. A total 60% of CIS Managers have indicated that they render financial services in respect of investment products to clients and 42.08% of FSPs render financial services in respect of investment products.

1.4. Offshore exposure

Investment with offshore exposure is very prominent in the CIS sector. Most CIS Managers (70%) render financial services in respect of products with offshore exposure. In the case of the financial advisory and intermediary services sector, a total of 28.57% of FSPs render services in respect of products with offshore exposure. While investments with offshore exposure may be high, offshore investments are subject to South African Exchange Control Regulations.

From a flow of funds in an out of South Africa perspective, a lot of money is leaving South Africa and flowing back to South Africa in the two sectors as can be seen from the table below. This increases the vulnerabilities of these sectors to ML/TF/PF abuse.

Sector	Inflow		Outflow	
	2019	2020	2019	2020
CIS Managers	R85 billion	R125 billion	R79 billion	R110 billion
FSPs	R74 billion	R100 billion	R59 billion	R95 billion

[8] CISCA Board Notice 90 of 2014 determines the securities and assets that a CIS can invest in, and the limits and conditions under which securities and foreign exchange for investment may be included in a CIS portfolio.

1.5. Exposure to crypto assets

The rendering financial services in respect of products with exposure to crypto assets is not prevalent in the CIS and Financial Advisory and Intermediary Services sectors. It was noted that 2% of CIS Managers and 0.63% FSPs reported that they render financial services in respect of products with crypto asset exposure[9]. High exposure to crypto assets makes the sectors more vulnerable to misuse by criminals to launder money and fund terrorism.

1.6. Unlisted Securities

Unlisted securities are financial instrument that are not traded on a formal exchange but Over-the-Counter (OTC) and subject to little or no regulatory oversight. Most CIS Managers and FSPs do not render financial services in respect of investments in unlisted securities. A total of 4.35% of FSPs and 12% in the case of CIS Managers provide financial services in respect of investments in unlisted securities. Many transactions are concluded electronically and across international borders with possibly relative or complete anonymity which can make investments in unlisted securities attractive to those who would abuse it for illicit purposes, including ML and TF.

1.7. Foreign Exchange (Forex)

None of the CIS Managers render financial services in respect of investments in forex products. A small percentage (2.71%) of FSPs render financial services in respect of forex. Transactions in forex are particularly vulnerable to abuse because criminals may move their illegal funds through multiple forex brokers or FSPs, using different currencies, to disguise the origin of the illicit funds and integrate them within the financial system.

[9] The DPI questionnaire was general and did not specifically enquire whether the exposure to crypto assets is direct or indirect.

1.8. Private Equity

It was noted that rendering of financial services in respect of private equity in both the CIS and Financial Advisors and Intermediary Services sectors is very low. 2% of CIS Managers and 4.11% of FSPs render financial services in respect of private equity. The prevalence of financial services in respect of private equity may expose CIS Managers and FSPs to being used to facilitate financial crime, including ML in the context of capital raising and transactional activity to reintegrate illicit funds into the financial system.

2. Distribution Channels

2.1. Distribution of products through other FSPs, group entities or third parties

Engagements with clients via persons acting on behalf of clients are not prevalent in the CIS and Financial Advisory and Intermediary Services sectors. 7.41% of FSPs indicated that they have engaged with third parties, whereas 40% of CIS Managers reported that they have entered engagements with persons acting on behalf of clients.

A total of 6% of CIS Managers and 2.91% of FSPs engage with clients through juristic representatives.

2.2. Non-face-to-face transacting using telephone or internet

A total of 18% of CIS Managers described that the majority type of engagement with clients is face-to-face and 56.15% in the case of FSPs. A low percentage of CIS Managers (38%) and FSPs (43.93%) indicated a majority of their engagements with clients as being telephonic. However, it was noted that many of CIS Managers (82%) mainly engage with clients electronically. Only 44.88% of FSPs make use of electronic engagements with clients as a main channel of distribution.

Over the years criminals have been increasingly turning to online payment services and gift cards (through both prepaid cards and store gift cards) to move illicitly

acquired funds because they provide a level of anonymity. Engagements with clients via mobile applications is not prevalent in both the CIS Managers and Financial Advisors and Intermediary Services sectors. 2% of CIS Managers engage with clients via mobile applications and 4.82% in respect of FSPs as a major distribution channel.

Engaging with clients face-to-face lowers anonymity and therefore reduces ML/TF risks.

3. Geographies

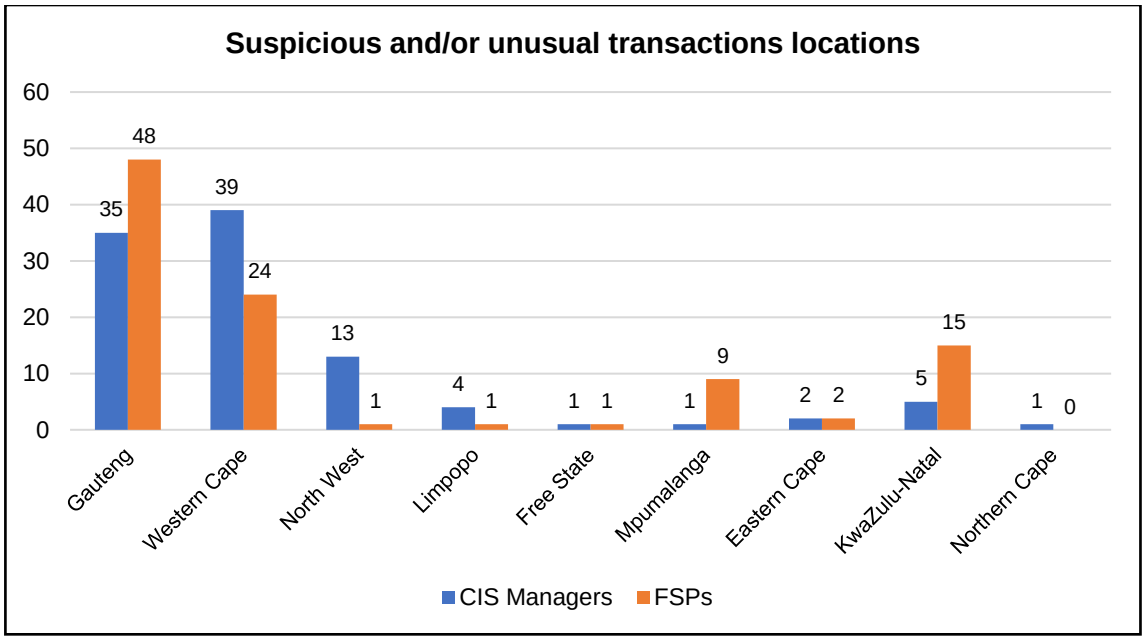
3.1. Residence of clients in sanctioned jurisdictions

None of the CIS Managers reported having clients that have appeared on UN Sanction List. A very low percentage (0.46%) of FSPs reported that they have clients that have appeared on the UN Sanction List in the past 12 months.

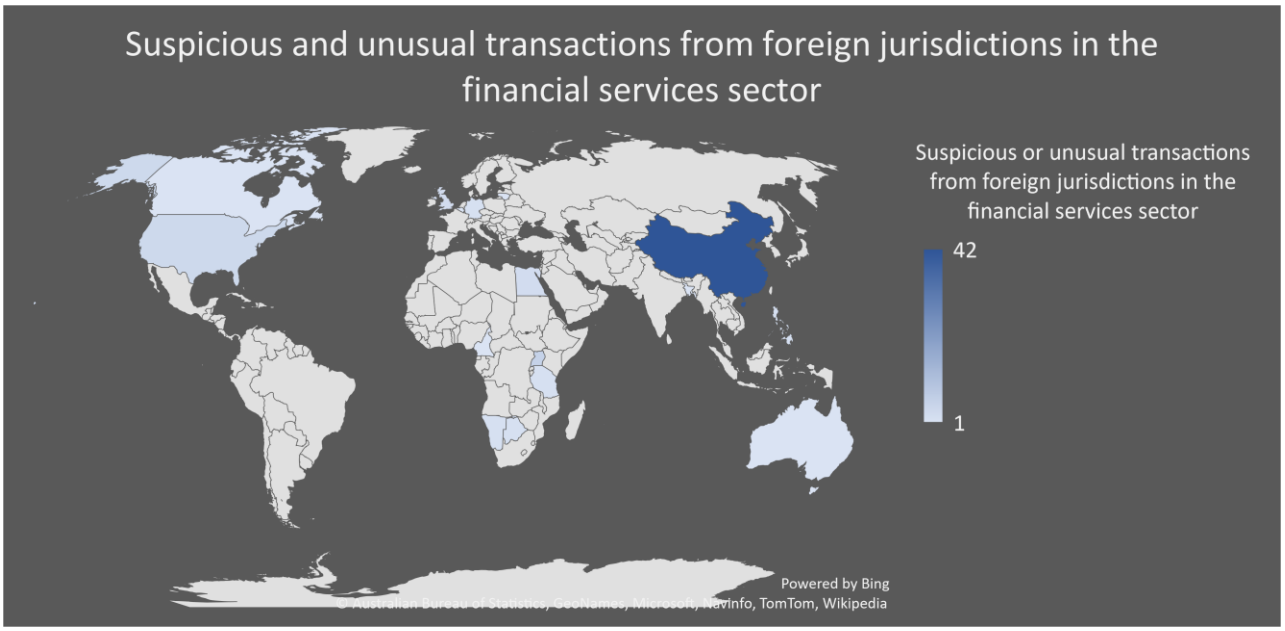
3.2. Domiciled or operations outside of South Africa

Most CIS Managers are domiciled or operate in South Africa, with only 2% operating in foreign jurisdictions. Similarly, most FSPs are domiciled or operate in South Africa. It was noted that 1.42% of FSPs operate in foreign jurisdictions.

Transactions emanating in STRs are in various locations within South Africa. Most transactions in the CIS sector are located in the Western Cape. Whereas most of transactions in the Financial Advisory and Intermediary Services sector are located in Gauteng. This is not unusual as Gauteng and the Western Cape are the financial hubs in South Africa.



From an international perspective, transactions in the Financial Advisory and Intermediary Services sector originating from China were the most reported by FSPs. See the graph below.



4. The use of cash

The use of cash in the economy is regarded as high risk as it allows for anonymity and ease of flow of funds. Cash also contribute to the masking of illicit activity.

During the period under review CIS managers and FSPs submitted 2,030 and 38,900 CTRs, respectively to the FIC. This is a reduction of CTRs submitted to the FIC by CIS managers and FSPs, respectively. The value of these transactions reported by CIS Managers and FSPs amount to about R125 million and R4 billion, respectively. Although there was a decrease in the use of cash in the sectors, it appears that the use of cash is still prevalent in the sectors, especially in the Financial Advisory and Intermediary Services sector.

The results of the DPI illustrated that 24% of CIS Managers filed CTRs and 3.5% in respect of FSPs in the last 12 months.

5. Mitigation of ML/TF risks

5.1. Risk assessment

All the CIS Managers indicated that they have conducted ML/TF risk assessment to identify ML/TF risks faced by the AIs' businesses. In the case of FSPs, a total of 3.06% have not conducted ML/TF risk assessments to identify risks faced by the AI.

The results of the DPI show that all the CIS Managers that responded have developed an RMCP and a total of 98% indicated that the RMCP provides for client identification and verification of beneficial owners. It was noted that 1.51% of FSPs have not developed an RMCP and 1.38% do not take appropriate steps as set out in the RMCP to identify beneficial owners.

All the CIS Managers indicated that they conduct client identification and verification on beneficial owners as set out in the RMCP.

5.2. Client due diligence (CDD)

A very high rate of CIS Managers and FSPs conduct CDD in line with the RMCP. A total of 2% of CIS Managers indicated that they do not conduct CDD in line with the RMCP, however most (98%) do establish and verify the identity of a client on a risk-based approach. With regards to FSPs, 1.2% indicated that they do not conduct CDD in line with the RMCP and 1.15% do not establish and verify the identity of clients on a risk-based approach to establish the type and extent of CDD that must be conducted.

5.3. Registration with the FIC

A total of 96% of CIS Managers have updated their registration details on the FIC GoAML portal. With regards to FSPs, a low percentage (2.51%) indicated that they have not updated their details.

5.4. Submitting of STRs by CIS Managers

The quality of the Section 29 reports submitted appeared to be predominantly complete. The reports contained information that the AI is expected by FIC to have as either part of the course of establishing a particular person's identity or the conducting of a particular transaction(s).

5.5. Submitting of STRs by FSPs

The quality of the Section 29 reports submitted appeared to be varied. Indicators relating to the contravention of a prohibition under section 26B of the FIC Act have mostly been used incorrectly, and the reported individuals do not relate to persons appearing on the Targeted Financial Sanctions lists.

The quality of the Section 29 reports submitted appeared to be varied. The FIC noted that the following concerns that can be improved on in terms of submission of STRs:

- Potential late reporting;
- Quality of transaction location provided;

- Minimum required information needs to be submitted for payors and payees.

According to the results of the DPI, 56.61% of FSPs have written guidelines on what constitutes reports in respect of suspicious and unusual transactions and activities.

In terms of section 27 of the FIC Act, the FIC may issue a request to an AI to confirm if a person/entity is a client of them and if they acted for a client. The FIC sent out 149 and 1898 requests in terms of section 27 of the FIC Act to CIS Managers and FSPs, respectively. CIS managers and FSPs only responded 110 and 963 requests, respectively. This is a compliance percentage of 74% and 51% which are relatively low. It therefore appears that a large percentage of CIS managers and FSPs are not adhering to this obligation of the FIC Act or may be slow in providing feedback. The response rate is similar to compliance with section 32 of the FIC Act. Section 32 authorises the FIC to request additional information from an AI that submitted an STR and CTR.

5.6. Non-compliance sanctions imposed by regulators

In the past 12 months, none of the CIS Managers were sanctioned by a regulator for non-compliance with a law. 0.57% of FSPs indicated that have been sanctioned by a regulator for the contravention of a law.

F. CONSEQUENCES

Consequences refer to the impact or harm that ML/TF may cause and includes the effect of the underlying criminal and terrorist activity and, in this case, the non-banking financial sector supervised by the FSCA.

1. Harm or loss to clients

Clients may lose confidence in the financial sector which will result in them not investing money in the sectors. Clients may also suffer financial losses because of fraudulent activities on their accounts. Clients may also suffer emotional damages as a result of the ML/TF activities.

2. Harm or loss to individual financial institutions

The controls put in place by the sector will minimise any harm or damage caused by ML/TF through these institutions. The controls largely refer to compliance with the FIC Act.

Other harm or loss consequences include:

- The financial institution may suffer financial losses as a result of being abused for criminal purposes;
- The financial institution may suffer reputational damage and as a result may lose clients;
- Other financial institutions may decide not to do business with the financial institution that was abused for ML/TF purposes;
- Administrative sanctions being imposed by the FSCA on the financial institution or even debarments of individuals or revocation of the license;
- Criminal prosecution of persons in the financial institution for assisting another to benefit from proceeds of unlawful activities or to finance terrorist activities;
- This may even lead to unemployment;
- Increase in costs to prevent a reoccurrence of the ML/TF/PF or to change the reputational damage to attract more clients.

3. Harm or loss to the financial sector

The biggest harm to the sector is reputational damage. This will lead to a reduction of investments. The FSCA may also suffer reputational damage. Money launderers may abuse the sector even more if it has a bad reputation. This may also lead to financial exclusion and a lack of transformation.

4. Harm or loss to the South African economy

The following harm or loss to the South African economy will occur should ML/TF occur in the industries assessed:

- Economic distortion and instability;
- Increase in criminal activity;
- Undermine integrity of the financial system;
- Affect savings and investments;
- Reduced revenue;
- Possible blacklisting of South Africa by organisations e.g., FATF.

FINANCIAL SECTOR CONDUCT AUTHORITY