www.fsca.co.za

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

SECURITIES SECTOR

ISSUED BY THE FINANCIAL SECTOR CONDUCT AUTHORITY

FEBRUARY 2022

FSCA

Financial Sector Conduct Authority

Key statistics

*** As at 31 December 2020**

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

The number of Exchanges*

5

Number of AUs*

134

Number of authorized ODPs*

7

Total value of assets under management by AUs*

R1,275 Trillion

Total market capitalization AUs*

R17,87 Trillion

Number of trades per day by AUs*

467 Million

The value of equity trades per day by AUs*

R23 billion

Percentage of equity traded by foreigners (AUs)*

17%

Number of STRs filed by AUs**

1031 to the value of R1,697,453,318

Number of CTRs filed by AUs**

99864 to the value of R11,935,036,369

Number of TPRs filed by AUs**

0

Market abuse/ insider trading cases opened**

94

TABLE OF CONTENTS

GLOSSARY

AFU	Asset Forfeiture Unit of the National Prosecuting Authority
AI	Accountable institutions referred to in Schedule 1 to the FIC Act.
AML	Anti Money-laundering
AML/CFT	Anti Money-Laundering and/or Combating the Financing of Terrorism
Authorised User	Authorised user of an exchange as defined in the Financial Markets Act, 19 of 2012
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
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FIC Act	Financial Intelligence Centre Act, 38 of 2001
FMA	Financial Markets Act, 19 of 2012
FSCA	Financial Sector Conduct Authority
FSP	Financial Services Provider requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, 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 18 of 2017 and a health service benefit provided by a medical scheme as defined in section 1(1) of the Medical Schemes Act, 131 of 1998.

ML/TF/PF	Money Laundering and/or Terrorist Financing and/or Proliferation of Finance for weapons of mass destruction
NGO	Non-Government organization
NPA	National Prosecuting Authority
NPO	Non-Profit Organization
ODP	Over-the-Counter Derivatives Provider
OTC	Over-the-Counter derivatives market
POCA	Prevention of Organised Crime Act, 121 of 1998
PEP	Politically Exposed Person
PF	Proliferation of finance for weapons of mass destruction
RUSI	Royal United Services Institute
SAPS	South African Police Service
SARS	South African Revenue Services
SRA	Sector Risk Assessment
SSA	State Security Agency
STR	Suspicious Transaction Report(ing) and Suspicious Activity Report(ing)
Strate	South Africa's principal Central Securities Depository (CSD)
TPR	Terrorist Financing Report in terms of section 28A of the FIC Act
TF	Terrorist Financing

1. EXECUTIVE SUMMARY

Securities markets are often characterized by complexity, internationality, a high level of interaction, high volumes, speed and anonymity. Many of the core economic functions of securities markets are critical to efficient price-formation and capital allocation, which contribute to economic growth, financial inclusion, high levels of investment and overall prosperity of South Africa. However, some of the same characteristics associated with the sector can create opportunities and safe havens for criminals. The FATF Report: Money Laundering and Terrorist Financing in the Securities Sector (October 2009) outlines the main ML/TF vulnerabilities in the securities sector.[1]

This assessment covers AUs and ODPs. The FSCA is a supervisory body in terms of the FIC Act and responsible to supervise AUs which are accountable institutions in terms of the FIC Act. ODPs are not accountable institutions in terms of the FIC Act, however, the FSCA authorises and supervises this sector in terms of the FMA Regulations.

The risk assessment can be used by AUs and ODPs as an important resource for feedback on ML/TF/PF risks in the sectors. Based on this assessment, the FSCA expects AUs and ODPs to refine their compliance controls and mitigation strategies. In addition to identifying and monitoring risk factors that may apply to their individual businesses, this risk assessment seeks to assist AUs and ODPs in reporting suspicious and unusual transactions or AML/CFT related matters to the FSCA and FIC.

Below is a summary of the findings of the risk assessment conducted on the above-mentioned sectors in order 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 ML/TF/PF.

In conducting the sector risk assessment, the FSCA followed the FATF guidance which evaluates three areas namely **criminal threats**, **vulnerabilities** and **consequences**. The sector risk assessment report consists of input from the following sources:

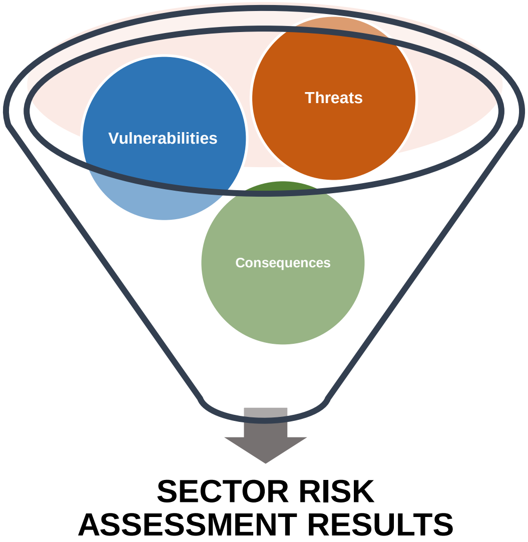
- analysis of survey results from AUs and ODPs.
- reports and intelligence from a variety of agencies, including FIC, FSCA Enforcement Division, South African Reserve Bank, Exchanges, Strate,

[1] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf

SAPS, SARS and other government agencies.

- Consultations with industry experts.

In accordance with this methodology, the primary objective is to identify, understand, and disrupt ML/TF/PF and other criminal offences targeting the Securities sector in South Africa.



1.1. Criminal Threats

A total of **3.1%** of AUs and **5,3%** of ODPs that participated in the survey indicated that their business has been abused for criminal activity during the period under review.

The most common issues reported in the STRs which point to possible ML/TF/PF threats are:

- Fraud;
- Large electronic transfers;
- Unexplained account activity;
- Rapid disposition of funds; and
- The transaction/activity does not match the profile or expected transaction patterns of the client;

Law enforcement and intelligence agencies assessed the ML/TF/PF threats in the securities sector as **LOW** during the period under review.

Money laundering

Both AUs and ODPs indicated that they suspected their business are being abused for ML. A total of 1,031 and 1,249 STRs were filed by AUs and ODPs, respectively.

TF/PF

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

Fraud

A total of **8,69**% of STRs submitted by AUs relate to fraud. A total of **10.05%** of surveyed ODPs indicated that they have reported suspected fraud to the FIC.

Insider trading and market manipulation

During the period under review, the FSCA investigated 91 cases of insider trading/ market abuse. Included in the list were cases of market manipulation initiated from foreign countries, particular from the United States of America and the United Kingdom through Direct Market Access platforms. The most popular products featuring insider trading/ market abuse are Shares, Derivatives (Futures, CFDs and Options) and Bonds.

Tax evasion

A total of 0,48% of STRs submitted by AUs relate to suspected cases of tax evasion.

1.2. Vulnerabilities

Clients

Entities operating in the securities sector are exposed to a wide array of client types. Amongst different types of clients for AUs **78.6%** consisted of natural persons and **54.76%** in respect of ODPs. AUs reported that their clients also include companies, trusts, and foreign entities. A total of **59,51%** of equities was traded by local companies while foreign companies traded **3,63%** of equities. Trusts traded **6,26%** of equity. The large presence of legal persons (local and foreign) makes the securities sector vulnerable to ML/TF/PF.

Vulnerabilities also increase due to AUs and ODPs having a large percentage of clients that are considered complex or multi-layered.

The use of third parties and agents

There are significant vulnerabilities associated with the use of third parties and agents by some entities, especially when located in foreign jurisdictions or in the case of transaction and trading accounts held with different financial institutions, since it can be difficult to obtain client identification and authorisation forms, and to do verification on such parties as well as limited visibility into a client's trading activity. **27.69%** of the AUs provide securities services to prospective clients through intermediaries and/or third parties. **26.32%** of ODPs provide securities services to prospective clients through intermediaries and/or third parties.

Online services or non-face-to-face transacting

Clients' use of online services to open accounts and trade creates additional challenges for AUs and ODPs mostly due to cybercrime. A high number of clients make use of non-face-to-face interactions with AUs and ODPs. **70.77%** of AUs included in the survey accept instructions on a non-face-to-face basis. **68.42%** of ODPs included in the survey accept instructions on a non-face-to-face basis

Products and services

The main products and services which were identified as vulnerable to criminal misuse were:

- **client accounts** in which funds in and out of the sector are primarily moved through general transaction and trading accounts.
- **trading** activity itself can be exploited by criminals, particularly insider trading and market manipulation, mostly due to the large volume of trades conducted each day and the speed with which trades are often executed.
- **off-market transfers** in which the transfer of shares, and their value, from one person to another without having to trade on an exchange can also be exploited.
- **third-party payments** in an instance where there is no apparent relationship between the AU and the third-party, transferring funds to third parties can lead to misuse, especially if funds are transferred or payment is made to foreign jurisdictions.

The use of cash

Cash can be deposited into general transaction accounts and quickly transferred between trading accounts, which makes the sector vulnerable to ML. **4.62%** of the AUs reported that they accept cash. A total of 45,219 CTRs and 54,645 CTRAs to the value of R12 billion was submitted to the FIC by AUs. However, there are some concerns whether these CTRs were filed correctly with the FIC, considering the threshold placed by the exchanges on AUs in terms of the exchange rules on the acceptance of cash. The ODPs which participated in the survey indicated that they do not accept cash.

Foreign Jurisdictions

The sector is exposed to foreign jurisdiction risks due to the percentage of ownership and trading in securities by foreign entities. **35.40%** of AUs included in the survey indicated that they have clients from foreign jurisdictions. ODPs reported that **43.40%** of their clients are foreigners. **26.3%** of the ODPs' clients are registered in countries that are on the FATF grey-list. **10.5%** of the

ODPs indicated that they have clients that reside or are registered in Syria, Sudan, Iran, Cuba, and North Korea. This increases the risk of PF in the ODP sector.

Mitigation of ML/TF/PF risks

AUs do have risk management and compliance programmes in place and do risk rate clients. Compared to the size of the sector (assets under management and trades per day) there appears to be an underreporting of STRs.

Despite ODPs not being classified as AIs s in terms of the FIC Act, ODPs that form part of a banking group still comply with the provisions of the FIC Act as witnessed through the number of STRs submitted by them.

1.3. Consequences

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 as a result of criminal misuse of the sector relate to financial losses and emotional distress. Financial institutions will suffer reputational damage, increased costs, and 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.

Overall ML/TF Risk Rating

The overall ML/TF/PF **threat, vulnerability and consequence** of the securities sector have been assessed as follows:

	Money laundering			Terrorist financing			Proliferation financing		
	Threats	Vulnerabilities	Consequences	Threats	Vulnerabilities	Consequences	Threats	Vulnerabilities	Consequences
AUs	LOW	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM
ODPs	LOW	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM

2. BACKGROUND

The FSCA conducted an SRA on AUs in 2018/2019 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 in order 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 FATF mutual evaluation of South Africa in this review. This report sets out the findings of the risk assessment conducted by the FSCA on the securities sector.

What has changed from the previous SRA report?

- The previous report set out the risk assessment of three sectors being **AUs**, **CIS Managers** and **FSPs**. This report focuses on the securities sector which also includes the OTC derivatives sector. The FSCA has prepared a separate report on CIS Managers and FSPs.

- The FSCA received updated information on ML threats and vulnerabilities for the period **1 April 2018 – 31 December 2020**.

- This report also considered TF and PF threats, vulnerabilities and consequences in the securities sector.

- Wider consultation with law enforcement and intelligence agencies as well as industry experts.

- The FSCA also conducted a risk assessment on the OTC sector for the first time.

Why has the FSCA conducted a SRA?

- The SRA assists the FSCA to identify, assess and understand their sector's ML/TF/PF risks. Once we understand the ML/TF risks, it helps to plan our supervisory 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 prioritized.

- SRAs should be reviewed and updated regularly in order to remain relevant by:
    - setting out the frequency and triggers for updates to sectoral and entity risk assessments under the supervisory risk assessment methodology;

- identifying and assessing emerging risks and trends within their supervised population, then revising the risk assessment on an ongoing basis; and 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. AUs and ODPs should consider the risks identified by the SRA and amend their own risk assessments where applicable.
- The FSCA can provide guidance and clarify the supervisory expectations for entity-level risk assessments.

Although there were some threats, vulnerabilities and challenges identified during the review of the risk assessment, there was no change in ratings in relation to AUs from the previous period of assessment. The Securities Sector remains **MEDIUM** risk for ML/TF/PF. The main reason for this rating relates to the vulnerabilities/inherent risks in the sector, specifically client type and jurisdictional areas.

How should AUs and ODPs use this SRA?

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

3. RISK ASSESSMENT METHODOLOGY

The FSCA followed the methodology as recommended by the FATF[2]. In terms of the methodology three areas needs to be evaluated namely criminal threats, vulnerabilities and consequences. In assessing the risks related to ML/TF/PF, questionnaires and FATF guidelines were used with data collection from AUs and ODPs.

Threats refer to criminal threats, including the extent and nature of ML/TF risks that face the industry or sector. In assessing threats, the following information was considered:

- Materiality;
- ML/TF/PF cases investigated and prosecuted in the securities sector during 1 April 2018 – 31 December 2020;
- Predicate offences investigated and prosecuted in the securities sector during 1 April 2018 – 31 December 2020;
- Proceeds of crime seized in the securities sector during 1 April 2018 – 31 December 2020;
- Reporting information submitted by the sector to the FIC; and
- ML/TF trends in the industry.

Vulnerabilities or inherent risks refer to the features and characteristics of the industry or sector 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;
  - Clients that are part of a complex or multi-layered structure of ownership or control.

- **Products**
  - Cash intensity;
  - Whether products allow clients to remain anonymous;
  - Complexity of the products;
  - Cross-border transactions;
  - Third party payments or deposits;
  - Transactions that are not settled through an exchange;
  - Services or products that are not subject to regulatory approval or oversight;
  - Financial instruments that are quick to execute;
  - Financial instruments that have been discontinued;

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

- Unusual or suspicious activity.

- **Distribution channels**
  - Dealings with non-banked, walk-in or occasional clients;
  - Distribution of products through intermediaries or third parties;
  - Non-face-to-face transacting using telephone or internet;
  - The use of innovative technologies or payment methods (fintech or crypto assets).

- **Geographic locations**
  - Residence of clients in high-risk jurisdictions;
  - Residence of clients in sanctioned jurisdictions;
  - Use of intermediaries outside South Africa;
  - Residence of clients in countries with strict secrecy laws.

- **The Use of Cash**
  - The prevalence of cash in the sector.

- **Mitigation of ML/TF risks**
  - Risk assessment conducted by the AUs and ODPs;
  - Client due diligence conducted by the AUs and ODPs;
  - Reporting of suspicious transactions by the AUs and ODPs.

Consequence refers to the impact or harm that ML/TF/PF 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 methods were used to collect data from a number of sources e.g., consultation with the FIC, NPA, SAPS, SARS, SARB, SSA, The South African Council for the non-proliferation of weapons of mass destruction, RUSI, the exchanges, Strate and industry experts as well as the results from sector surveys issued, review of internal records and databases and onsite & off-site inspections.

Each sector was 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 AU and OTC (ODP) sectors. 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 through 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.

Overall ML/TF/PF Risk Levels

The overall risk assessment of the securities sectors has been assessed as follows:

	Money laundering	Terrorist financing	Proliferation financing
AUs	**MEDIUM**	**MEDIUM**	**MEDIUM**
ODPs	**MEDIUM**	**MEDIUM**	**MEDIUM**

4. SECTORAL CRIMINAL THREAT ANALYSIS

Materiality

There are two main areas in the securities sector which are the focus of the report, being AUs and ODPs.

A. Authorised users (AUs)

AUs are persons authorised by a licensed exchange to perform one or more securities services in terms of the exchange rules. AUs can act as agents or as principal. AUs engage in the business of buying and selling securities listed on an exchange and match orders of buyers and sellers without taking ownership of the securities. AUs may hold membership in more than one exchange. Trading is usually conducted on an "execution only" basis; but can be on an "advised" or "managed account" basis. AUs can also offer custodian services.

South Africa has a mature securities sector that serve the domestic economy and the wider continent. The market capital is about R17.87 trillion and the assets under management is R1,275 trillion. This is significant compared to the assets under management by Banks[3]. South Africa has five licensed exchanges. Historically the JSE has operated the only licensed exchange in South Africa, however, in 2016/2017 the FSCA (formally Financial Services Board) awarded licences to four new exchanges.

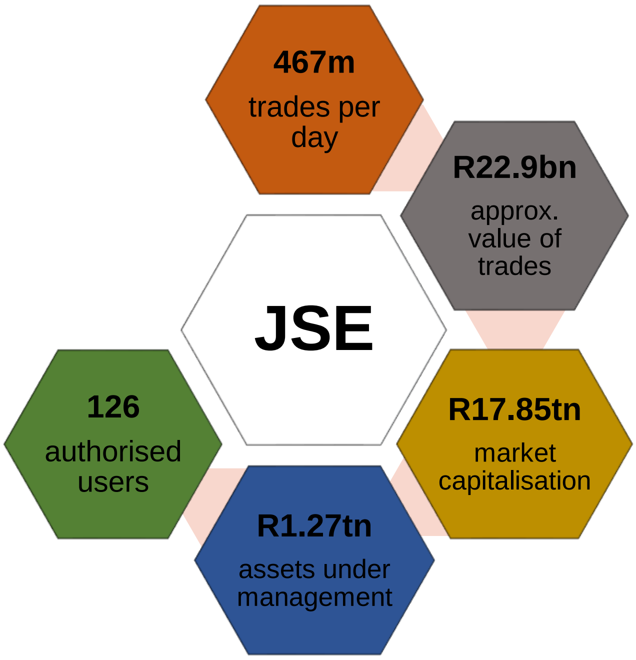
The five licensed exchanges in South Africa are:

(1) Johannesburg Stock Exchange (JSE)
(2) A2X (secondary listings exchange)
(3) 4Africa Exchange (4AX)
(4) ZAR X[4]
(5) Equity Express Securities Exchange (EESE)

Financial markets include the Equities market (incl. shares, REITs, ETFs), Debt market (incl. government bonds, corporate bonds, green bonds, repos) and the Derivatives market (incl. Equity Derivatives, Commodity Derivatives, Interest Rate and Currency Derivatives and Bond Derivatives).

[3] R5,517 billion as at end 2018.
[4] The exchange licence of ZAR X (Pty) Ltd (ZARX) has been suspended by the FSCA, with effect from 20 August 2021. The suspension is subject to litigation at the time of issuing this report.

Transactional Data reported by Exchanges



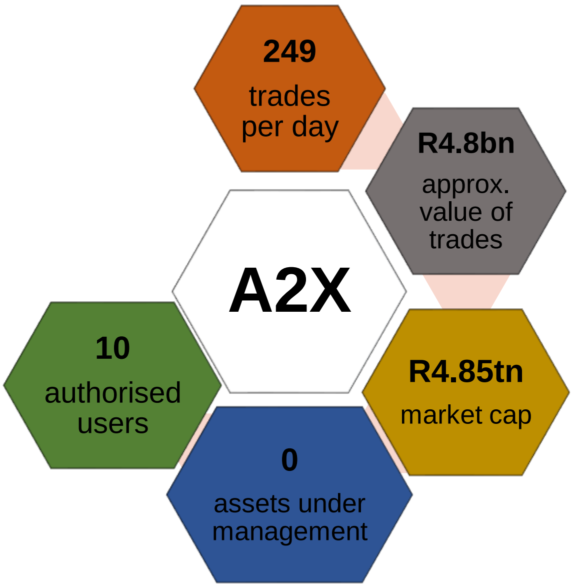
17% equity traded by foreign investors|

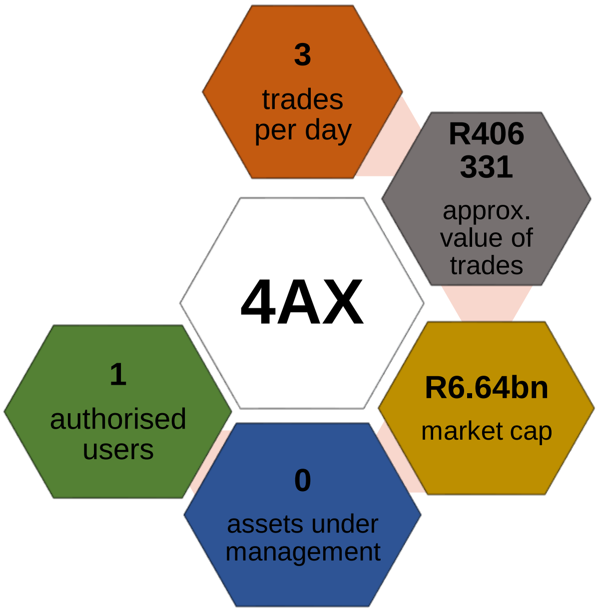
83% equity traded by local investors|

Markets| equities|

derivatives (equity, commodities, interest rate & currency|

debt|





0% equity traded by foreign investors| investors|

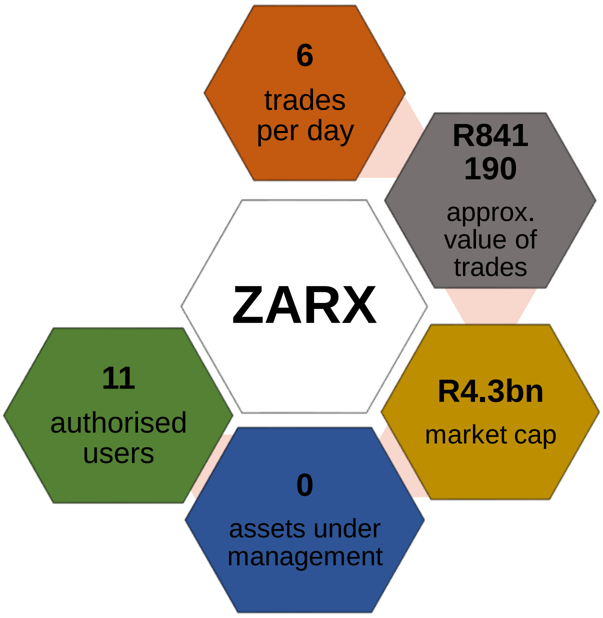
100% traded by SA investors|

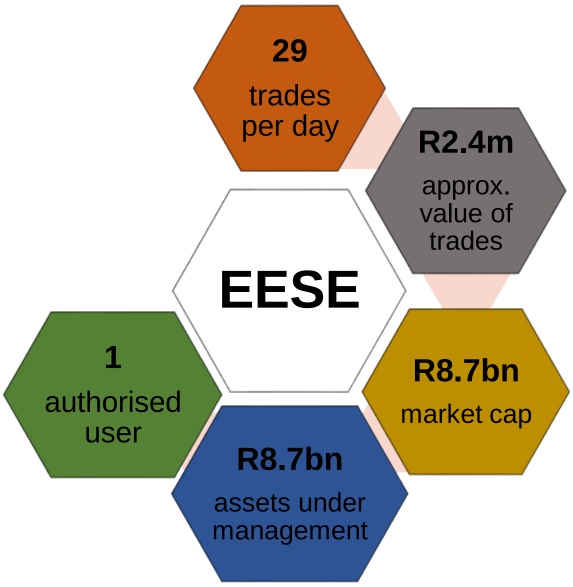
Markets| equities, ETNs and ETFs

11.25% equity traded by foreign

88.75% equity traded by SA investors|

Markets| equities and bonds





>1% equity traded by foreign investors|

<99% equity traded by SA investors|

Market| Equities

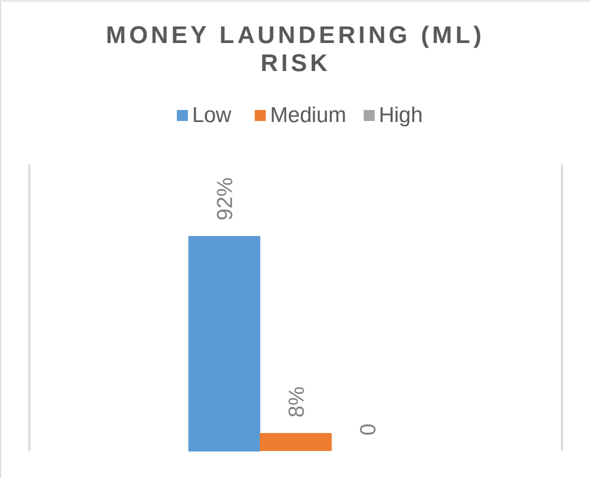
0% equity traded by foreign investors|

100% equity traded by SA investors|

Market| Equities

Money Laundering (ML)

The figure below shows the percentage of clients considered to be a ML risk by AUs:



92% of the AUs reported that they rate their clients low for ML risk and only **8%** rated their clients medium for ML risk. There were no AUs which identified their clients as rated high for ML risks. In the overall analysis, most clients were considered to be a low risk for ML.

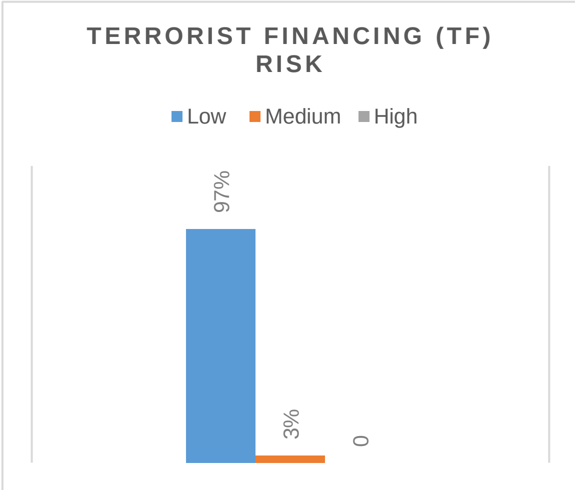
Terrorist Financing (TF)

The risk of TF related to the securities market was found to be very **LOW** by the AUs that participated in the survey.

Terrorist Financing Reports

There were no cases of possible TF reported in the last 5 years.

The figure below shows the TF risk ratings in the Securities Sector as submitted by participating AUs:



In a scale from low, medium to high (L, M, H), **97%** of the AUs scored their clients as a low possible consideration and **3%** as a medium consideration. There were no AUs that scored their clients as a high possible consideration for TF risk.

B. Over-the-counter Derivative Providers (ODPs)

On 9 February 2018, the Minister of Finance enacted into law the final version of the Regulations to the Financial Markets Act, 2012 ("FMA Regulations" or "FMA") which govern the provision of securities services under the FMA including in respect of OTC derivatives.
The FSCA authorised 7 ODPs during 1 April 2018 – 31 December 2020 of which 4 are local banks and 3 are foreign banks. A further 61 ODPs, of which 14 are banks,

have submitted applications to be authorized to trade in OTC derivatives.

The South African OTC derivatives market comprises mainly interest rate, forex, credit, currency and commodity derivatives.

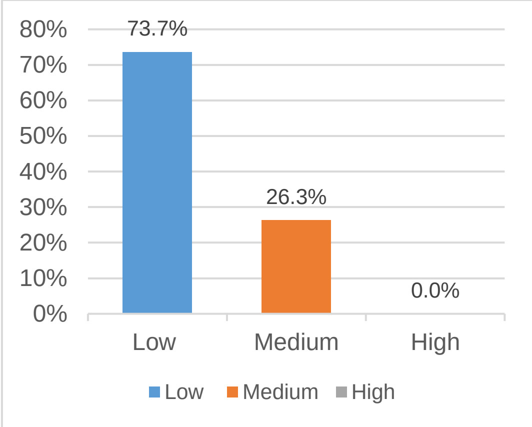
According to the independent research conducted by PWC[5], as at 30 June 2018, the analysis of size and composition of South African OTC derivatives market indicated that at an aggregate level, the total notional outstanding balance for the South African market as at 30 June 2018 was **R44.7 trillion**.

This indicated a 65% increase from the prior analysis conducted as at 30 June 2012, where the notional balance was **R27.7 trillion**.

As at 30 June 2018, 75% of the notional outstanding balance in the South African OTC derivatives market was dominated by interest rate derivatives.

Money Laundering (ML)

The figure below shows ODPs' clients' money laundering risk as per the results of the survey:



73.7% of ODPs' clients have a **LOW** ML risk.

Terrorist Financing (TF)

There were no reported cases of possible TF in the 5-year period under review. The risk of TF related to the ODPs' clients was found to be very **LOW**.

ML/TF/PF cases investigated and prosecuted in the Securities Sector during 1 April 2018 – 31 December 2020

Money laundering (ML)

There were no ML/TF cases investigated or prosecuted in the securities sector during the period under review.

Proliferation of financing (PF) risks

Proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions (TFS) obligations

[5] PricewaterhouseCoopers Incorporated. (2020). Independent research analysis exploring OTC derivatives central clearing for South African market participants. Report commissioned by The Banking Association South Africa. https://www.banking.org.za/reports/independent-research-otc-derivatives-clearing-sa/ (Accessed 31 August 2021)

referred to sections 26A-26C of the FIC Act. The source of proliferation financing risks would depend on a number of factors[6]:

- **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 for example as a result of delay in communication of designations at the national level, lack of clear obligations on financial institutions, failure on the part of financial institutions to adopt adequate policies and procedures to address their proliferation financing risks (e.g. weak Client onboarding procedures and ongoing monitoring processes, 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, and requires countries to freeze without delay the funds or other assets of, 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; and
(c) those owned or controlled by them.

No PF cases were investigated in the securities sector during the period under review.

Predicate offences investigated and prosecuted in the Securities Sector during 1 April 2018 – 31 December 2020

Money laundering 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

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

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 predicate offence. In order to prove money laundering, 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 money laundering. In the majority of the matters (**42%**), the predicate offence is indicated as fraud. Other predicate offences relate to dealing in drugs, abalone smuggling, racketeering and theft. This is supported by statistics from the FIC. There were, however, no ML prosecutions emanating from the securities sector.

A. Authorised Users (AUs)

Fraud

In the period between 1 April 2018 and 30 December 2020, **3.1%** of the AUs who participated in the survey agreed that their business was exploited for criminal activity. Two types of criminal activity are involved in these crimes:

- Fraudulent Activity was done on a client account; and
- Person or persons forged client’s documents in order to try and get access to a transaction.

6.2% of the AUs that participated in the survey were served with subpoenas; which included fraud claims, subpoenas which were stated as SAPS investigations and other reasons which were kept confidential.

Insider trading and market manipulation

Market abuse is a general term used to describe a wide range of types of unlawful behaviour in the financial markets including market manipulation, wash trading, insider trading, misappropriation, layering, unauthorized pooling, spoofing, front running and the like. Market abuse risk is relevant in the AML/CFT context for two principal reasons. Firstly, some forms of market abuse may constitute predicate offences for ML. Secondly, certain controls which financial institutions may be required to be implemented to comply with market abuse laws, in particular, the surveillance of trading activity, may also be of use in monitoring for suspicious activity for AML/CFT purposes. Such commonalities and efficiencies are to be encouraged so long as both market abuse and AML/CFT obligations are each fully met.

During the period under review, the FSCA opened 91 cases of insider trading/ market abuse. There were cases of market manipulation initiated from foreign countries, particular from the United States of America and the United Kingdom through Direct Market Access platforms. The most popular products featuring insider trading/ market abuse are Shares, Derivatives (Futures, CFDs and Options) and Bonds.

There is no particular trend for insider trading. The number of cases is consistent with both bull and bear markets. With regards to price manipulation, there is a trend whereby the FSCA has seen an increase in cases when individuals are under pressure because of a bear market who in turn have derivative exposure. They therefor manipulate the price to avoid margin calls.

The FSCA also had to deal with a matter regarding the contravention of section 81 of the FMA. The breach related to the misrepresentation by an entity of its financial performance in prior years which resulted in the restatement of its opening balance for the following reporting period.

The survey data indicated that criminal activity accounts for a significant portion of insider trading profits and market manipulation profits. **1.5%** of AUs were found to be buying or selling securities while possessing unpublished price sensitive information, and those securities were cash equities.

3.1% of AUs reported that they had clients who traded aggressively in cash equities just before a price sensitive market announcement.

1.5% of the AUs had clients whose trading activities did not align with their objectives or profiles. **1.5%** of AUs reported that they have clients that have engaged in trading activities that were inconsistent with their objectives or profiles and the type of securities traded is cash equities.

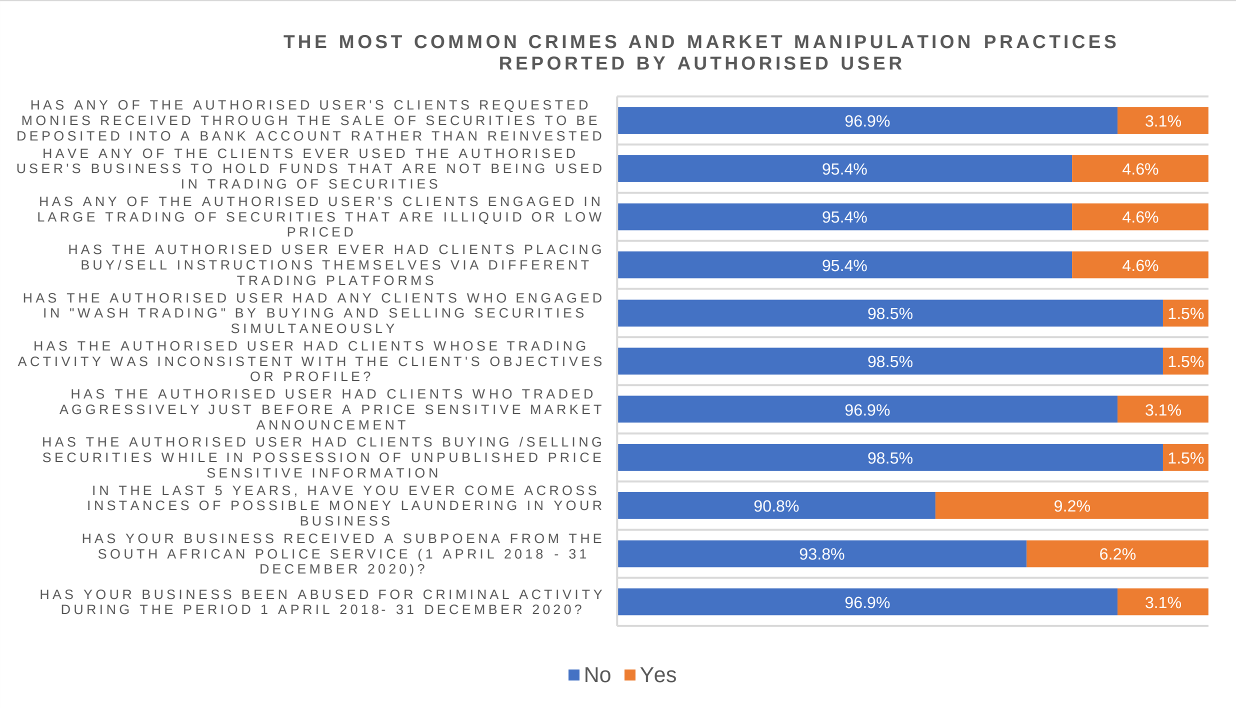
4.6% of the AUs reported that their clients placed their own buy/sell orders using different trading platforms.

4.6% of AUs had clients who traded large quantities of illiquid or low-priced securities. A total of 555 clients traded illiquid or low-priced securities, and the type of securities was cash equities. Approximately **1.5%** of the AUs reported having clients that engaged in "wash trading" by simultaneously buying and selling securities to artificially bolster share prices and encourage other investors to invest.

Tax Evasion

There were **10.8%** AUs who reported possible tax evasion. **4.6%** reported that they have clients that used their business to hold funds that are not being used in trading of securities or financial instruments for an extended period.

The figure below shows the most common financial crimes and market manipulation practices reported by AUs e.g., fraud, insider trading/market abuse/ tax evasion are being committed via transactions executed on the exchanges. Over **90%** of the AUs that participated in the survey indicated that their businesses have not been abused for financial crime and/or market manipulation practices.

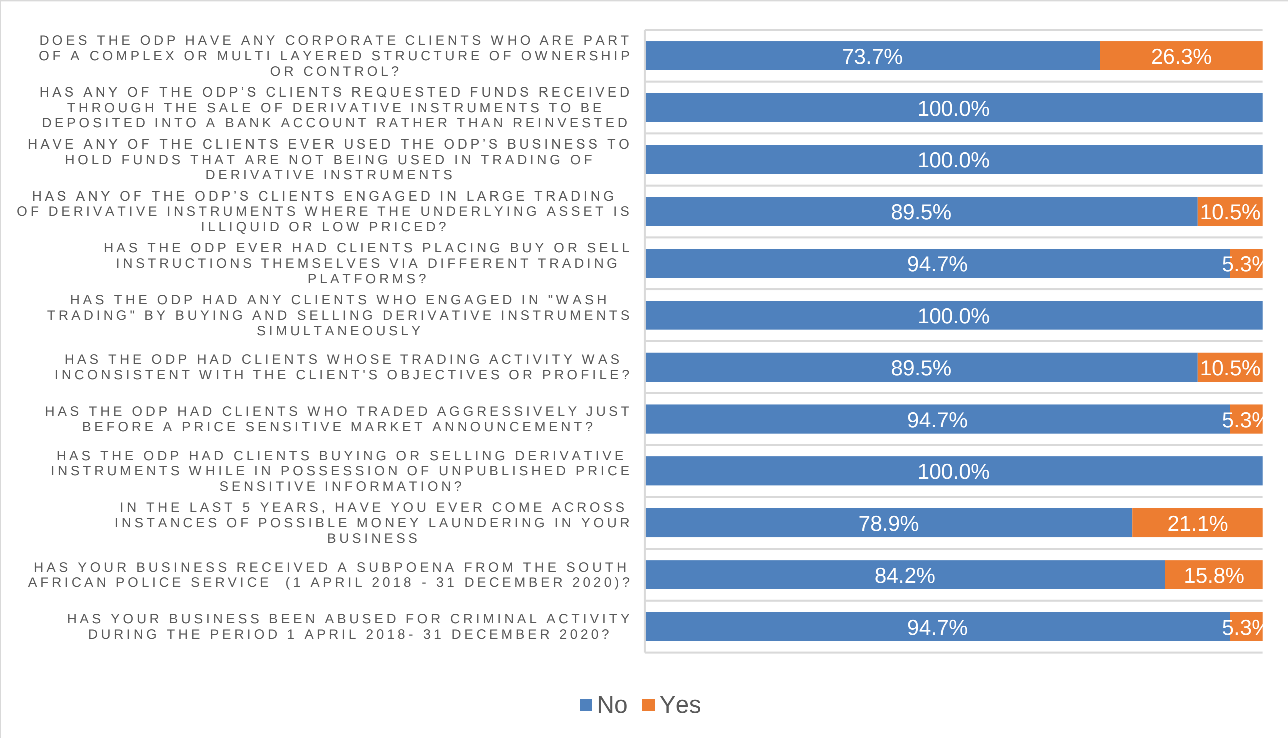


B. Over-the-Counter Derivatives Providers (ODPs)

ODPs indicated that they have not suffered any terrorism financing attack in the last 5 years and as such they have mentioned that all clients are a low rating regarding TF risk. The measure taken by the ODPs to mitigate the TF risks is mainly: funds are only processed to verified payment methods under the account holder's name.

Most of the clients consist of investment managers and other banks which are either regulated or listed on an exchange, clients undergo FIC Act checks and verification, every application must undergo a Politically Exposed Person (PEP) check, most of the entities are South African, and third-party payments are done through a multi factor identification method.

The figure below shows the crimes and market manipulation practices reported by ODPs:



Proceeds of crimes seized in the securities sector during 1 April 2018 – 31 December 2020

According to the Asset Forfeiture Unit of the National Prosecuting Authority the ML/TF/PF risks in the securities sector is very **low** and no reported AFU cases exist during the period under review.

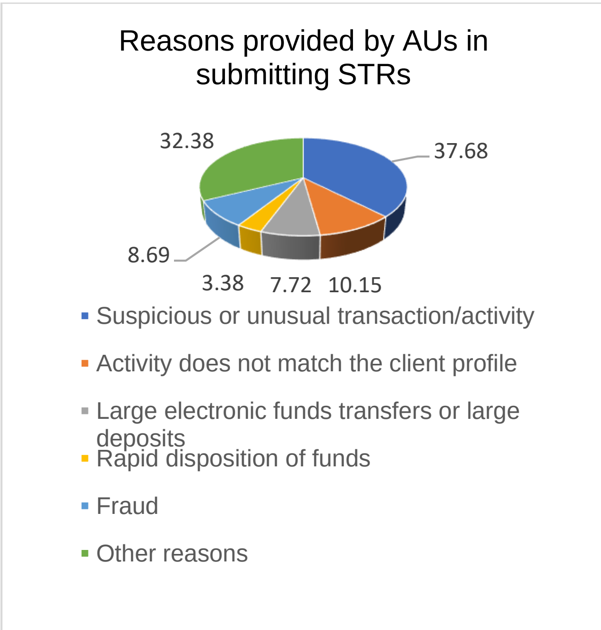
STRs and TPRs submitted by the industry

A. Authorised Users (AUs)

During the period under review AUs submitted 505 STRs to the FIC of which 443 were batch reports.

The value of the STRs submitted to the FIC amount to R1,7 billion.

Compared to all other sectors, the number of STRs submitted by AUs is relatively **LOW** as it only accounts for **0,03%** of the total STRs submitted to the FIC.



- As at 31 December 2020 a total of 151 AUs were registered with the FIC. AUs filed 33 suspicious activity reports, 969 suspicious transaction reports and 4 batch reports that contained 29 transactions to the value of R1, 697, 453,318. The reason for submitting STRs related to suspicious and/or unusual transactions/activities mentioned in section 29 of the FIC Act, followed by the fact that the activity does not match the client profile. Section 29 of the FIC Act directs 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 financing of terrorist 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 money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.

AUs filed 3 STRs where the reason for suspicion was that the client appeared on a sanction/ watch list. Another 1 STR was submitted where the reason for submitting the STR related to the contravention of a prohibition under section 26B. They also filed 1 STR where the reason for suspicion related to an offence of financing of terrorism and related activities. No evidence of TF/PF, however, could be identified as a result of these reports.

9.23% of the AUs that participated in the survey reported suspicious transaction reporting to FIC in the last five years for possible instances of ML. One of the AUs who participated in the survey accounted for **44%** of suspicious transaction reports to FIC.

No TPRs were submitted by AUs.

We also considered STRs submitted by other accountable institutions (Banks, FSPs etc.) where the subject matter was an AU. Sixteen STRs were identified where the subject matter was an AU. The majority (**69%**) 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,
- Corruption, and
- Tax evasion.

B. Over-the-Counter Derivative Providers (ODPs)

1,249 suspicious transactions involving suspected ML were reported during in the last 5 years as reported by the ODPs.

The table below shows the suspicious transaction reporting over the last five years from the ODPs for possible instance of ML:

Security type	Number of reports submitted to the FIC
Commodity derivatives, foreign exchange derivatives, equity derivatives	749
Other	500
Total	**1,249**

21.1% of the ODPs reported suspicious transactions to the FIC in the last five years for possible instances of money laundering.

Overall, ODPs accounted for 1,249 suspicious transactions which were reported to the FIC, of which one of the ODPs included in the survey accounted for **56.6%** of all suspicious transaction reporting. This ODP offers multiple asset classes.

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. However, the primary stages of money laundering remain the same for all crimes:

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

The securities sector is characterized by frequent and numerous transactions, and several mechanisms can be used to make proceeds appear as legitimate earnings from the financial markets. The sector most commonly is used during the layering and integration phases, since most law-abiding brokers do not accept cash transactions. However, this obstacle is not an issue for criminals operating within the financial sector itself, such as embezzlers, insider traders, or perpetrators for securities fraud, because their funds are already present in the financial system (Reuter P. & Truman E. D., 2004).

Case example: The FIC received a request from the AFU to block funds in terms of section 34 of the FIC Act. A complainant transferred R1 million to an individual who pretended to be investor. The investor claimed to be able to double the returns on investments through a stockbroker. The fraudster promised returns of up to **18%** per annum on investment.

The complainant requested documentary proof of his investment and contact details of the stockbroker. The fraudster indicated that the stockbroker could not be contacted and claimed that the entire investment had in the meantime collapsed, and the money was “lost”.

The FIC evaluated the facts of the matter, obtained bank statements and analysed the transactional movement of funds together with the provided affidavits. The FIC traced the alleged funds in the perpetrator’s bank account and the AFU was then able to preserve the funds amounting to R970 000.00.

There are currently no TF or PF trends in the securities sector in South Africa. The following are money laundering indicators in the securities sector:

- The client refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.
- The client’s address is associated with multiple other accounts that do not appear to be related.
- The client is or has been associated with a PEP.
- The client appears to be acting as a fiduciary for someone else but is reluctant to provide more information relating to whom he or she may be acting on behalf of.
- Electronic transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

- It is impossible to determine a physical location of a client company.
- The client acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.
- The client is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons.
- The client refuses to identify a legitimate source for the funds.

5. SECTOR VULNERABILITY ANALYSIS

Some of the key characteristics of the securities sector that make it vulnerable to abuse for ML/TF/PF include:

(a) The varying roles that securities providers and other intermediaries play in transactions; for example, a securities provider may be both an investment fund manager and a depository bank;

(b) Differences among jurisdictions in defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;

(c) ML/TF risks stem mainly from the types of securities products and services, clients, investors and payment methods used in the securities sector;

(d) Global reach of the securities sector and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;

(e) Ability to transact in securities products via an intermediary which may provide a relative degree of anonymity;

(f) High liquidity of some securities products, which often enables their easy conversion to cash;

(g) Complex products that may be offered;

(h) Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents, potentially limiting the ability of any one participant to have complete oversight of the transaction;

(i) An often highly competitive and incentive-driven environment, which may lead to a higher appetite for risk, or failure to adhere to internal controls;

(j) Pricing volatility of some products, particularly low-priced securities;

(k) Transactions executed both on registered securities exchanges and elsewhere, such as over-the-counter (where parties trade bilaterally), and reliance on alternative trading platforms, electronic communication networks and internet-based trading;

(l) Opportunity to use transactions in securities for generating illicit income within the sector, for example, market abuse or fraud; and

(m) Challenges in pricing some securities products due to their bespoke nature or complexity. [7]

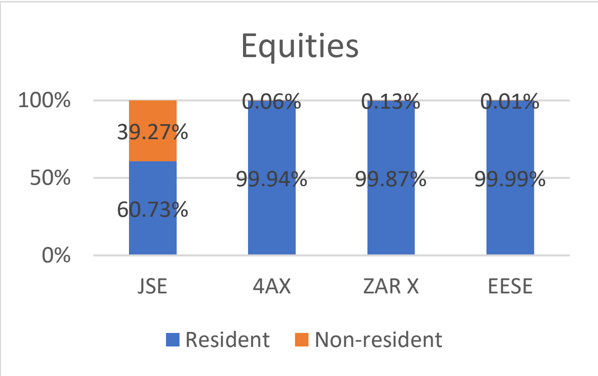
[7] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf

CLIENT TYPE

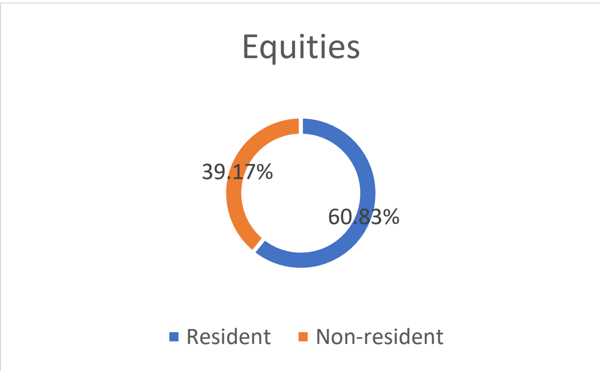
Resident and non-resident holdings

The graphs below depict resident and non-resident holdings in South Africa (Strate CSD Services, 2021):

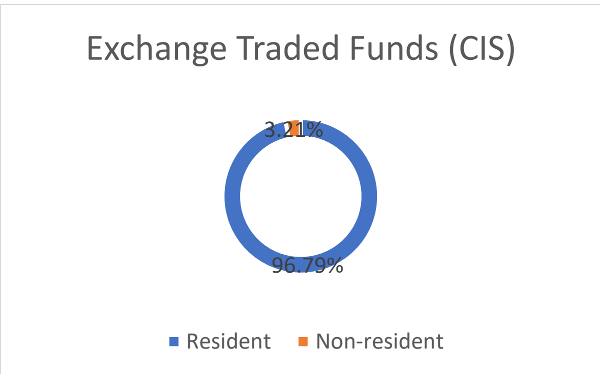
Equities holdings per exchange



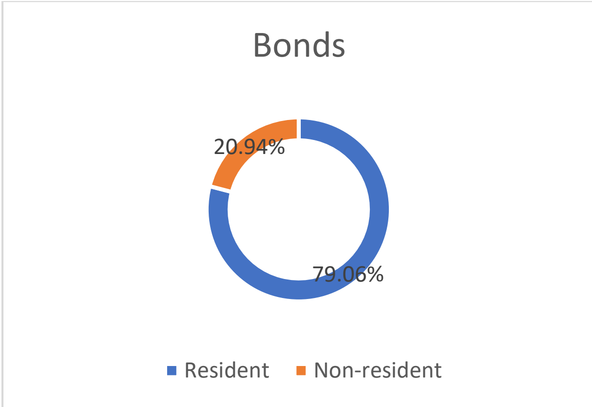
Overall equities holdings



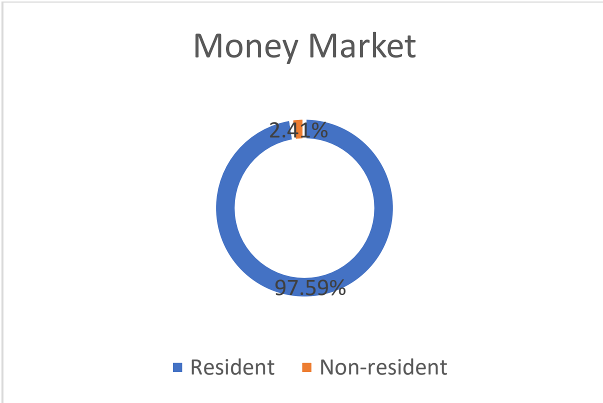
Exchange traded funds (CIS) holdings:



Bond holdings



Money Market holdings



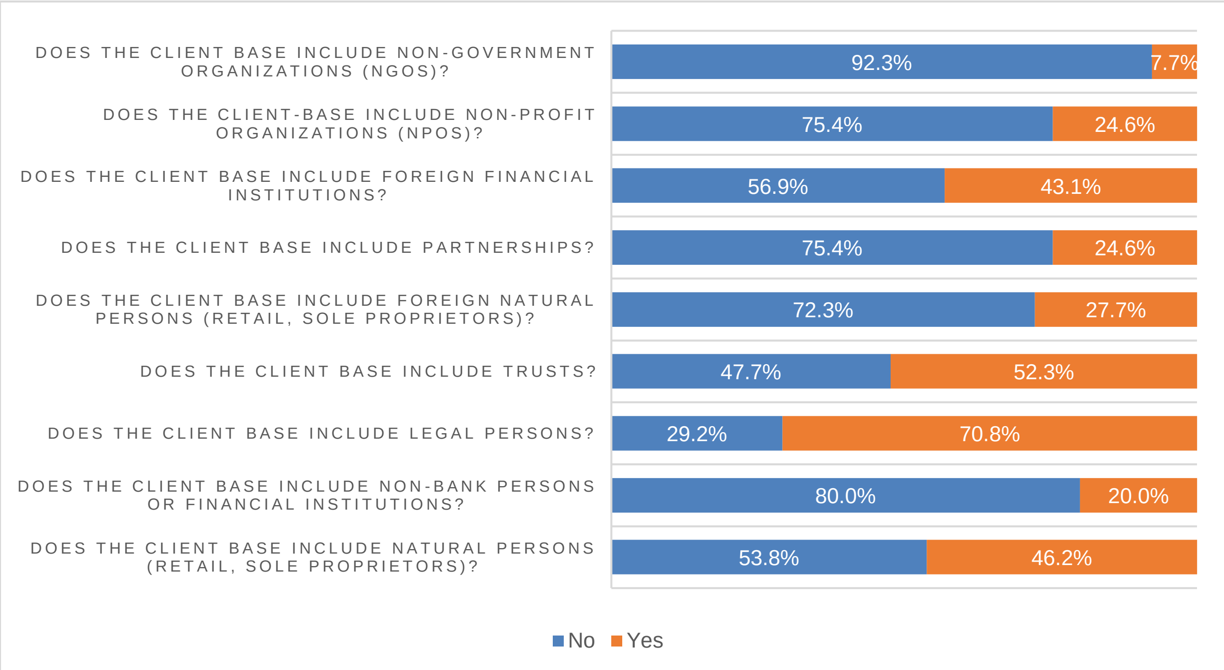
Money Market holdings per client type

0.03%	Close corporations
3.63%	Foreign companies
59.51%	Local companies
0.01%	Natural persons (local)
6.26%	Trusts
30.55%	Other

A. Authorised Users (AUs)

Type of clients

The figure below shows the various types of clients in respect of whom AUs render securities services



The survey results indicated that a majority of AUs render securities services to legal persons, followed by trusts, natural persons, foreign financial institutions, foreign natural persons, partnerships, and non-profit organisations. NGOs were reported as the least prevalent client type.

24.6% of the AUs reported that they have corporate clients that are part of an ownership or control structure that is complex or multi-layered.

3.1% of the AUs indicated that clients requested monies received through the sale of securities to be deposited into a bank account rather than be reinvested in a trading account.

The use of agents and third parties

9.2% of AUs' clients were introduced by a third party whose business activity is unrelated to securities services. **27.7%** of the AUs indicated that some of the security services provided to their prospective clients were achieved using intermediaries and/ third parties. **16.9%** stated that the securities services they rendered allowed or facilitated payment to a third party and **9.2%** stated that the securities services rendered allowed or facilitated payments by or from a third party. AUs can be at a significant disadvantage, given how large the client base is, when they are trying to establish whether clients are engaged in criminal activities.

Source of Funds and Wealth

In identifying a client's ML and/or TF risk, AUs must consider information relating to a c's source of funds and/or wealth.

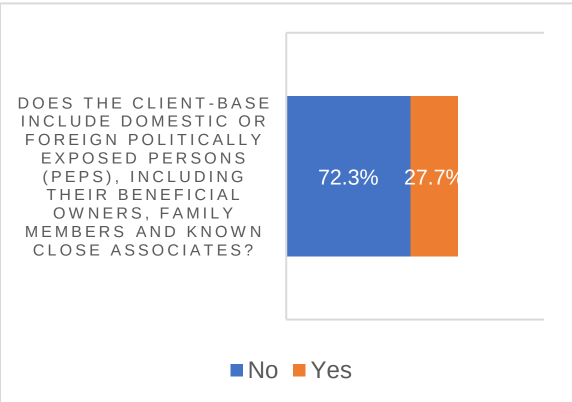
Some AUs expressed concerns about their clients' sources of funds or wealth. Only **1.5%** of the AUs' clients transact in large amount of cash.

Source of wealth for foreign clients

3.1% of AUs' clients have an unknown source of funds. These clients mainly traded in cash equities.

Politically Exposed Persons (PEPs)

The figure below shows the percentage of PEPs as clients of AUs as per the results of the survey:



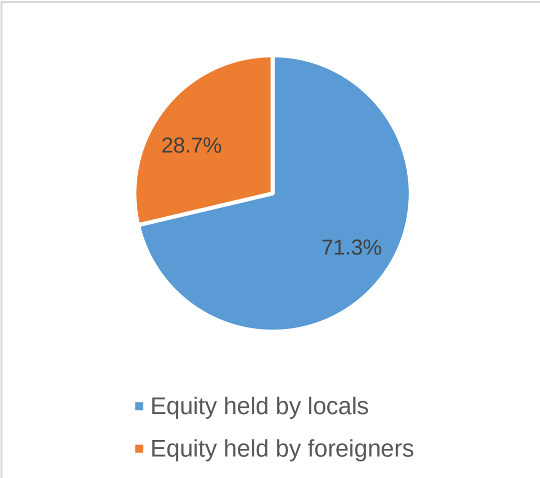
27.7% of the AUs reported that their client-base include domestic or foreign politically exposed persons (PEPs), including their beneficial owners, family members and known close associates.

B. Over-the-counter Derivatives Providers (ODPs)

Types of clients

Resident and non-resident holdings

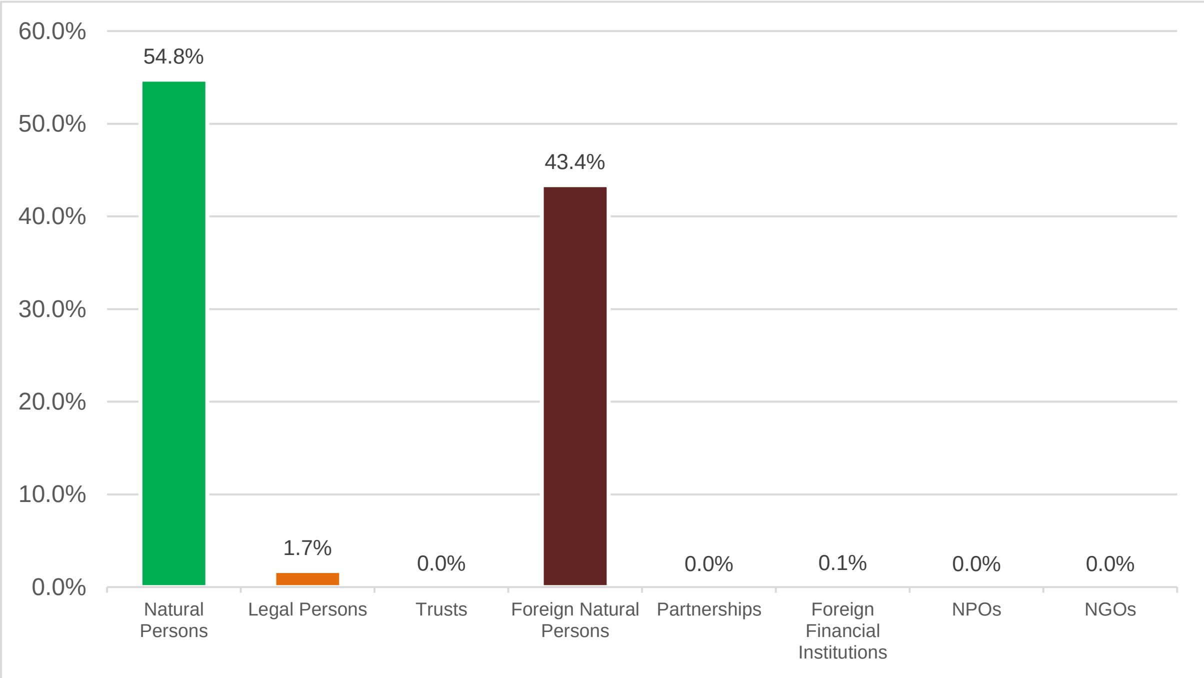
The figure below shows data provided by ODPs in the survey on equity traded by foreigners (non-resident) versus local residents. The percentage of equity derivatives traded by local residents is high, making it less susceptible to ML.



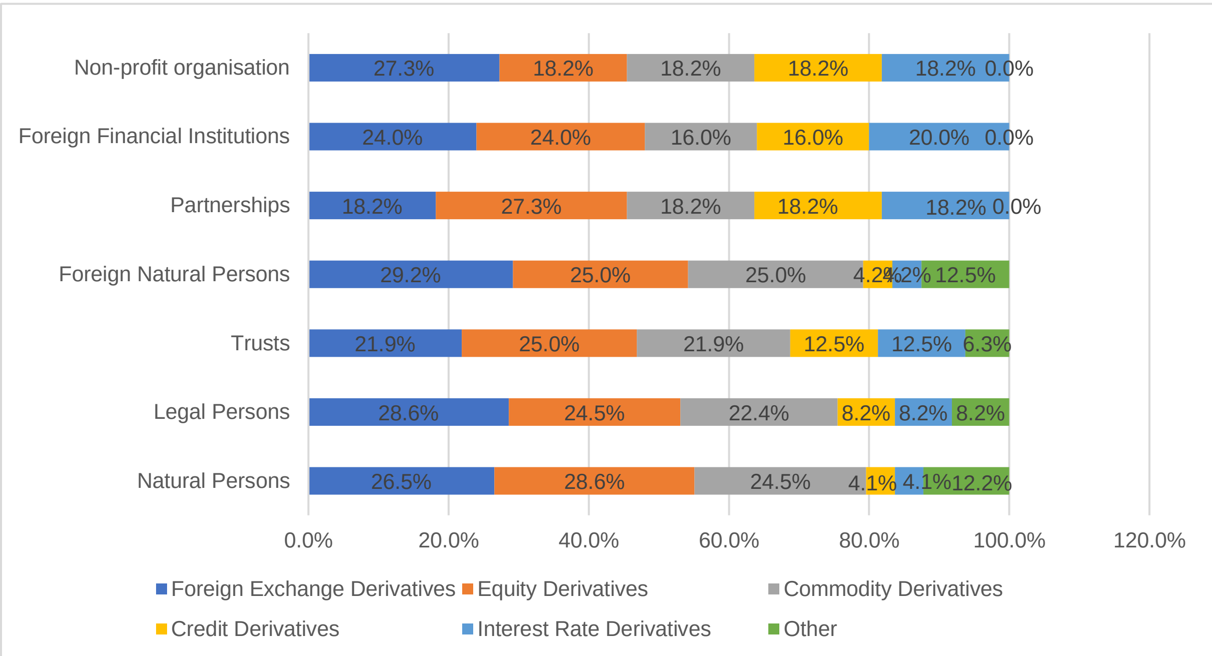
Clients of ODPs mostly comprise natural persons at **54.8%** and foreign natural persons at **43.4%**.

The rest of the client base consists of legal persons at **1.7%** and foreign financial institutions at **0.1%.**

The figure below depicts the client types prevalent in the sector reported by ODPs



The figure below shows various asset classes as traded by various client types



The use of agents and third parties

26.3% of the ODPs provide services to clients through intermediaries and/or third parties. None of ODPs' clients have been introduced by a third party whose business activities are unrelated to securities. None of the ODPs that participated in the survey have allowed nor facilitated payments from a third party.

Source of Funds and Wealth

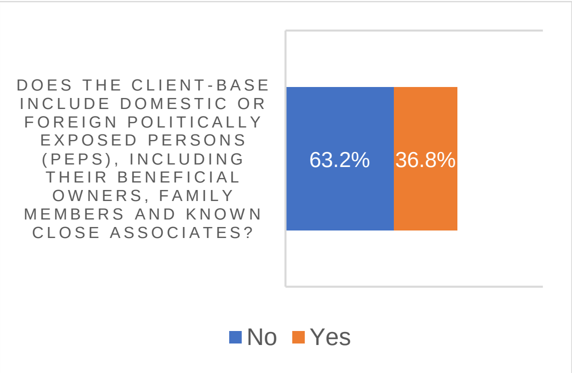
All the ODPs that participated in the survey indicated that they have no clients whose nature of business activity involves transacting in large amounts of cash.

Unknowns source of wealth for foreign clients

Only **5.3%** of the ODPs had clients whose source of funds is unknown.

Politically Exposed Persons (PEPs)

The figure below shows the percentage of PEPs as clients of ODPs as per the results of the survey:



PRODUCTS AND SERVICES

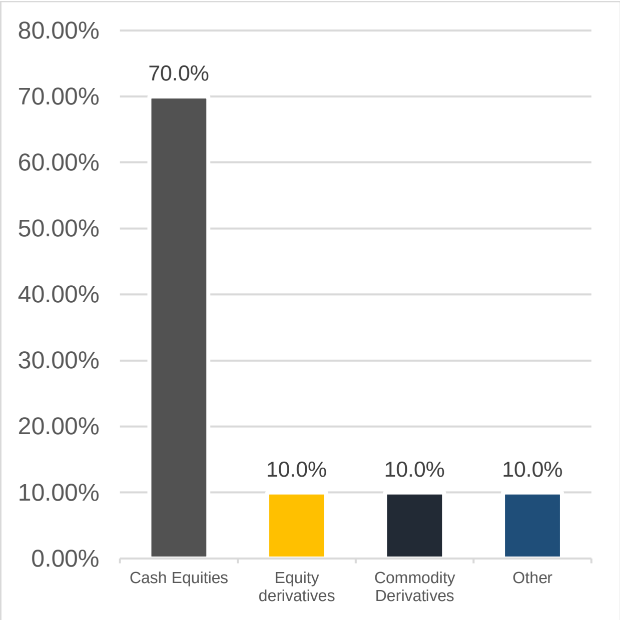
A. Authorised Users (AUs)

Accounts

There is no evidence that the AUs provide securities services to hide/mask client identity. Furthermore, clients have no securities that allow them to be anonymous, so it is easy to identify them.

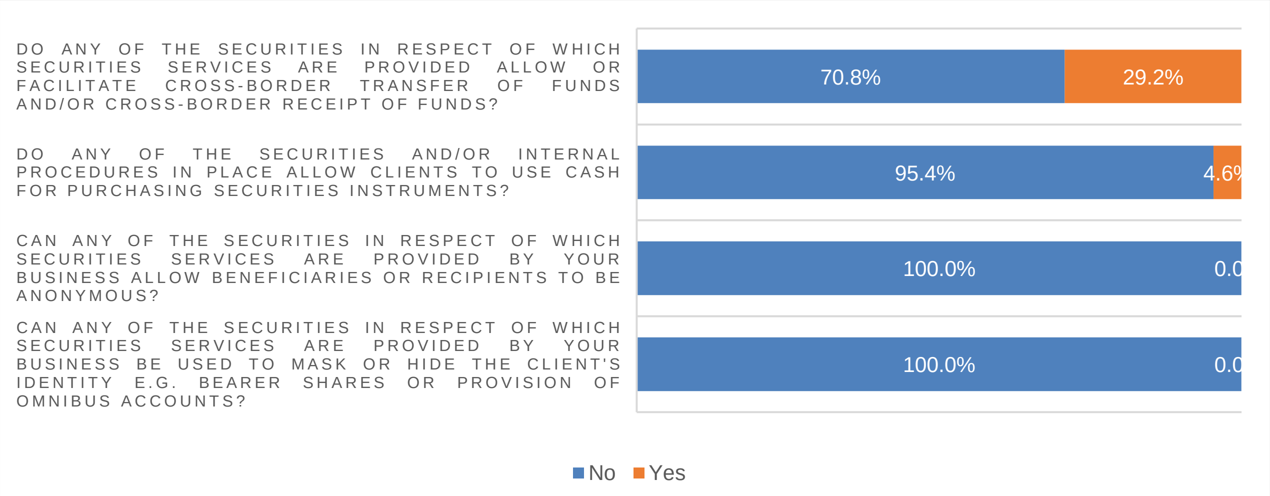
95.4% of the AUs do not allow their clients to use cash for purchasing securities instruments.

The figure below shows the type of asset classes predominantly traded by AUs:



AUs predominantly trade in cash equities.

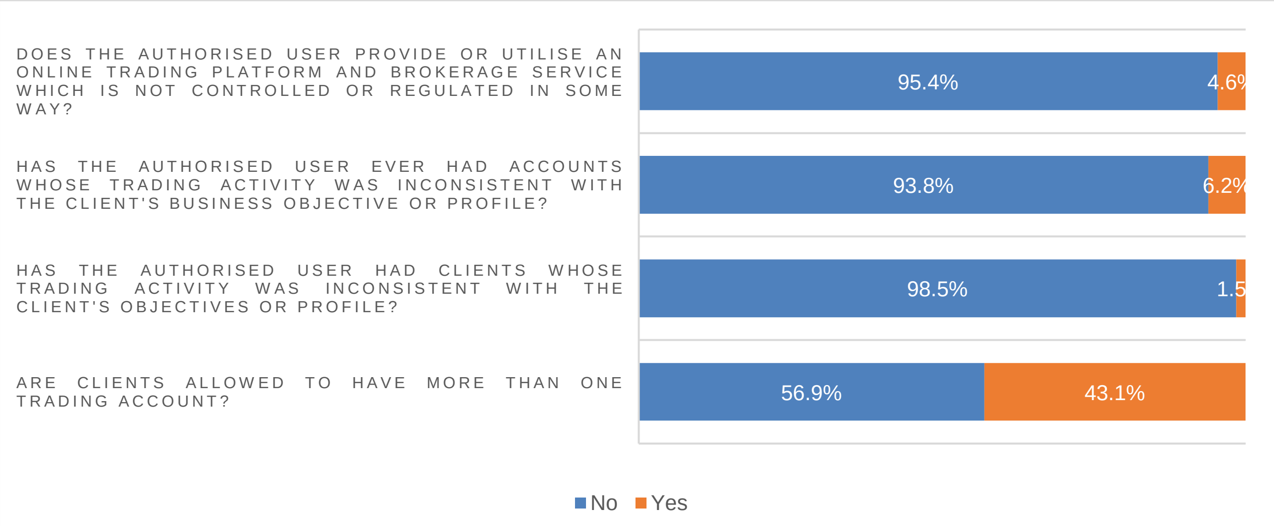
The figure below shows the AUs products and services



Trading

Trading is considered as one of the easiest ways in which clients can conduct insider trading and manipulation.

The figure below shows the AUs trading products and services



43.1% of the AUs reported that they allowed their clients to have more than one trading account. **4.6%** of AUs who reported to have provided/utilised an online trading platform and brokerage service which was not controlled or regulated.

Off-market transactions

Off-market transfers is one of the major risks in the securities sector since criminal activities such as fraud and tax evasion can easily occur. Unusual or suspicious activity concerns are mainly raised by inactive accounts which suddenly receive funds, large investments that are inconsistent with the client's profile, and non-face-to-face services.

4.6% of the AUs have had clients with inactive accounts that suddenly received funds that are unexplained, repetitive, unusual, or suspicious. **52.3%** of the AUs stated that they provided securities services on a non-face-to-face basis. Whilst **26.2%** of the ODPs stated that there was trading in financial instruments that were settled through an exchange.

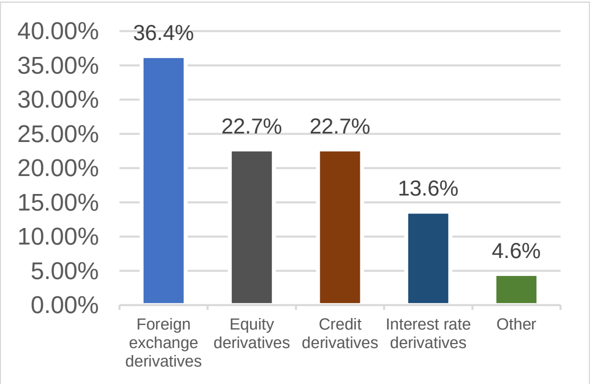
Third party payments

90.8% of the AUs reported that they do not allow third party payments on behalf of clients. Third-party payments provide a high risk to institutions if not monitored carefully.

B. Over-the-counter Derivatives Providers (ODPs)

Accounts

The figure below depicts the type of asset classes predominantly traded by ODPs:



ODPs' clients predominantly traded in foreign exchange derivates, as well as equity and credit derivates.

Trading

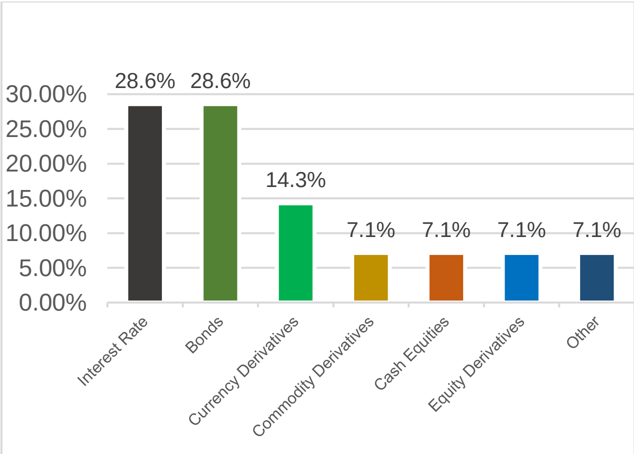
68.4% of ODPs allow their clients to have more than one trading account.

Off-market transactions

Off-market transfers is one of the major risks in this sector since criminal activities such as fraud and tax evasion are easy to occur. Unusual or suspicious activity concerns are mainly raised by inactive accounts which suddenly receive funds, large investments that are inconsistent, and non-face-to-face basis services.

70.8% of the ODPs do not allow cross-border transfers of funds or receipt of funds.

The figure below illustrates ODPs that facilitated trading in financial instruments that are settled through an exchange:



DISTRIBUTION CHANNELS

A. Authorised Users (AUs)

A delivery channel is the method used to deliver services and products to the Authorised users' clients. In the securities industry, most clients trade online with little or no face-to-face interaction with their brokers. Though, without a face-to-face relationship, it can be difficult to determine the legitimacy of a transaction or to form suspicions about a client.

Face-to-face trading versus other modes of trading

27.7% of the AUs provided securities services to their prospective clients using intermediaries or third parties. **70.8%** of the AUs accepted instructions on a non-face-to-face base and **21.5%** AUs have clients that have been physically present for identification and verification purposes.

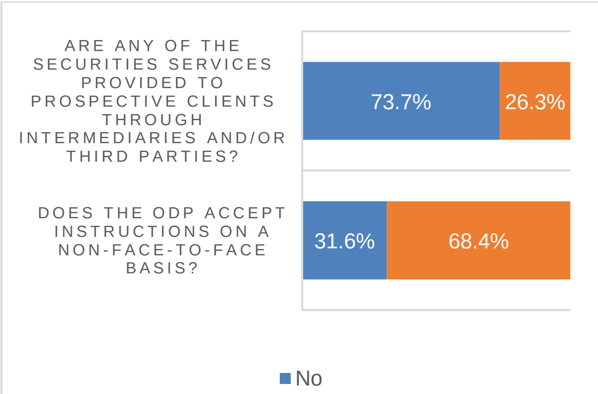
1.5% of the AUs use new or innovative technologies and payments methods to provide securities services. **4.6%** of AUs provide securities services independent of the AUs' trading system and transaction platforms. **4.6%** of the AUs provided/utilised online trading platforms and brokerage services which were not controlled. **9.2%** of the AUs had clients who have been introduced by a third party to the business activity which is unrelated to securities.

AUs do not interact or transact through intermediaries that are not subject to licensing nor provide services to non-banked walk-in clients.

B. Over-the-counter Derivatives Providers (ODPs)

Face-to-face trading versus other modes of trading

The figure below shows the statistics on no-face-to-face versus other engagements:



10.5% of the ODPs stated that they use new or innovative technologies and payments methods to provide securities services. **5.3%** of the ODPs had clients who placed a buy or sell instruction via different platforms.

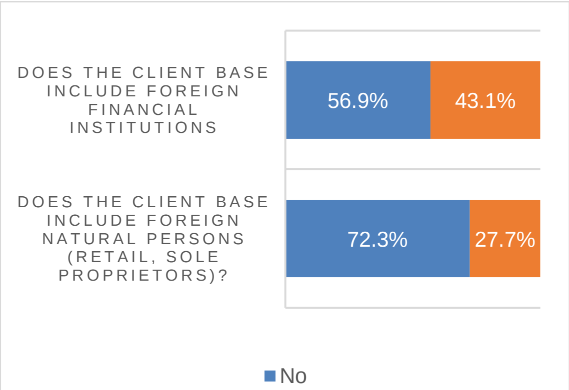
ODPs do not utilise online trading platforms and brokerage service, which is not controlled, nor do they deal with non-banked walk-in clients.

GEOGRAPHIC LOCATION

A. Authorised Users (AUs)

Foreign Clients

The figure below depicts the information related to foreign and non-foreign client base:



43.1% of AUs have a client base which included foreign financial institutions. **27.7%** AUs have foreign natural persons included in their client base.

Residence of clients in high-risk jurisdictions

1.5% of the AUs operated in jurisdictions where ML is a primary concern.

18.5% of AUs have clients that are registered in countries who are on the Financial Action Task Force's (FATF) grey-list. None of the AUs have clients who reside or registered in Syria, Sudan, Iran, Cuba and North Korea.

The table below reflects data on holdings by foreigners (non-residents) versus residents provided by Strate. As depicted, the percentage of equity held by residents is high, making it more vulnerable to ML:

Security type	Resident	Non-resident
Bonds	79.06%	20.94%
Equities	60.83%	39.17%
Money Market	97.59%	2.41%
Exchange traded funds (CIS)	96.79%	3.21%
Overall Strate view	**69.49%**	**30.51%**

B. Over-the-counter Derivatives Providers (ODPs)

Foreign Clients

36.8% of the ODPs have a client base which included foreign financial institutions. **50%** of ODPs had foreign natural person clients in their client base.

Residence of clients in high-risk jurisdictions

ODPs do not have clients in jurisdictions where ML is a primary concern and have no clients which have accepted orders that were not subjected to AML/CFT checks. **5.3%** of ODPs had clients from locations which are known to apply excessive client confidentiality.

26.3% of the ODPs' clients are registered in countries who are on the Financial Action Task Force's (FATF) grey-list. **10.5%** of the ODPs indicated that they have clients that reside or are registered in Syria, Sudan, Iran, Cuba, and North Korea.

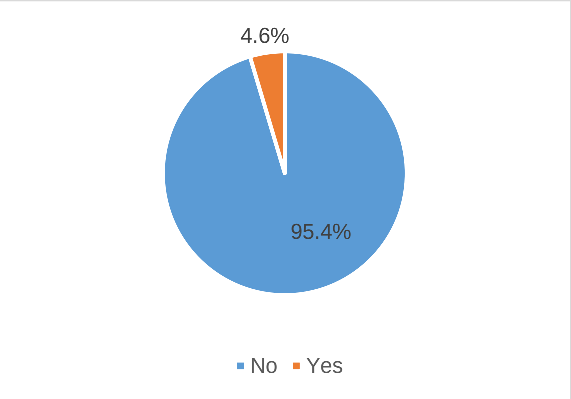
THE USE OF CASH

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

During the period under review AUs submitted 45,219 CTRs and 54,645 CTRAs to the FIC. This is more or less the same than the previous period under review. The value of these transactions reported amounts to almost R12 billion. Exchanges place a R5,000 threshold on the acceptance of cash. It is therefore doubtful whether these CTRs were submitted under the correct category.

A. Authorised Users (AUs)

The figure below shows the number of AUs that accept cash as per the survey results:



4.6% of AUs accept cash for purchasing securities such as commodity derivatives and cash equities.

In identifying a client's ML/TF risk, AUs must consider information relating to a client's source of funds and/or wealth.

The securities data analysis indicated that a small number (**2%**) of clients who had source of funds/wealth concerns dealt with structured and large cash deposits.

The AUs that were engaged for this risk assessment noted it was challenging to establish the source of funds.

B. Over-the-counter Derivatives Providers (ODPs)

Overall, ODPs had no clients whose nature of business activity involves transacting in large amounts of cash.

MITIGATION OF ML/TF RISKS

A. Authorised Users (AUs)

Risk assessment

All of the AUs that participated in the survey indicated that they conducted risk assessments on money laundering and/or terrorist financing risks faced by their businesses.

Customer Due Diligence and Customer On-Boarding

1.5% of AUs indicated that they had clients who are classified as "Other" and "Unknown" and have not provided relevant information to complete the customer due diligence or Know Your Customer (KYC). **16.9%** of the AUs reported that some of their clients have been on-boarded before the amendment of to the FIC Act came into effect on 02 October 2017 which implies that these clients have not been identified and verified in terms of the Risk Management and Compliance Programme (RMCP).

Suspicious activities

During the 2019/2020 and 2020/2021 financial years, 11 (**8,2%**) and 12 (**9%**) AUs, respectively, out of a total of 134 AUs, reported STRs. There appears to be some underreporting of STRs.

The AUs surveyed indicated that they did not have clients who purchased a security which did not correspond to the client's investment profile nor any of the clients who ever faked their identification or used false information to open or set up an account for trading.

3.1% of the AUs indicated that some of their clients have funds which sources are unknown and that **1.5%** of the AUs had clients who have made repeated changes to their profile information.

The quality of the Section 29 reports submitted appeared to be varied. The FIC noted 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 required to be submitted for payors and payees.

In terms of section 27 of the FIC Act, the FIC may issue a request to an accountable institution to confirm if a person/entity is a client of them and if they acted for a client. The FIC sent out 34 requests in terms of section 27 of the FIC Act to AUs. AUs only responded to 15 out of the 34 requests (44% response rate). It therefore appears that the majority of AUs are not adhering to this obligation of the FIC Act or may be slow in providing feedback.

In terms of section 32 of the FIC Act, the FIC may request an accountable institution to provide additional information on a STR or CTR submitted by the accountable institution. The FIC sent out 4 requests in terms of section 32 of the FIC Act to AUs. AUs responded to 3 out of the 4 requests (**75%** response rate). One response was outstanding during the period under review.

B. Over-the-counter Derivatives Providers (ODPs)

5.3% of the ODPs indicated that they have clients that have been classified as either "Unknown" or "Other". These clients have not provided relevant information to complete the customer due diligence or KYC process.

5.26% of ODPs indicated that they have clients whose source of funds is unknown and made repeated changes to their profile information within a 12-month period.

5.3% of ODPs had clients that have purchased a derivative instrument which doesn't correspond with the client's investment profile.

15.8% of the ODPs stated that their clients have used fake identification or false information to open or set up an account.

6. CONSEQUENCES

Consequences refer to the impact or harm that ML/TF may cause and includes the impact of the underlying criminal and terrorist activity on the financial sectors supervised by the FSCA.

Harm or loss to clients

Clients may lose confidence in the exchanges which will result in them not investing money in the sector. Clients may also suffer financial losses as a result of fraudulent activities or insider trading on their accounts.

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. ODPs are not accountable institutions and therefore do not have to adhere to the provisions of the FIC Act. However, the majority of licensed ODPs are part of a banking group which will lead to the banking group extending compliance with the FIC Act in respect of ODPs. ML/TF will therefore be mitigated in both AUs and ODPs.

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.

Harm or loss to the financial sector

The biggest harm to the sector is reputational damage. A bad reputation will inhibit the capital-raising process for listed companies and fewer investments will be made.

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;
- Undermine integrity of the financial system;

- Affect savings and investments; and
- Decreased revenue.

FINANCIAL SECTOR CONDUCT AUTHORITY