



FINANCIAL INTELLIGENCE CENTRE

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

Tel: + 264 61 283 5100, Fax +264 61 283 5259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

VULNERABILITY/RATE OF ABUSE OF DIFFERENT TYPES OF LEGAL PERSONS AND ARRANGEMENTS IN THE ADVANCEMENT OF MONEY LAUNDERING

JULY 2023

TABLE OF CONTENTS

1. DEFINITIONS5

SECTION A.....6

2. INTRODUCTION6

3. OBJECTIVES OF THIS REPORT6

4. METHODOLOGY.....6

5. SUMMARY OF POTENTIAL PREDICATE OFFENCES REFERRED FOR INVESTIGATIONS.....7

 Table: 1 Potential ML in FIC cases referred for further investigations7

 Table: 2 Cases disseminated for investigations per predicate offence7

6. UNDERSTANDING LEGAL PERSONS AND ARRANGEMENTS7

SECTION B.....9

7. ASSET RECOVERY (PRESERVATIONS, FORFEITURES AND CONVICTIONS)9

 Table 3: Cases by Legal Persons9

 Chart 1: Cases by Predicate Offences.....9

 Chart 2: Convictions by Predicate Offense10

 Table 4: Convictions by Predicate Offense and Region11

SECTION C.....12

8. SUMMARY OF STRs RELATED TO LEGAL PERSONS AND ARRANGEMENTS REPORTED TO FIC.12

 Chart 3: Summary of STRs received as per Legal Persons12

8.1 PROPRIETARY LIMITED COMPANIES (PTY LTD).....13

 Chart 4: STRs received per Sectors: Potential Tax-Related Offence13

 Chart 5: Classification of STRs received per Sectors: Potential Tax-Related Offence.....14

 Chart 6: STRs received per Sector: Potential Fraud-Related Offence.....15

 Chart 7: Classification of STRs received per Sectors: Potential Fraud-Related Offence15

 Chart 8: STRs received per Sector: Potential Corruption-Related Offence16

 Chart 9: Classification of STRs received per Sector: Potential Corruption-Related Offence.....16

8. 2 TRUST LEGAL ARRANGEMENTS.....17

 Chart 10: STRs received per Sector: Potential Tax-Related Offence18

 Chart 11: Classification of STRs received per Sector: Potential Tax-Related Offence19

 Chart 12: STRs received per Sector: Potential Fraud-Related Offence.....19

 Chart 13: Classification of STRs received per Sector: Potential Fraud-Related Offence20

 Chart 14: STRs received per Sector: Potential Corruption-Related Offence21

8. 3 CLOSE CORPORATIONS (CCs).....21

 Chart 15: STRs received per Sector22

 Chart 16: Classification of STRs received per Sector23

 Chart 17: STRs received per Sector: Potential Tax-Related Offence23

 Chart 18: STRs received per Sector): Potential Fraud-Related Offence24

 Chart 19: STRs received per Sector: Potential Corruption-Related Offence24

8. 4 INDIVIDUALS (NATURAL PERSONS).....	25
Chart 20: STRs received per Sector	25
Chart 21: Classification of STRs received.....	26
Chart 22: STRs received per Sector: Potential Tax-Related Offence	27
Chart 23: STRs received per Sector: Potential Fraud-Related Offence.....	28
Chart 24: STRs received from Sectors: Potential Corruption-Related Offence.....	29
9. SUMMARY OF SARs RELATED TO LEGAL PERSONS AND ARRANGEMENTS.....	29
Chart 25: Summary of SARs received by Legal Persons	30
9.1 PROPRIETARY LIMITED COMPANIES	30
Chart 26: SARs received from Sectors	31
Chart 27: Classification of SARs received.....	32
9.2 TRUSTS	32
Chart 28: SARs received per Sector	33
Chart 29: Classification of SARs per Sector.....	34
9.3 CLOSE CORPORATIONS	34
Chart 30: SARs received per Sector.....	34
Chart 31: Classification of SARs per Sector.....	35
SECTION D.....	36
10. SPONTANEOUS DISCLOSURES (SDs) AND AMOUNTS INVOLVED PER LEGAL PERSON/ARRANGEMENT	36
Table 5: Close Corporation.....	36
Table 6: Proprietary Limited.....	36
Table 7: Trusts Companies.....	36
Table 8: Individual Persons	37
SECTION E.....	38
11. MOST COMMON IDENTIFIABLE POTENTIAL TAX OFFENCES, FRAUD AND CORRUPTION INDICATORS.....	38
11.1 Potential indicators from cases under the FIC domain and general potential indicators	38
Table 9: potential indicators under FIC domain.....	38
Table 10: General potential indicators of tax, fraud, corruption and bribe.....	40
11.2 Unexplained wealth or income.....	40
Table 11: Potential indicators of unexplained wealth or income	41
11.3 Corruption in public procurement.....	41
Table 12: Indicators of Corruption in public procurement.....	41
SECTION F.....	43
12. SAMPLED CASE STUDIES.....	43
Case Study 1: Potential corruption and bribery.....	43
Case Study 2: Potential employee fraud, corruption, and theft.....	45

Case Study 3: Mobile Risks (Potential Tax-related offence)46

Case Study 4: Awarding of Mining Licence (Potential corruption and fraud offence).....48

SECTION G.....50

13. KEY FINDINGS.....50

14. CONCLUSION.....53

15. ANNEXURES55

Annexure 1. Pty Ltd STRs transactions as per GoAML Portal.....55

Annexure 2. Trust Legal Arrangements STRs transactions as per GoAML Portal56

1. DEFINITIONS

Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation framework (AML/CFT/CPF): Refers to the national (or international) framework which combats and prevents money laundering, terrorism and proliferation financing activities;

Money laundering (ML): Generally, refers to the act of disguising the true source of proceeds generated from unlawful activities and presenting such in the financial system as sourced from legitimate activities. However, in terms of the Prevention of Organized Crime Act, 2004, as amended (POCA), the definition of ML is broad enough to include engagement, acquisition and concealment of proceeds of crime whether directly or indirectly;

Proliferation financing (PF): “the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations”¹;

Terrorist financing (TF): includes “acts which are aimed at directly or indirectly providing or collecting funds with the intention that such funds should be used, or with the knowledge that such funds are to be used, in full or in part, to carry out any act of terrorism as defined in the Organization for African Unity (OAU) Convention on the Prevention and Combating of Terrorism of 1999, irrespective of whether or not the funds are used for such purpose or to carry out such acts”;

Legal Persons (LP): This refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. These can include companies, bodies corporate, foundations, partnerships, or associations and other similar entities; and

Vulnerabilities: When used in a risk assessment, this term comprises of those weaknesses that can be exploited by the threat or that may support or facilitate its activities.

¹ FATF Recommendation 7

SECTION A

2. INTRODUCTION

The FIC is committed to preventing the misuse of legal persons and arrangements such as companies, partnerships and trusts as channels for Money Laundering, Terrorism and Proliferation Financing (ML/TF/PF). As the threats from illicit financial flows continue to evolve, the FIC and the country at large need to understand the risks and design appropriate mitigation measures. The purpose of this typology report is to determine the degree to which legal persons in Namibia are vulnerable to ML/TF/PF risks considering the specific legal services they provide and to describe red flag indicators of ML/TF/PF which may be useful to competent authorities and law enforcement agencies.

3. OBJECTIVES OF THIS REPORT

The objectives of this typology report are to:

- a. identify specific types of transactions in which legal persons may have been unknowingly involved in ML/TF;
- b. identify vulnerable areas within different types of legal persons' frameworks that may need improvement;
- c. rank the products and services in terms of their vulnerability to ML/TF threat;
- d. provide a basis and rationale that informs FIA compliance supervision and monitoring activities in terms of the risk-based approach;
- e. highlight red flags or indicators that may assist in combatting ML/TF threats; and
- f. enhance understanding of the modus operandi employed by perpetrators in sectors.

4. METHODOLOGY

The FIC analysed relevant data, and various reports at its disposal to understand potential methodologies, trends, typologies, and other related red flags associated with different types of legal persons and arrangements which potentially leads to ML/TF activities. The information contained in this report was derived from STRs/SARs data filed with the FIC by various reporting institutions.

Specifically, the sources of data and information analysed primarily include:

- i. Sanitized intelligence emanating from reports and closed databases;

- ii. Competent Authorities' investigation outcomes; and
- iii. Open-source research.

Such data was analysed and the information from such is summarized herein.

5. SUMMARY OF POTENTIAL PREDICATE OFFENCES REFERRED FOR INVESTIGATIONS

Table: 1 Potential ML in FIC cases referred for further investigations

PERIOD: 2009 - 2021				
	Total STRs Received	No. of Cases (SDs)	Total Financial Value from such Cases/SDs (NAD)	Average Financial value Per Case (NAD)
Close Corporations (CCs)	228	104	34,807,766,160.75	334,690,059.24
Companies	232	115	8,659,067,618.13	75,296,240.16
Trusts	96	55	1,613,992,815.33	29,345,323.92
Natural Persons	5,690	1,696	23,404,719,080.81	13,799,952.29

Table: 2 Cases disseminated for investigations per predicate offence

PERIOD: 2009 - 2021						
	Fraud	Total Financial Value (NAD)	Potential Tax Evasion	Total Financial Value (NAD)	Corruption	Total Financial Value (NAD)
Close Corporations (CCs)	25	404,533,140.88	66	28,400,797,080.66	7	394,575,890.57
Companies	56	656,836,151.56	141	738,080,077.59	35	284,419,187.68
Trusts	3	14,016,585.60	7	776,270,899.40	6	56,516,585.60
Natural Persons	667	1,695,855,636.13	2264	15,632,296,444.92	84	1,955,490,671.17

6. UNDERSTANDING LEGAL PERSONS AND ARRANGEMENTS

Legal persons refer to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. These can include companies, body corporates, foundations, or associations and other similar entities. On the other hand, legal arrangements refer to partnerships, express trusts or other similar arrangements. Examples of other similar arrangements (for AML/CFT purposes) include trusts, trust agencies and escrows².

² Glossary to the FATF Recommendations, 2012

Since the inclusion of legal persons in the scope of professionals in the FATF Recommendations of 2003, there has been extensive debate as to whether there is evidence that legal persons have been involved in ML/TF. The debates also venture into unpacking whether the application of the Recommendations is consistent with fundamental human rights and the ethical obligations of legal persons.

Namibia, like all other countries, should take measures to prevent the misuse of legal persons and such arrangements for ML/TF. In furtherance of the same, countries should ensure that there is adequate, accurate and timely information on ultimate beneficial ownership and control of legal persons and arrangements that can be obtained or accessed in a timely fashion by competent authorities. Specifically, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities³.

There is evidence that criminals seek to use legal persons in their ML schemes, sometimes because the involvement of legal persons is required to carry out certain types of activities. In some instances, it is because access to specialised legal and notarial skills and such related services may assist in the laundering of the proceeds of crime and the funding of terrorism. STRs, SARs and Case studies in Namibia point to the following legal services being vulnerable to misuse for the purpose of ML/TF:⁴

- a. client accounts (administered by the legal professional);
- b. purchases of real property;
- c. creation of trusts and companies;
- d. management of trusts and companies;
- e. setting up and managing NPOs such as charities and Faith Based Organisations ;
- f. administration of deceased estates;
- g. providing insolvency services;
- h. providing tax advice; and
- i. preparing powers of attorney.

³ FATF Recommendations.

⁴ FATF Report: Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals; and

SECTION B

7. ASSET RECOVERY (PRESERVATIONS, FORFEITURES AND CONVICTIONS)

This section of the report presents a summary of cases processed by the Office of the Prosecutor General (OPG).

The table below shows a summary of Cases by legal persons under the OPG’s domain, primarily the Asset Forfeiture Unit (AFU). A total of 62 Cases were referred to the above-mentioned unit from the year 2016 until 2022. Records show that 66% of these cases involved Close Corporations, while Trusts and PTYs represent 6% and 5% respectively.

Table 3: Cases by Legal Persons

	2016	2017	2018	2019	2020	2021	2022	Total
Natural Persons	15	10	10	8	4	8	7	62
Close Corporations	11	9	5	6	1	4	5	41
Trusts	0	1	0	0	1	1	1	4
PTYs	0	2	0	0	0	0	1	3

Chart 1: Cases by Predicate Offences

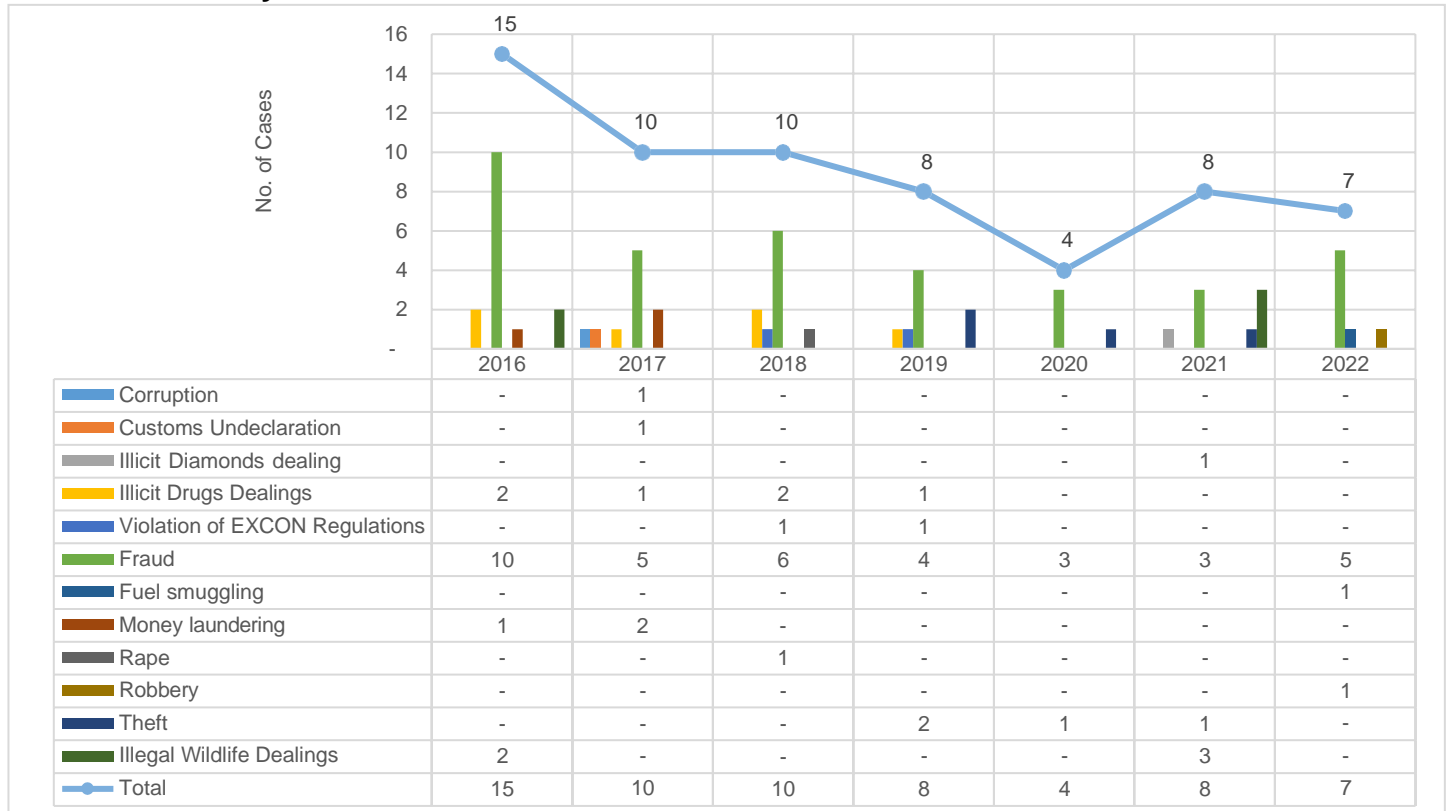
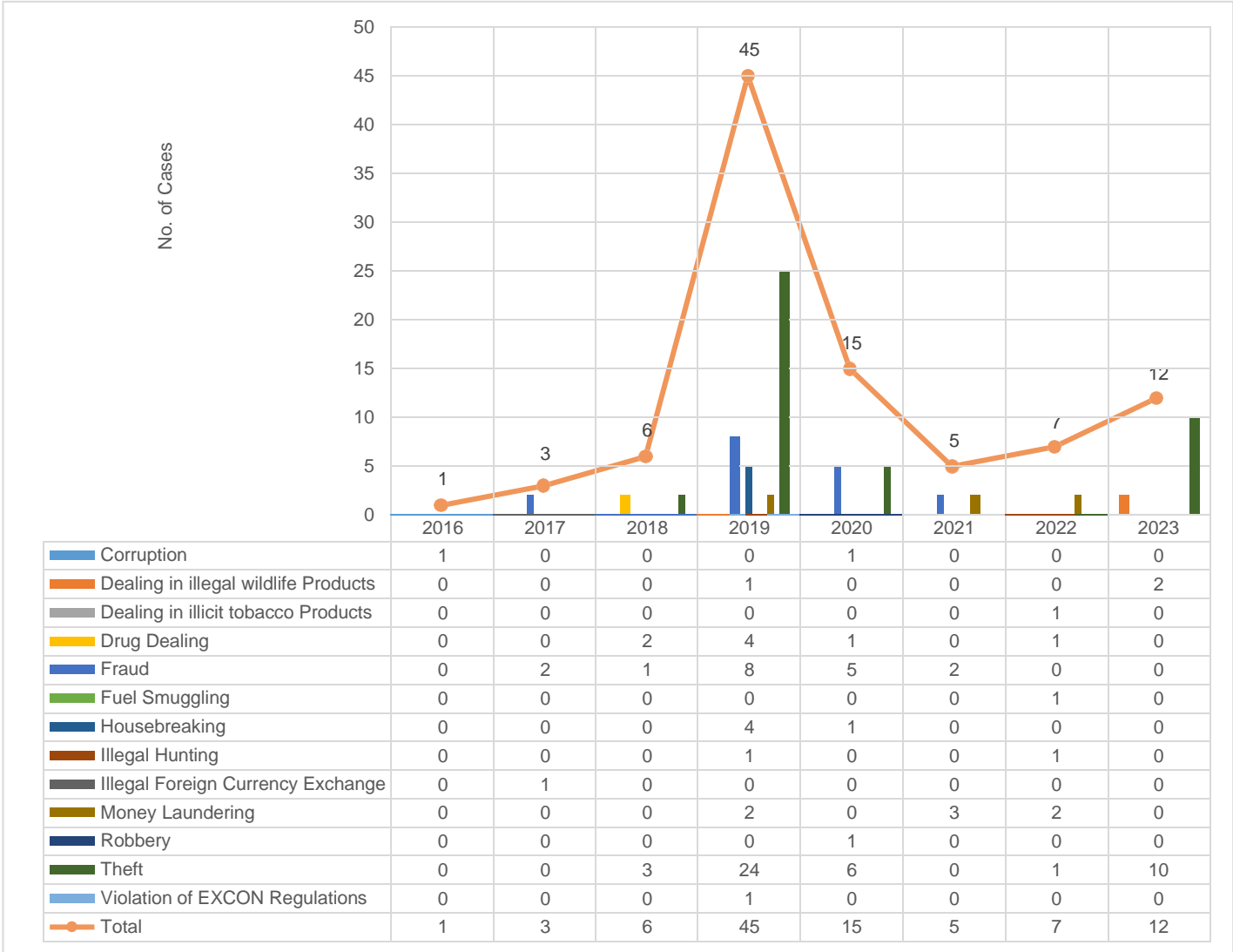


Chart 2 below shows that fraud featured as the leading predicate offence, followed by Illegal dealings in diamonds and wildlife crimes/products. The high prevalence of fraud as a predicate offence is similarly reflected in the 2020 NRA. As per the records, 80% of the accused in these cases are Namibia citizens while the rest are foreigners. The majority of the accused foreigners are Chinese and Zimbabwean at 40% and 25% respectively. Moreover, records indicate that NAD 103 million is preserved for forfeiture (at the time of issuing this report) and 13% of this amount was forfeited to the state.

Chart 2: Convictions by Predicate Offense



Overall, 94 convictions were attained by the OPG from the year 2016 until May 2023 relating to various ML predicate offences such as corruption, theft and fraud. The highest number of cases was recorded in the year 2019. Theft featured as the leading predicate offence followed by Fraud and then Drug Dealing. Worth noting is that there have been 7 successful ML convictions.

During the period under review, the potential monetary value per predicate offense amounted to a total of NAD 472 million. Fraud cases have the highest monetary value of NAD 444 million or 94% of the total amount, followed by Money Laundering with a total amount of almost NAD 14 million. The 2020 NRA found that potential tax evasion may have the highest values of laundered proceeds, followed by fraud. The lack of parallel investigations of tax evasion cases with ML offenses potentially explains why the OPG has hardly prosecuted any cases of tax evasion as a predicate offense for ML. NAMRA and the Namibian Police could do better by not only focusing on tax recoveries but deliberately ensuring subjects are charged for tax evasion offences.

Records also indicate that 97% of the cases involved Namibians while only 3% of these cases involved foreign nationals.

Table 4: Convictions by Predicate Offense and Region

	Domestic		Foreign		Not Indicated	
	No. of Cases	Amount Involved (NAD)	No. of Cases	Amount Involved (NAD)	No. of Cases	Amount Involved (NAD)
Corruption	2	810,254		-	-	-
Dealing In Illegal Wildlife Products	3	2,400,000	-	-	-	-
Dealing In Illicit Tobacco Products	0	-	-	-	1	1,120
Drug Dealings	7	5,174,796	1	802,000	-	-
Fraud	17	444,808,097	-	-	1	70,000
Fuel Smuggling	1	21,000	-	-	-	-
Housebreaking	5	22,828	-	-	-	-
Illegal Hunting	2	5,200	-	-	-	-
Illegal Foreign Currency Exchange	0	-	1	2,020,000	-	-
Money Laundering	3	13,142,836	-	-	4	351,335
Robbery	1	300	-	-	-	-
Theft	44	5,584,773	-	-	-	-
Violation Of EXCON Regulations	1	193,000	-	-	-	-
Total	86	472,163,084	2	2,822,000	6	422,455

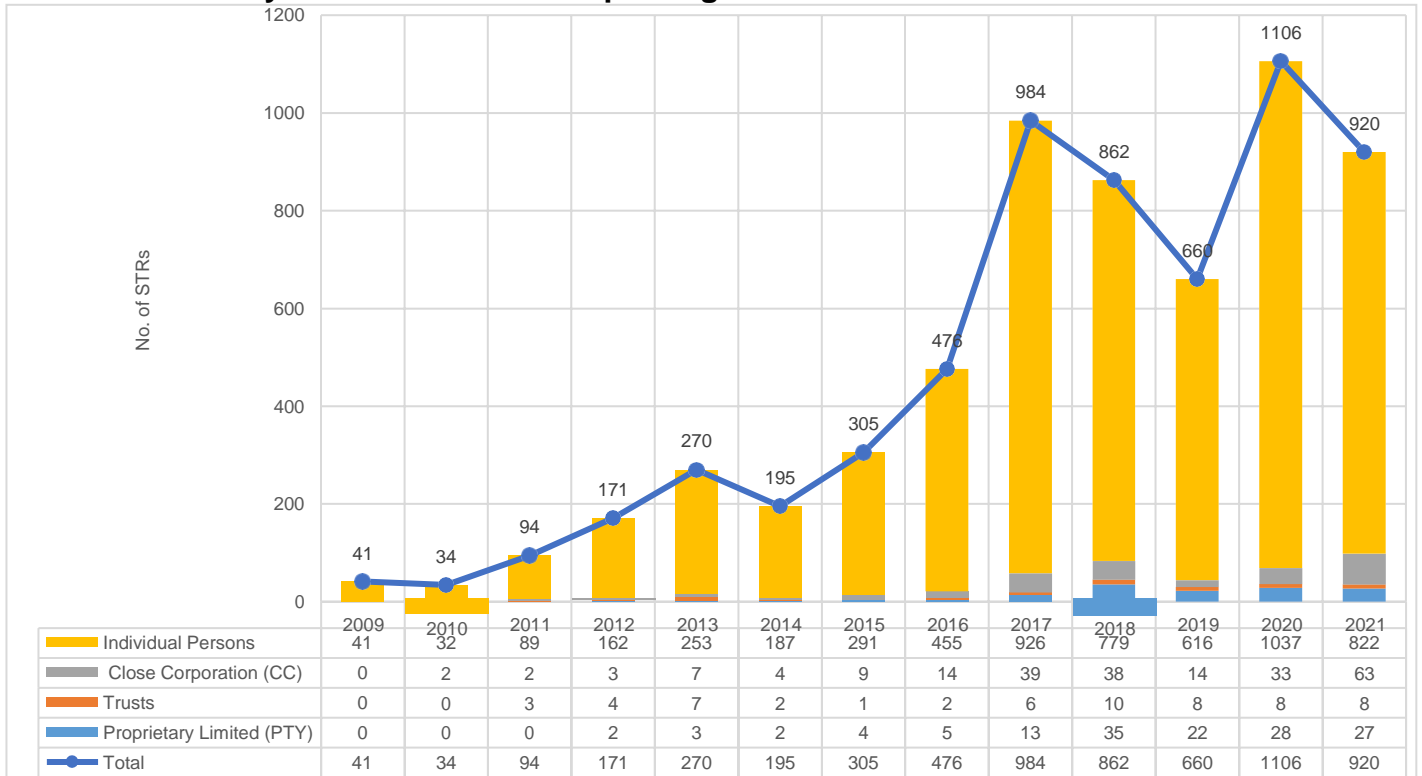
SECTION C

8. SUMMARY OF STRs RELATED TO LEGAL PERSONS AND ARRANGEMENTS REPORTED TO FIC

It is essential for combatting agencies and authorities to fully understand pressures and threats posed by ML/TF as criminal activities to effectively prevent predicate offences and related laundering activities.

This section provides an overview of STRs/cases⁵ related to possible ML/TF threats within legal persons and arrangements filed by reporting institutions since the reporting obligation commenced in 2009 until 31 December 2021. When reports are received by the FIC, they are assessed to determine if further investigations/analysis is required. If such is required, the reports are then turned into active cases for investigation/analysis. This section further presents information about the total number of reports escalated to cases, associated with various predicate offences such as potential tax-related offences, fraud, corruption and bribe amongst others.

Chart 3: Summary of STRs received as per Legal Persons



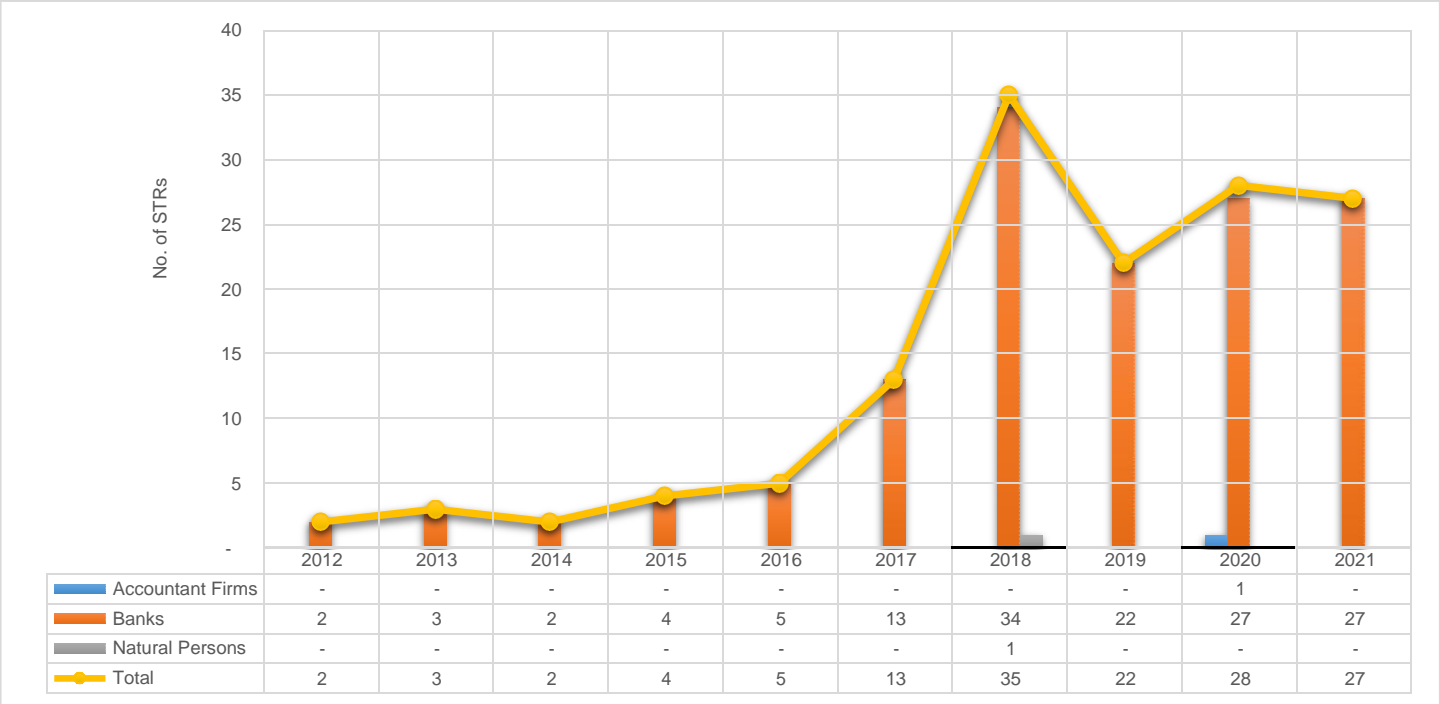
⁵ Cases within FIC domain.

Chart 3 presents a summary of STRs filed by AIs and RIs involved Legal Persons annually. The highest volume of STRs received involved Individual Persons at 93% (or 5,690 STRs), followed by Close Corporations at 4% (or 228 STRs) and then Proprietary Limited Companies at 2% (or 141 STRs).

8.1 PROPRIETARY LIMITED COMPANIES (PTY LTD)

This section of the report presents a summary of STRs involving Proprietary Limited Companies (Pty Ltd) and the classification of such reports in the period under review. As per information provided by the Business and Intellectual Property Authority (BIPA), only one (1) company is indicated to be locally owned. Classifications of other involved companies (whether local or foreign) was not provided because such information is not captured on the BIPA company registry system. This further adds to the Mutual Evaluation findings around poor controls within the company registry. It is further significant to indicate that these companies are 61% Namibian-owned (directors/beneficiaries) whereas 31% are foreign beneficiaries. Further, 9 foreign beneficiaries are Chinese, 5 South African, 3 British, 2 Spanish, 1 Zimbabwean, 1 Icelander, 1 Bulgarian and 1 Russian citizen.

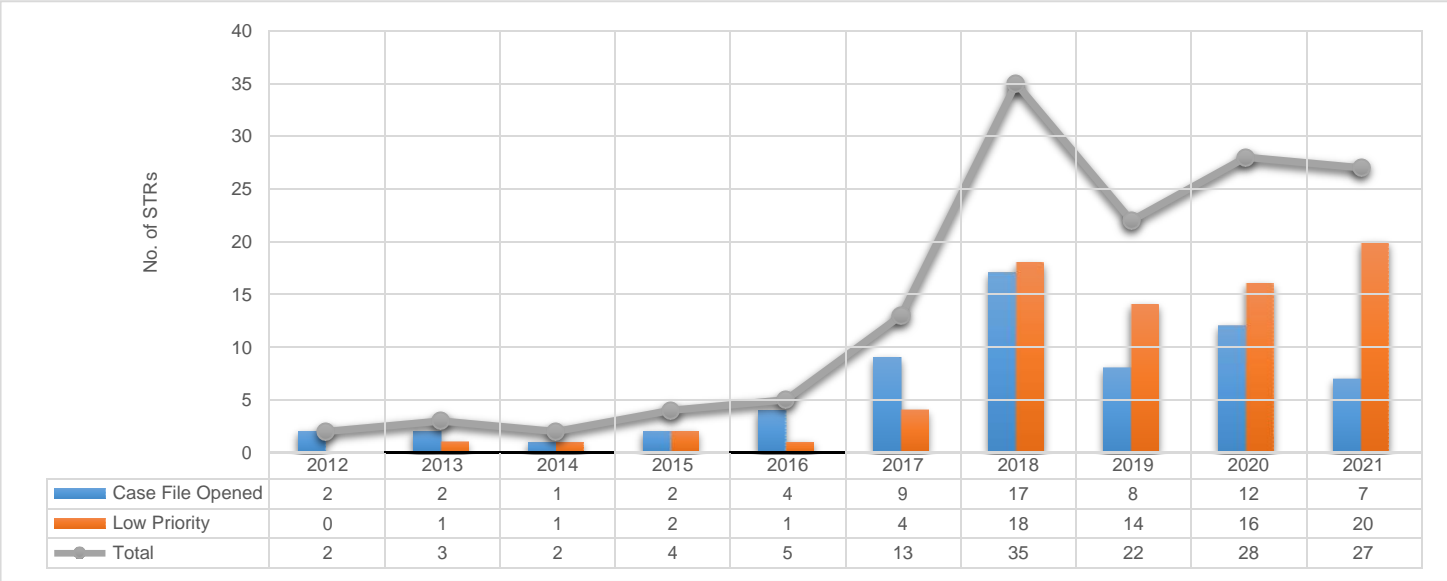
Chart 4: STRs received per Sectors: Potential Tax-Related Offence



The chart above presents a summary of STRs related to potential tax offences received from supervised entities involving various Proprietary Limited Companies. The general trend over the years

reflects an increase in the volume of potential tax-related offence reports reaching the FIC and being escalated to the relevant authorities. From the date the reporting obligations commenced until 31 December 2021, the FIC received a total of 141 STRs. Such is characterized by the lowest reports of 2 STRs in 2012, to the highest number of 28 STRs in 2020. The year 2018 saw the highest volume of reports potentially related to tax offences with 35 STRs. It is worth noting that a total of 139 STRs or 98% of the reports originate from the banking sector. This could be attributed to various factors, including the fact that the banks appear to have the most matured AML/CFT/CPF control systems. It can also be argued that banking services are generally exposed to a higher risk of abuse for tax-related offences as almost other sectors make use of banking systems, in one way or the other.

Chart 5: Classification of STRs received per Sectors: Potential Tax-Related Offence



Overall, the FIC observed that 45% (or 64 STRs) were accorded “high priority” status and escalated for further analysis (case files opened) whilst a total number of 77 STRs (or 55%) were categorized as ‘low priority’.

Chart 6: STRs received per Sector: Potential Fraud-Related Offence

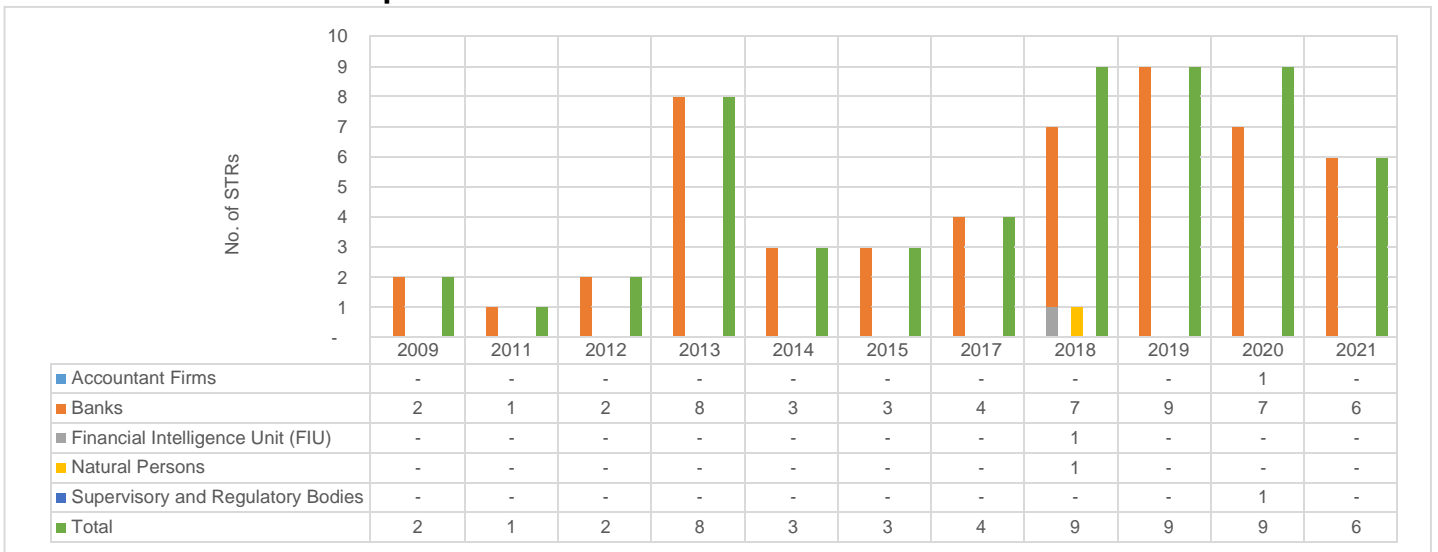
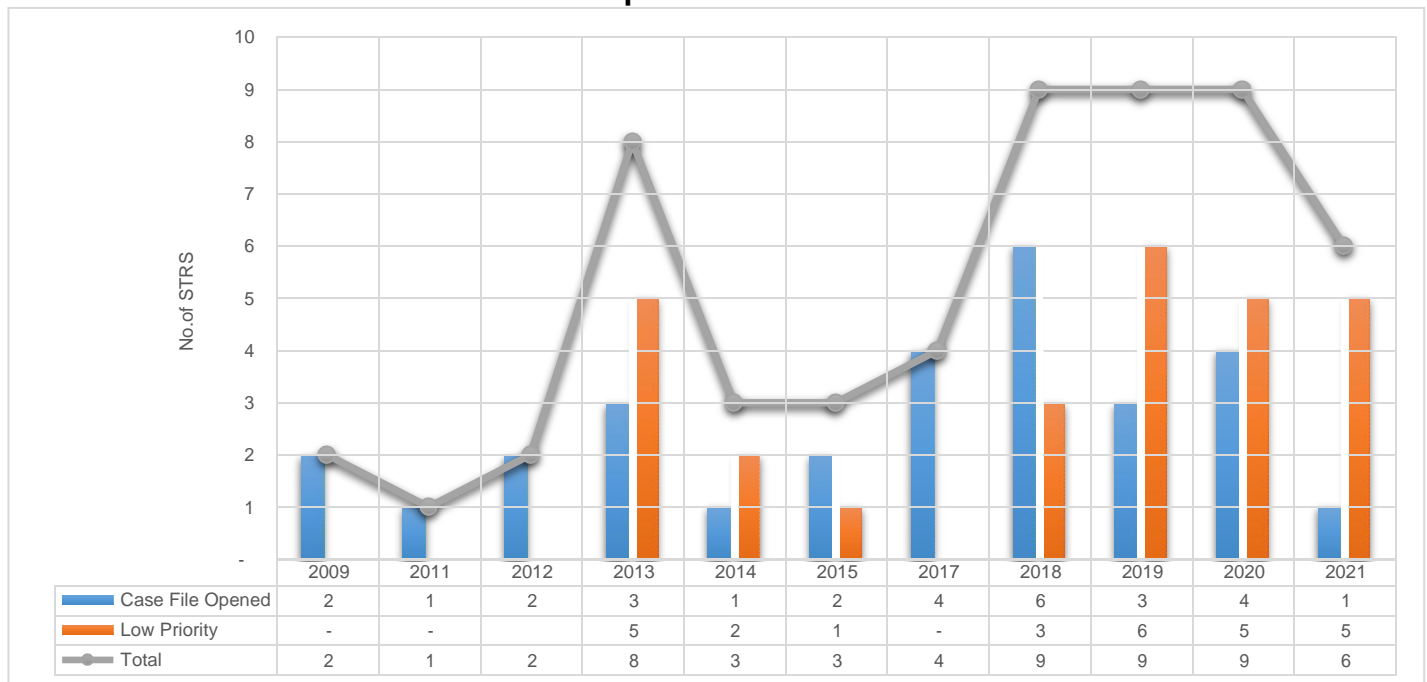


Chart 6 presents a summary of STRs related to potential fraud offences received from supervised entities involving various Pty Ltd companies. As of 31 December 2021, the FIC received a total of 56 STRs. The year 2018-2020 saw the highest volume of reports related to potential fraud offence. Further, a total of 52 STRs (or 93%) of the reports originate from the banking sector.

Chart 7: Classification of STRs received per Sectors: Potential Fraud-Related Offence



The FIC revealed that 52% (or 29 STRs) were accorded “high priority” status and escalated for further analysis, whilst a total number of 27 STRs (or 48%) were categorized as ‘low priority’. This shows a possible sign that value-adding reports have been filed by the sectors.

Chart 8: STRs received per Sector: Potential Corruption-Related Offence

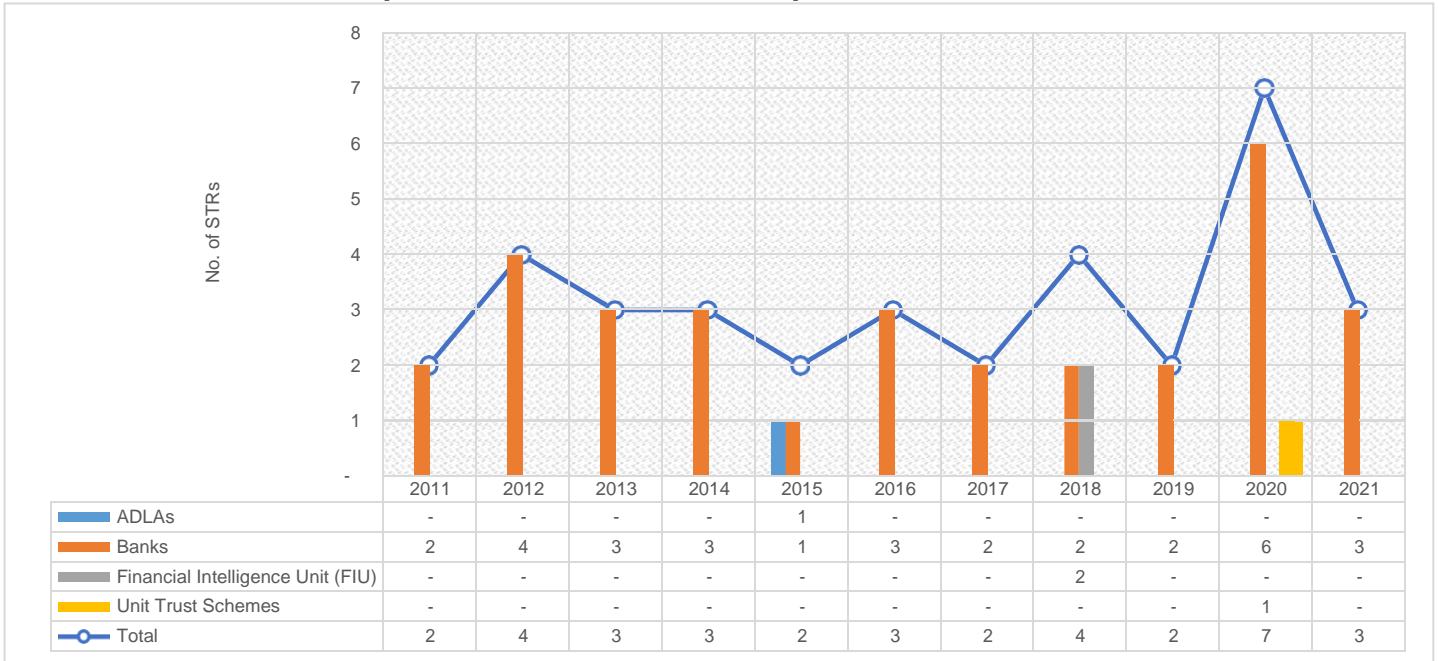
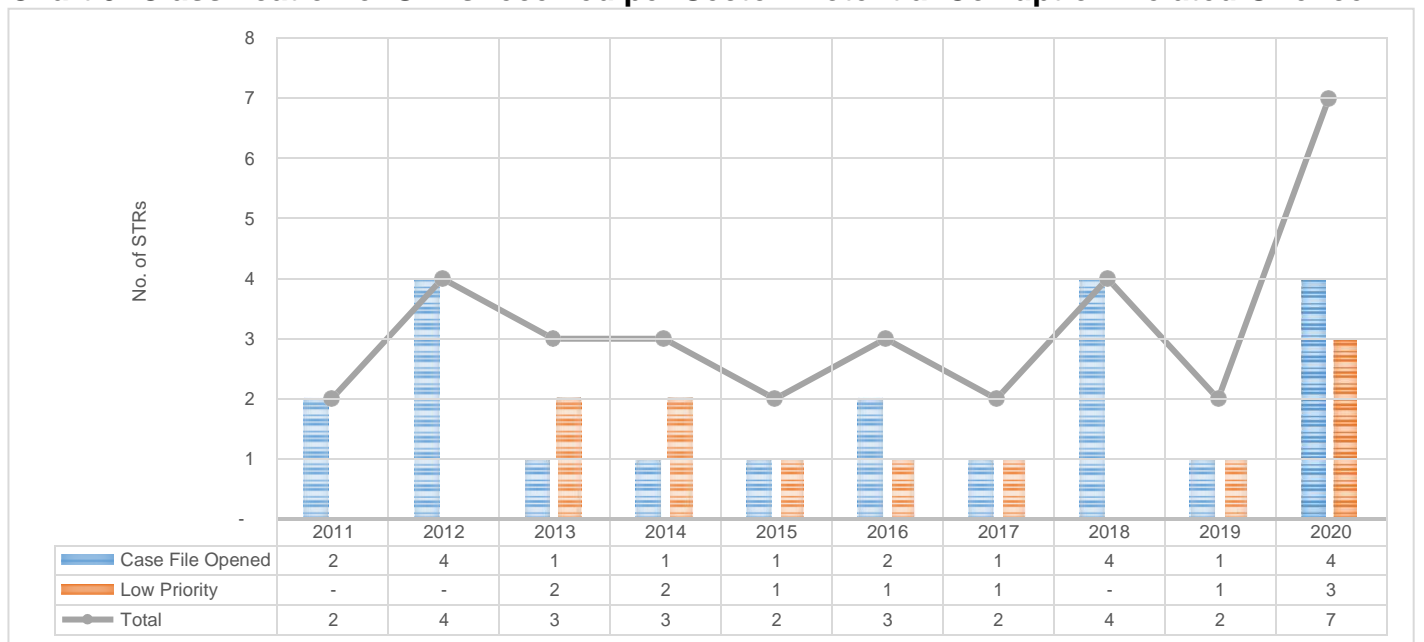


Chart 8 shows a summary of STRs related to potential corruption offence as one of the ML threats reported to FIC involving Pty Ltd companies. In the period under review, the FIC received a total of 35 STRs. The year 2020 saw the highest volume of reports related to potential corruption offences. It is further worth noting that a total of 31 STRs (or 89%) of the reports originate from the banking sector.

Chart 9: Classification of STRs received per Sector: Potential Corruption-Related Offence



The FIC noted that 63% (or 22 STRs) were accorded “high priority” status and escalated for further analysis, whilst 13 STRs (or 37%) were categorized as ‘low priority’. This further shows a possible sign that value-adding reports have been filed by sectors.

8.1.1 Pty Ltd Companies’ STRs as per GoAML Portal

Annexure 1 presents the transactional amounts of STRs filed and the names of involved entities (Pty Ltd companies) during the period under review. The highest single STR transaction value of **NAD 29,000,000.00** was reported involving an entity bearing the name “**PTY LTD-001**”. It is further significant to note that transactions with a combined monetary value of **NAD 13,640,220.45** were reported to the FIC through 77 STRs for an individual entity bearing the name “**PTY LTD-002**”. Overall, a total of 143 STRs were filed with a combined monetary value of **NAD 165,000,484.69**.

8. 2 TRUST LEGAL ARRANGEMENTS

Trusts are usually described as legal arrangements. Some can be structured to ensure a prudent mechanism to cater to the care of vulnerable people or used to administer and safeguard assets for other interests including family. A Trust can either be a private trust or a public charitable trust. This section presents a summary of STRs in which trusts may have been abused in the advancement of potential ML activities. It is worth noting that the trusts highlighted in this report are all inter-vivo trusts, meaning they are trusts created between living persons. It is further significant to indicate that these trusts are 100% Namibian entities registered with the Namibian Master of High Court under the Trust Moneys Protection Act 34 of 1934 and none of them are charitable trusts. This, therefore, suggests a limited exposure of charitable trusts to ML/TF activities. Records show that about 82% of these trusts have Namibian donors and Namibian trustees, respectively. Additionally, 40% of these trusts have foreign nationals listed as beneficiaries with the majority being South African citizens.

Chart 10: STRs received per Sector: Potential Tax-Related Offence

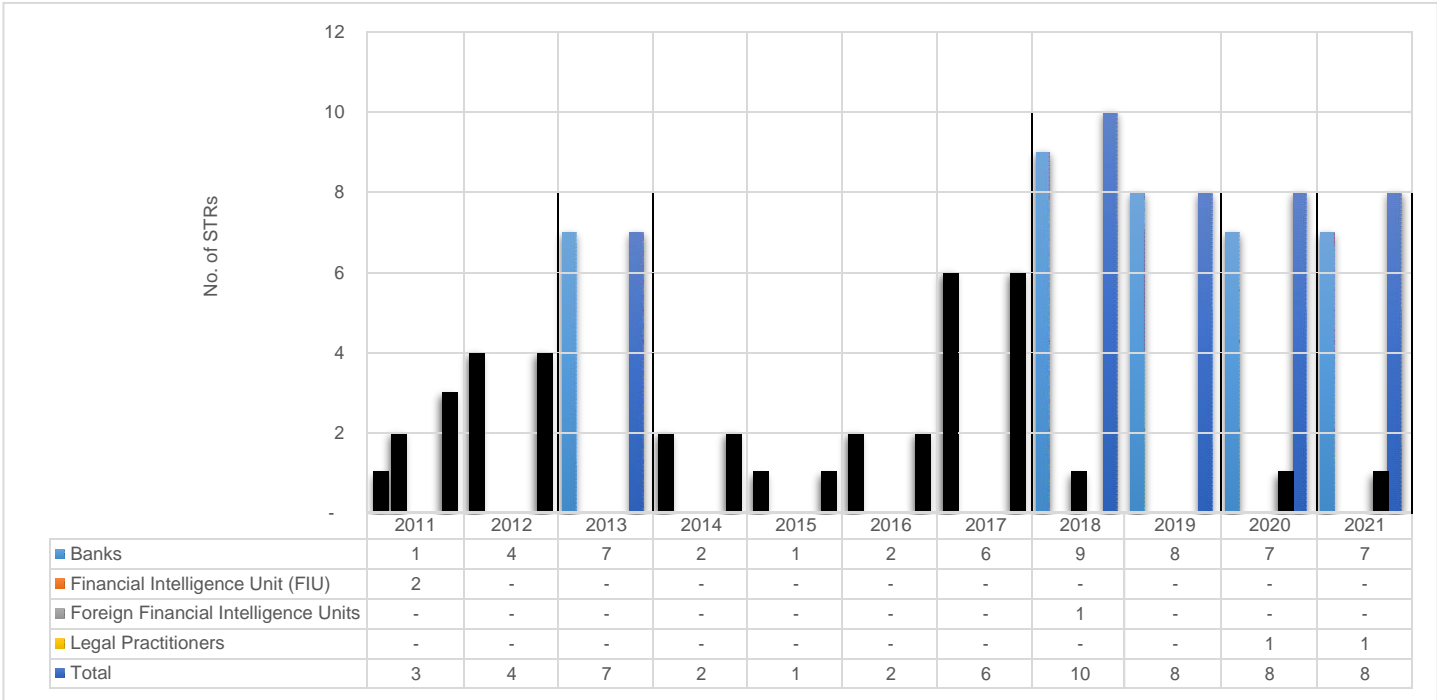
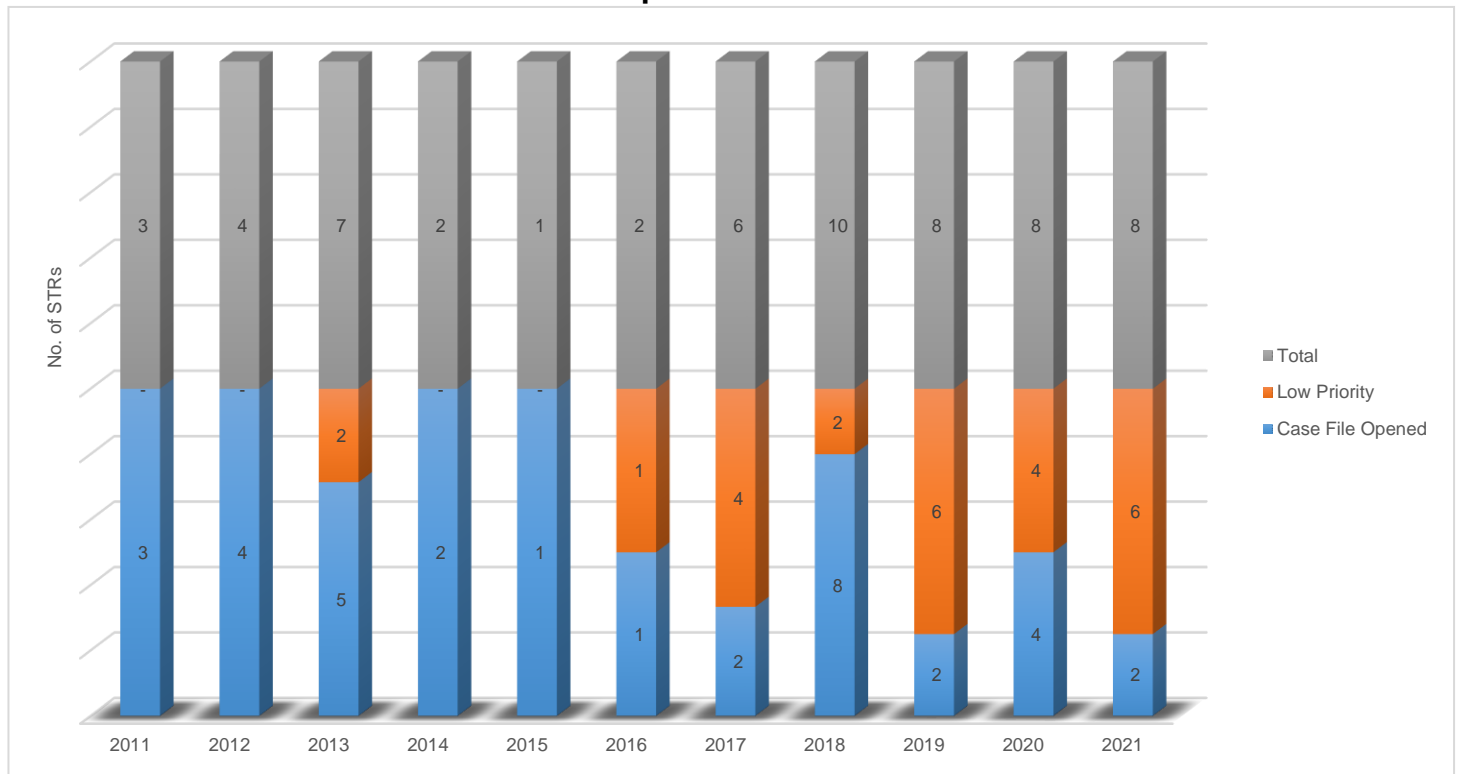


Chart 10 shows a summary of STRs related to potential tax offences as one of the leading ML threats reported to FIC within trust legal arrangements. In the period under review, the FIC received a total of 59 STRs. The highest volume of reports related to potential tax offences was recorded during the year 2018. Most reports (54 reports) originate from the banking sector.

Chart 11: Classification of STRs received per Sector: Potential Tax-Related Offence



The FIC noted that 58% (or 34 STRs) were accorded “high priority” status and escalated for further analysis, whilst 25 STRs were categorized as ‘low priority’.

Chart 12: STRs received per Sector: Potential Fraud-Related Offence

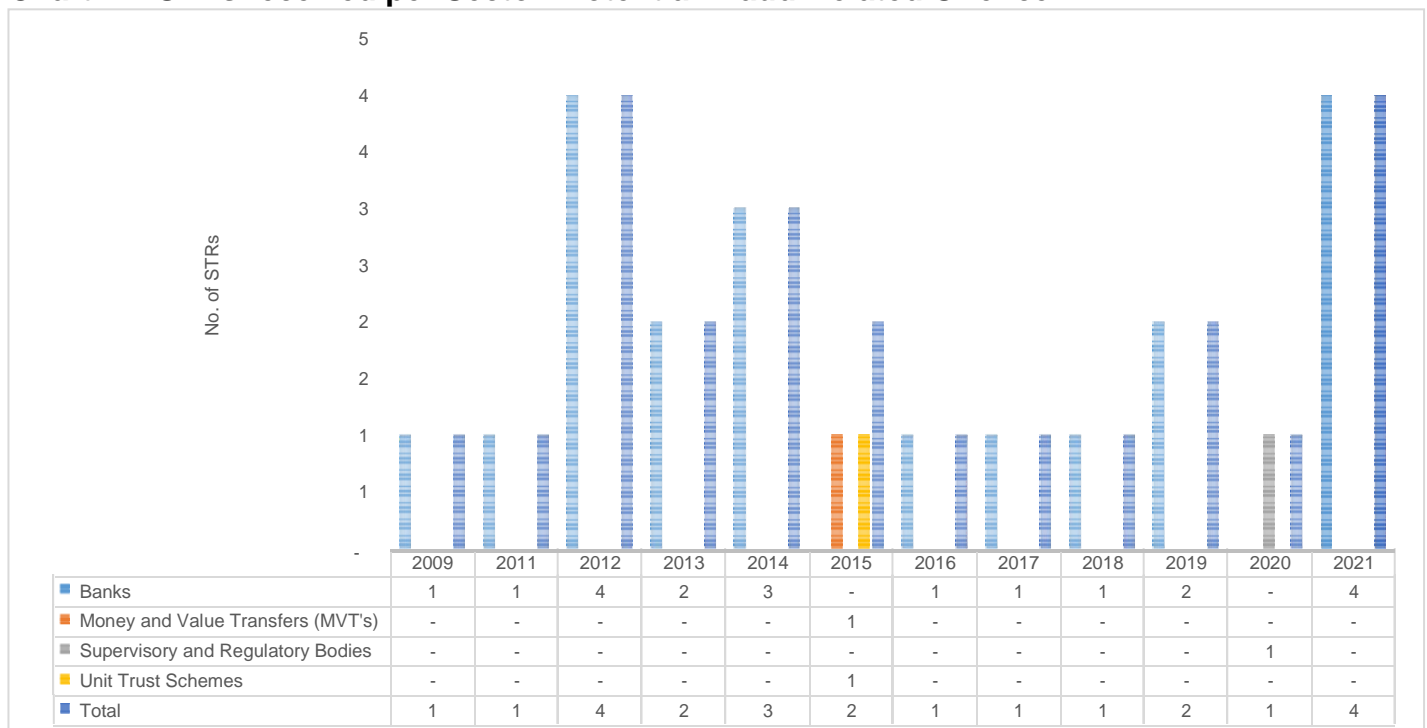
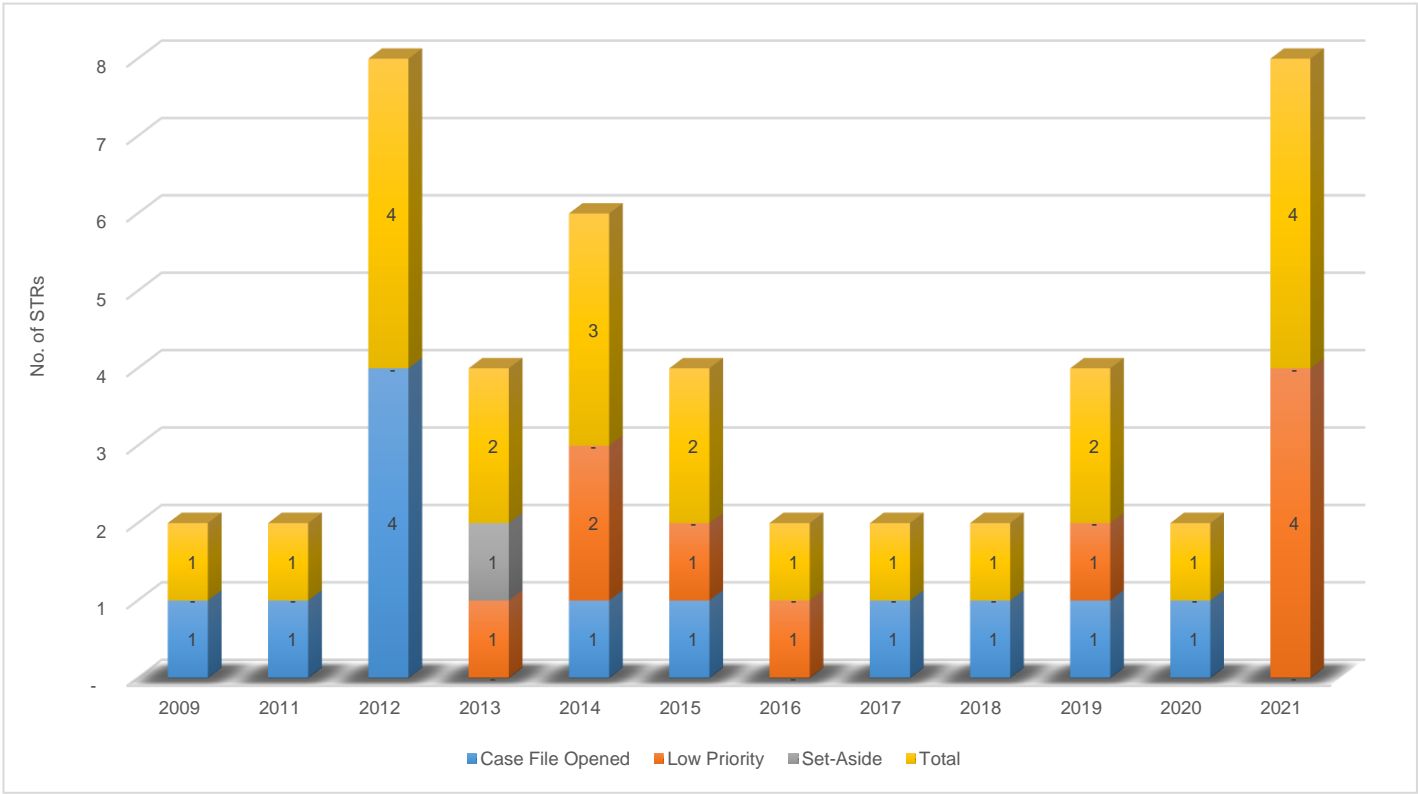


Chart 12 shows a summary of STRs related to potential fraud offence as the second highest leading ML threats involving trust legal arrangements. In the period under review, the FIC received 23 STRs. The highest volume of reports related to potential fraud offence was recorded in the years 2012 and 2021. Overall, 20 reports originate from the banking sector.

Chart 13: Classification of STRs received per Sector: Potential Fraud-Related Offence



The record shows that 52% (or 12 STRs) were accorded “high priority” status and escalated for further analysis, whilst 10 STRs were categorized as ‘low priority’.

Chart 14: STRs received per Sector: Potential Corruption-Related Offence

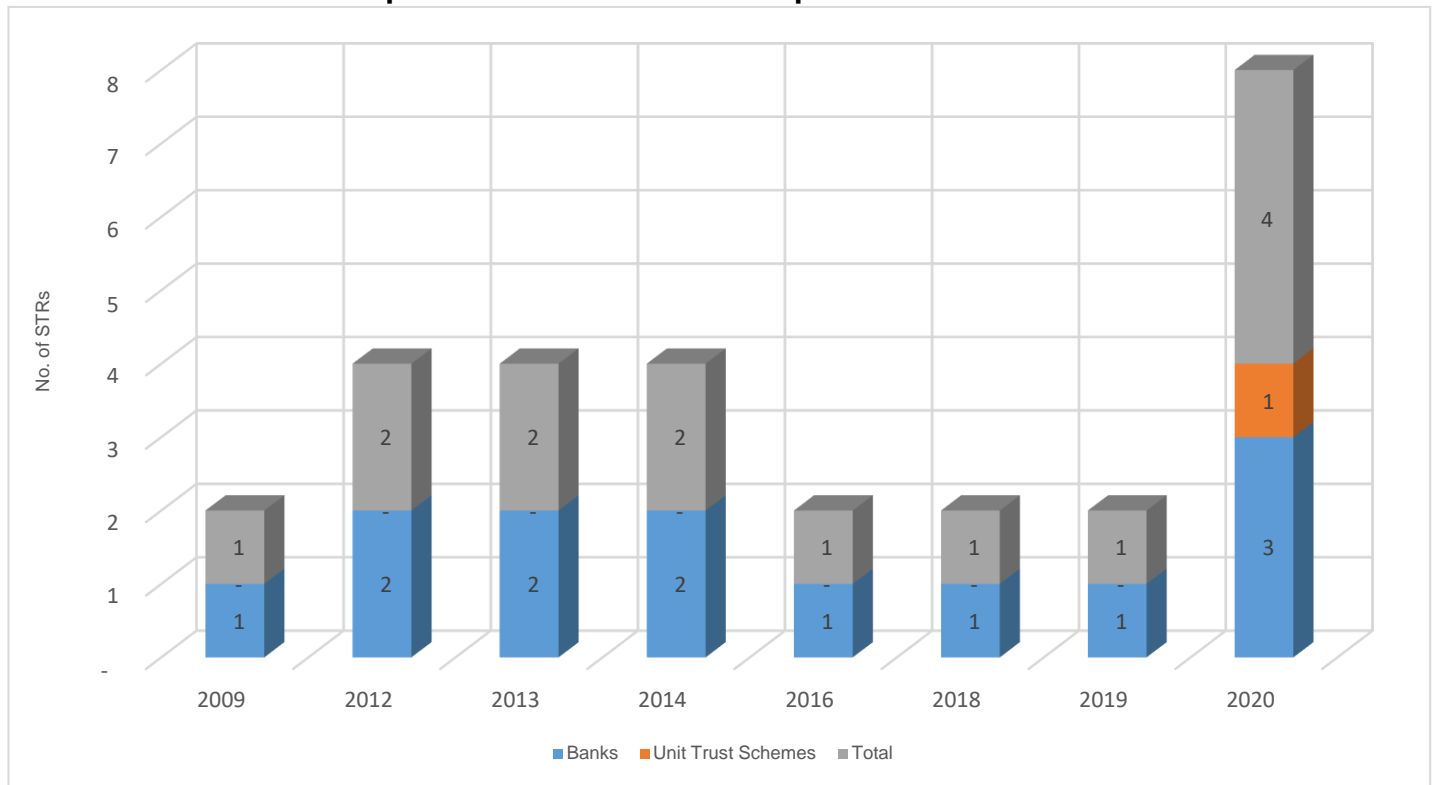


Chart 14 shows a summary of STRs related to potential corruption offences as the highest third ML threat prevalent in trusts. The FIC received a total of 14 STRs, and 99% of the reports originate from the banking sector. Further, 9 STRs were accorded “high priority” status and escalated for further analysis, whereas 5 STRs were categorized as ‘low priority’.

8.2.1 Trust Legal Arrangements STRs transactions as per GoAML Portal

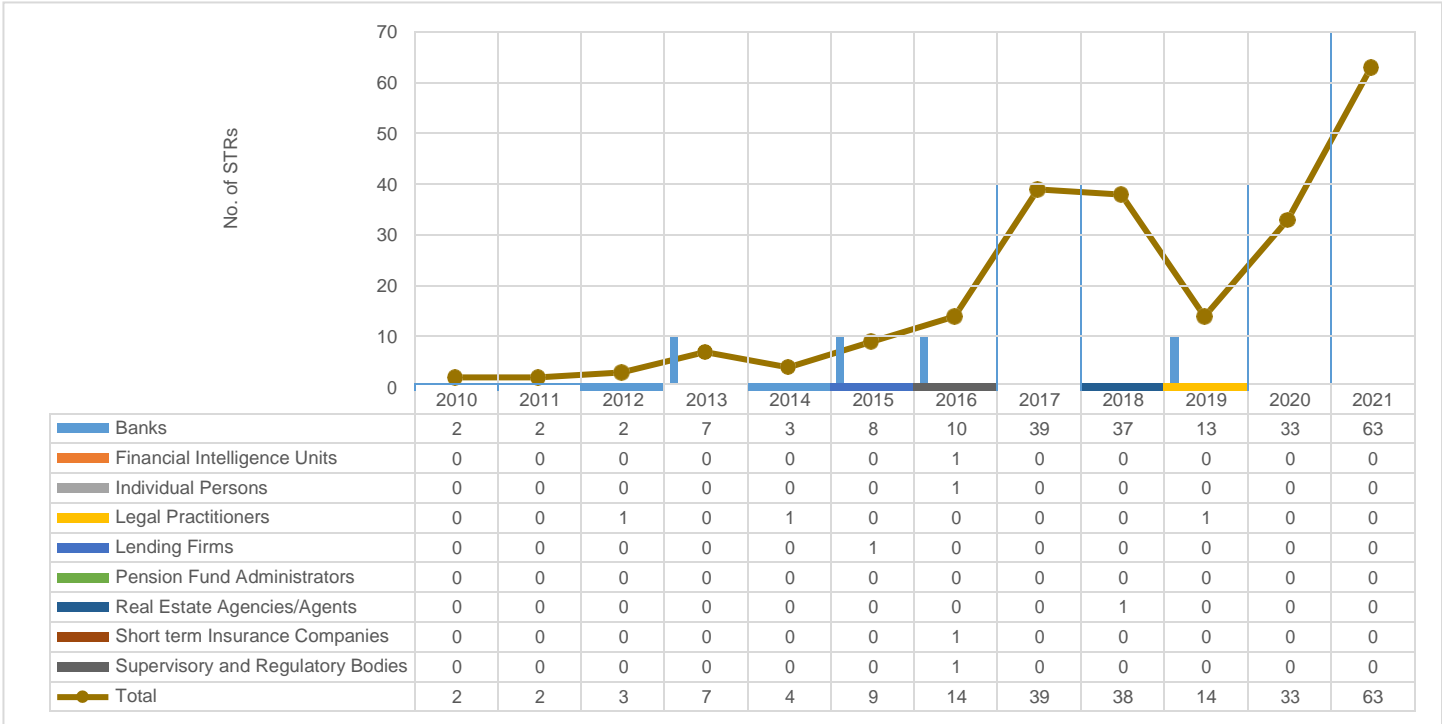
Annexure 2 presents transaction amounts of the STRs filed and the names of involved entities (Trust Companies) during the period under review. The highest single STR transaction of **NAD 30,000,000.00** was reported involving an entity bearing the name “**Trust-001**”, this was followed by “**Trust-002**” with a single STR with a monetary value of **NAD 22,333,792.12**. Overall, a total of 37 STR transactions involving a combined monetary value of **NAD 84,789,079.80** were filed.

8. 3 CLOSE CORPORATIONS (CCs)

This section of the report presents a summary of STRs involving CCs and the classification of such reports in the period under review. As per records from BIPA and the FIC, 85% of the involved CCs are locally owned. Note that the classifications (local or foreign) of around 12% of entities were not

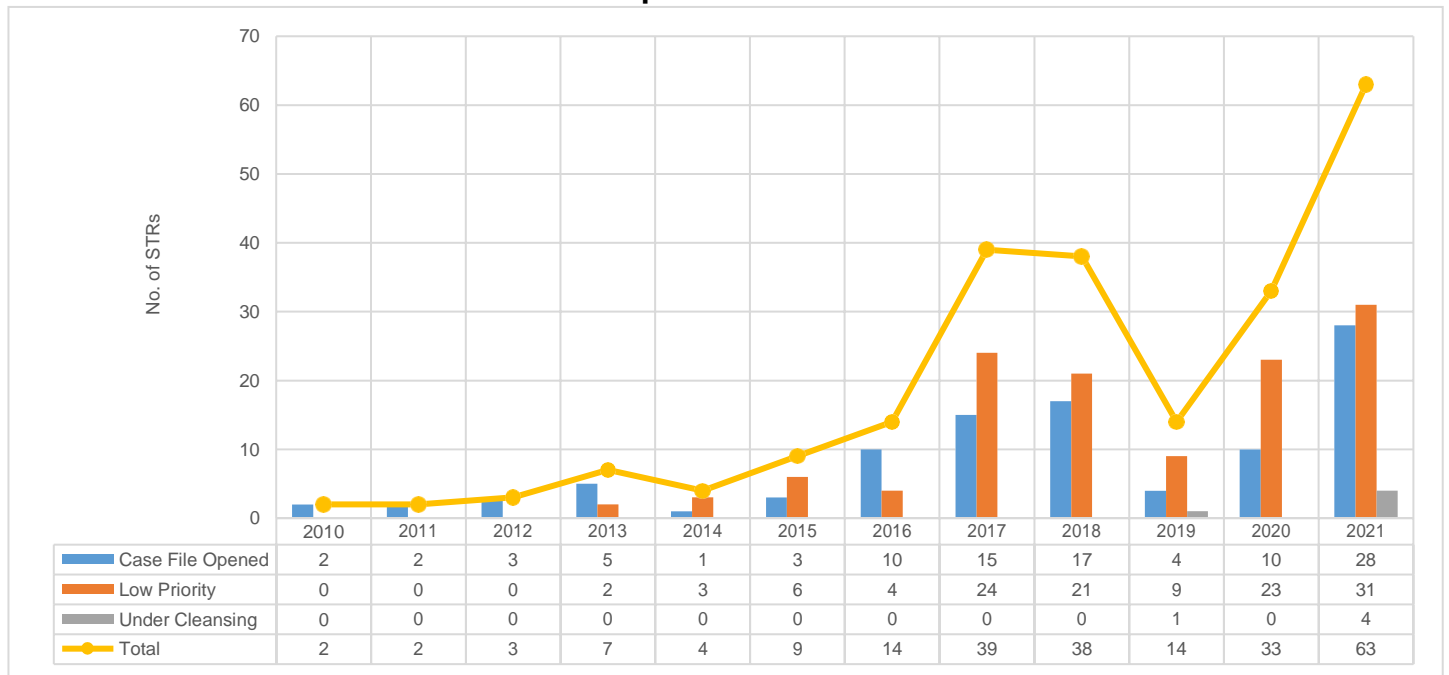
provided. The study also reveals that about 7 involved entities reported in STRs were not recorded or registered with BIPA. Importantly, 76% (or 69) of directors/beneficiaries of involved entities are Namibian nationals. Chinese nationals are the second highest beneficial owners at 7% followed by Indian nationals at 5% and Zimbabweans at 3%. Other least nationals involved as beneficiaries are Somalis, Pakistanis, Swedish, Kenyan, Egyptian and Canadian, though at very minor levels. It is generally accepted that control weaknesses that can be easily undermined to advance ML are also highly vulnerable to TF. Somalis, Pakistanis and Kenyans hail from countries with inherently high terrorism and TF risks. This can inherently contribute to an escalated risk level of potential TF in Namibia, seeing the ease with which they could advance ML.

Chart 15: STRs received per Sector



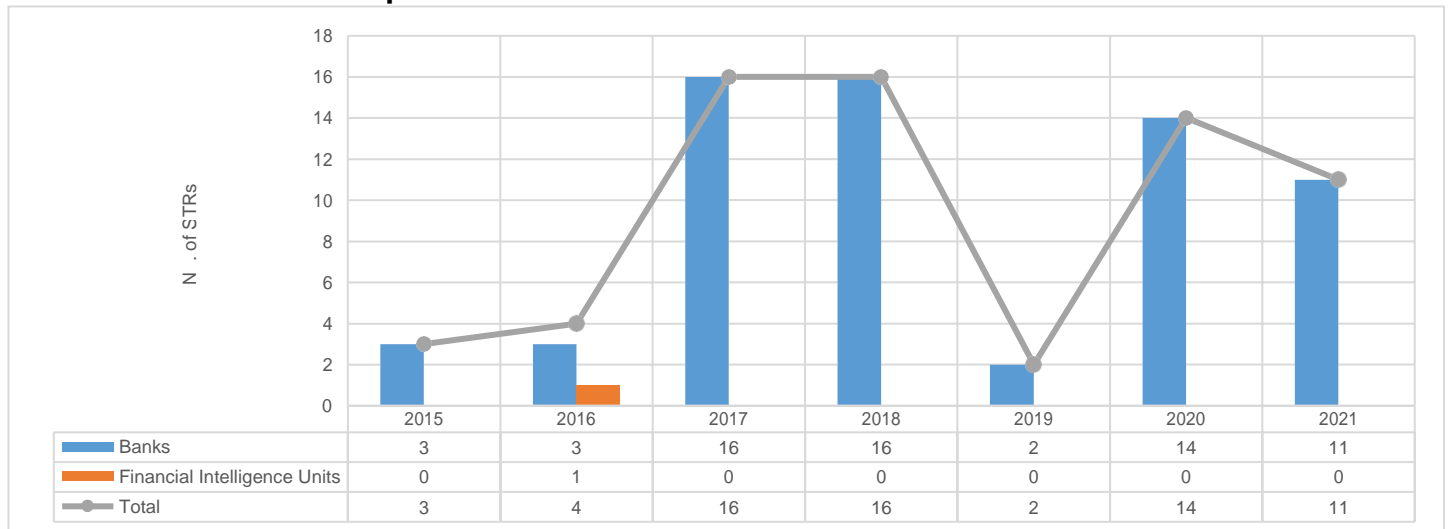
The chart above shows a summary of STRs reported to the FIC involving CCs. During the period under review, the FIC received 228 STRs. The banking sector reported the highest number of STR, 96% (or 219) followed by the Legal practitioners with 3 reports. Annually, the highest number of such (63 STRs) was received in 2021.

Chart 16: Classification of STRs received per Sector



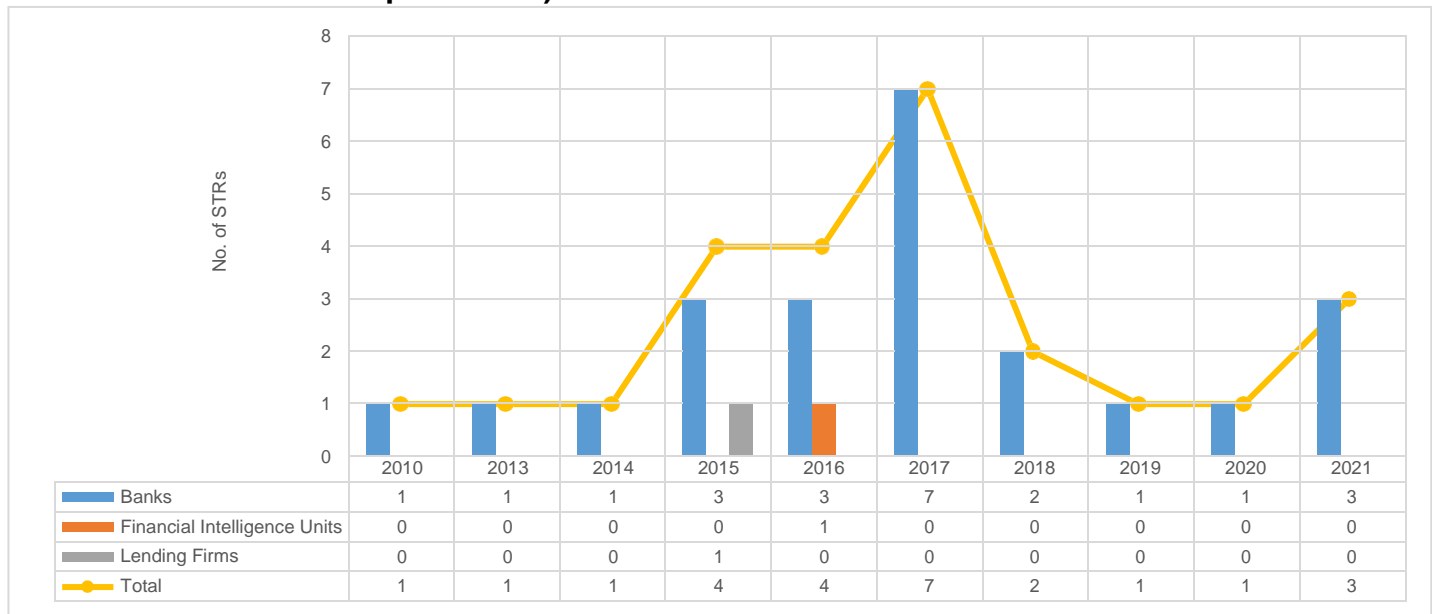
42% or 104 STRs were accorded “high priority” status and escalated for further analysis, whilst 129 STRs were categorized as “low priority”.

Chart 17: STRs received per Sector: Potential Tax-Related Offence



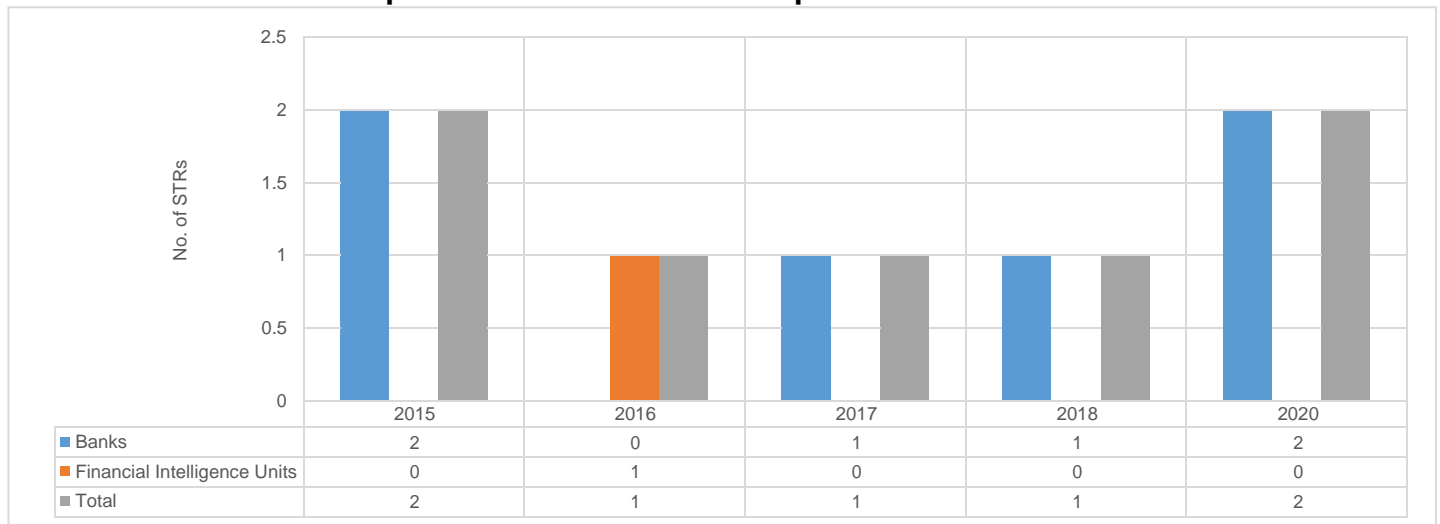
In the period under review, the FIC received 66 STRs related to potential tax offences involving CCs. Most of these reports were filed by the banking sector during the years 2017 and 2018.

Chart 18: STRs received per Sector): Potential Fraud-Related Offence



The Chart above shows a summary of STRs related to potential fraud offences involving CCs. During the period under review, the FIC received 25 such reports. The highest volume, 7 reports, was recorded during the year 2017. The banking sector filed most of these reports.

Chart 19: STRs received per Sector: Potential Corruption-Related Offence

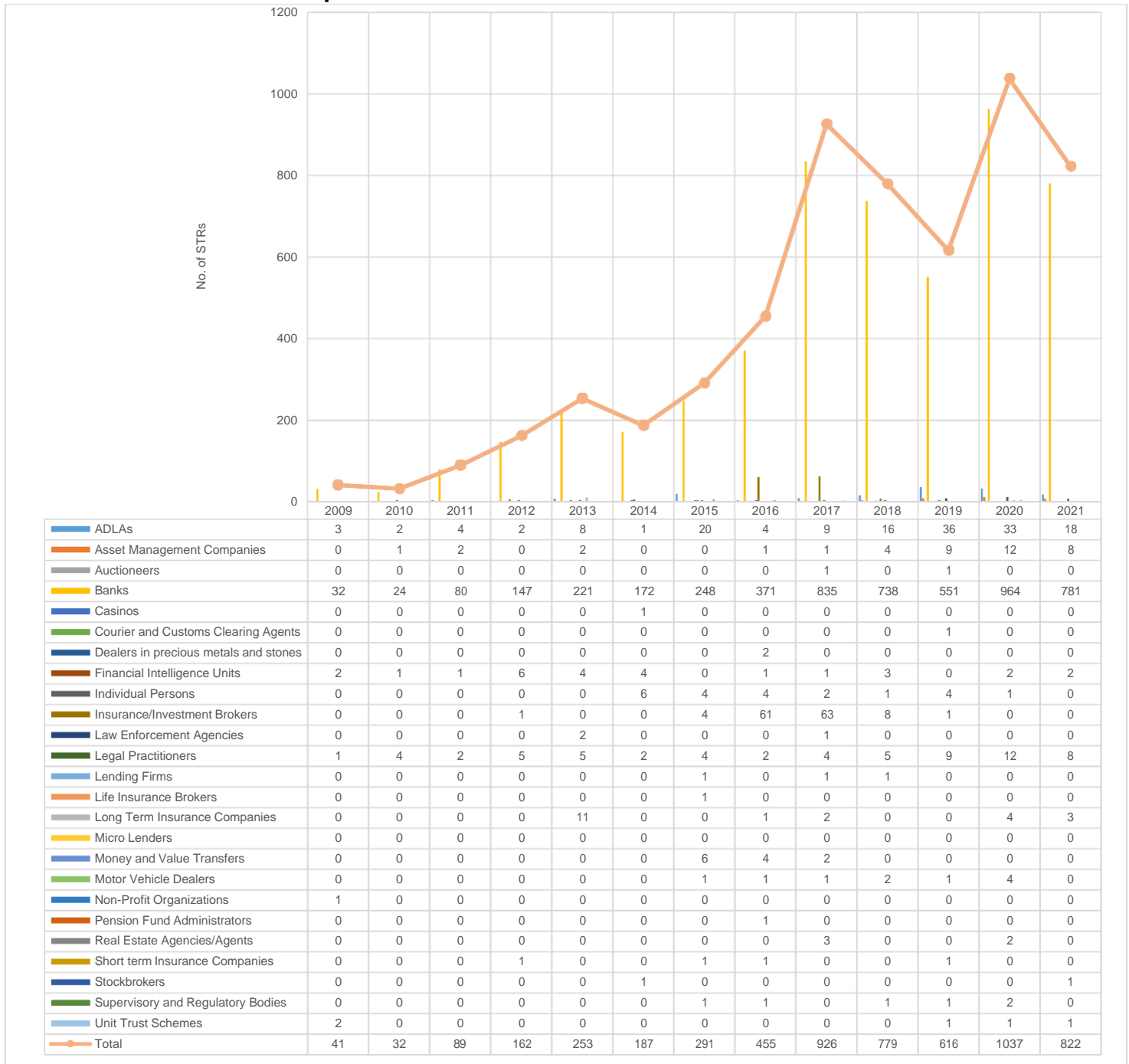


The chart above shows a summary of STRs related to potential corruption offence involving various CCs. The FIC received 7 such reports. The banking sector filed most of these reports.

8. 4 INDIVIDUALS (NATURAL PERSONS)

This section presents a summary of STRs involving several Natural Persons and the classification of such reports in the period under review.

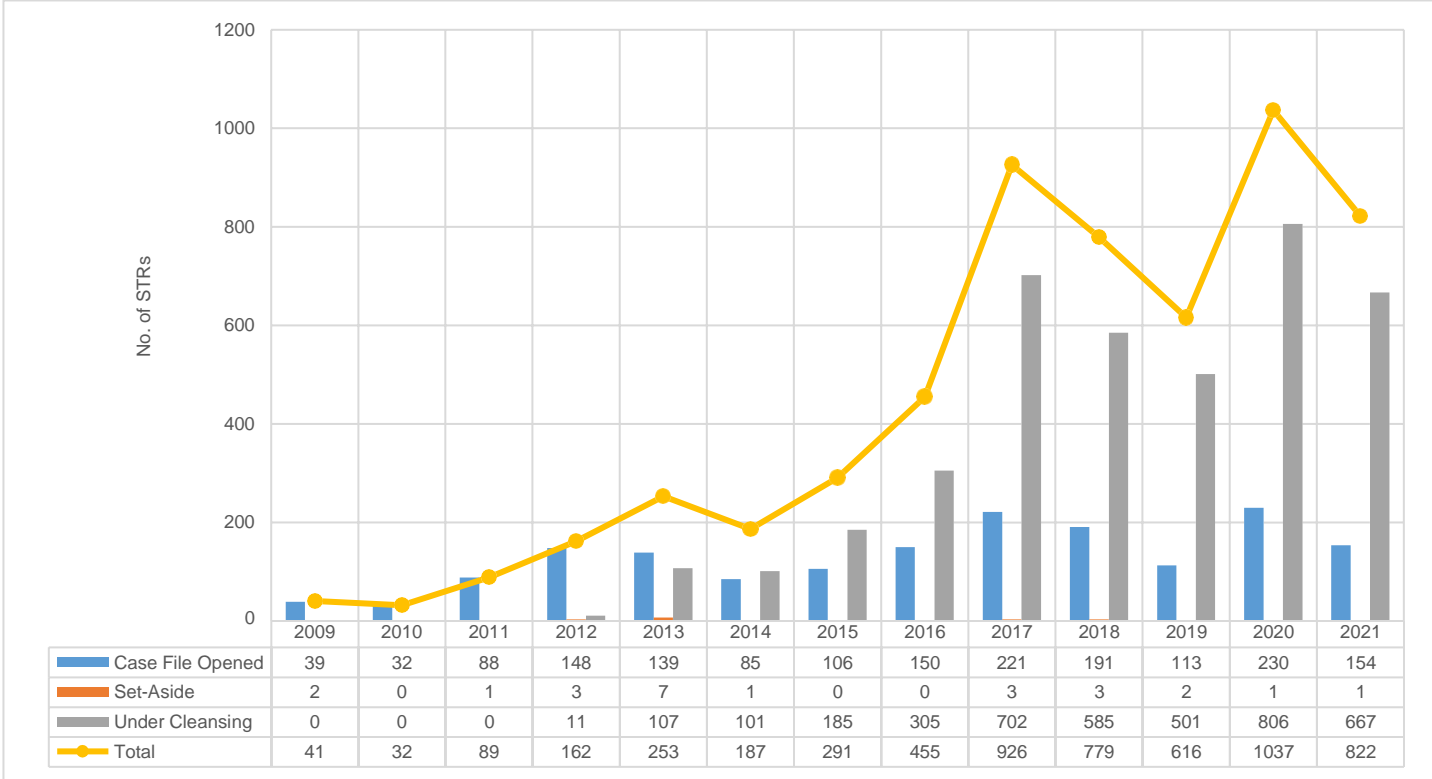
Chart 20: STRs received per Sector



The chart above shows a summary of STRs reported to the FIC involving individual Persons. The FIC received 5,690 STRs. The banking sector led in reporting volumes, filing 91% (or 5,164) of reports

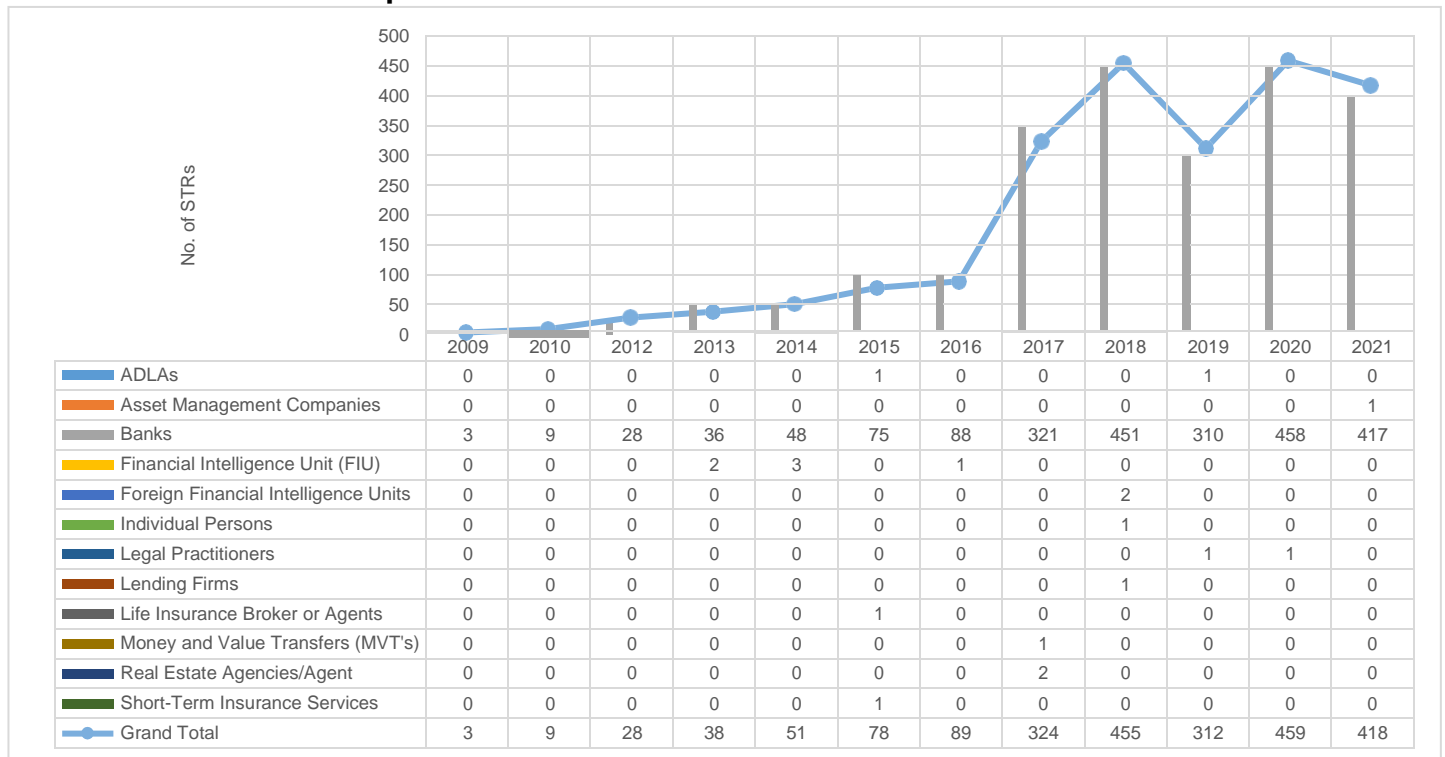
followed by the ADLAs and the Insurance/Investment Brokers sectors with 156 and 138 reports, respectively. Annually, the highest number of such STRs was received in 2020.

Chart 21: Classification of STRs received



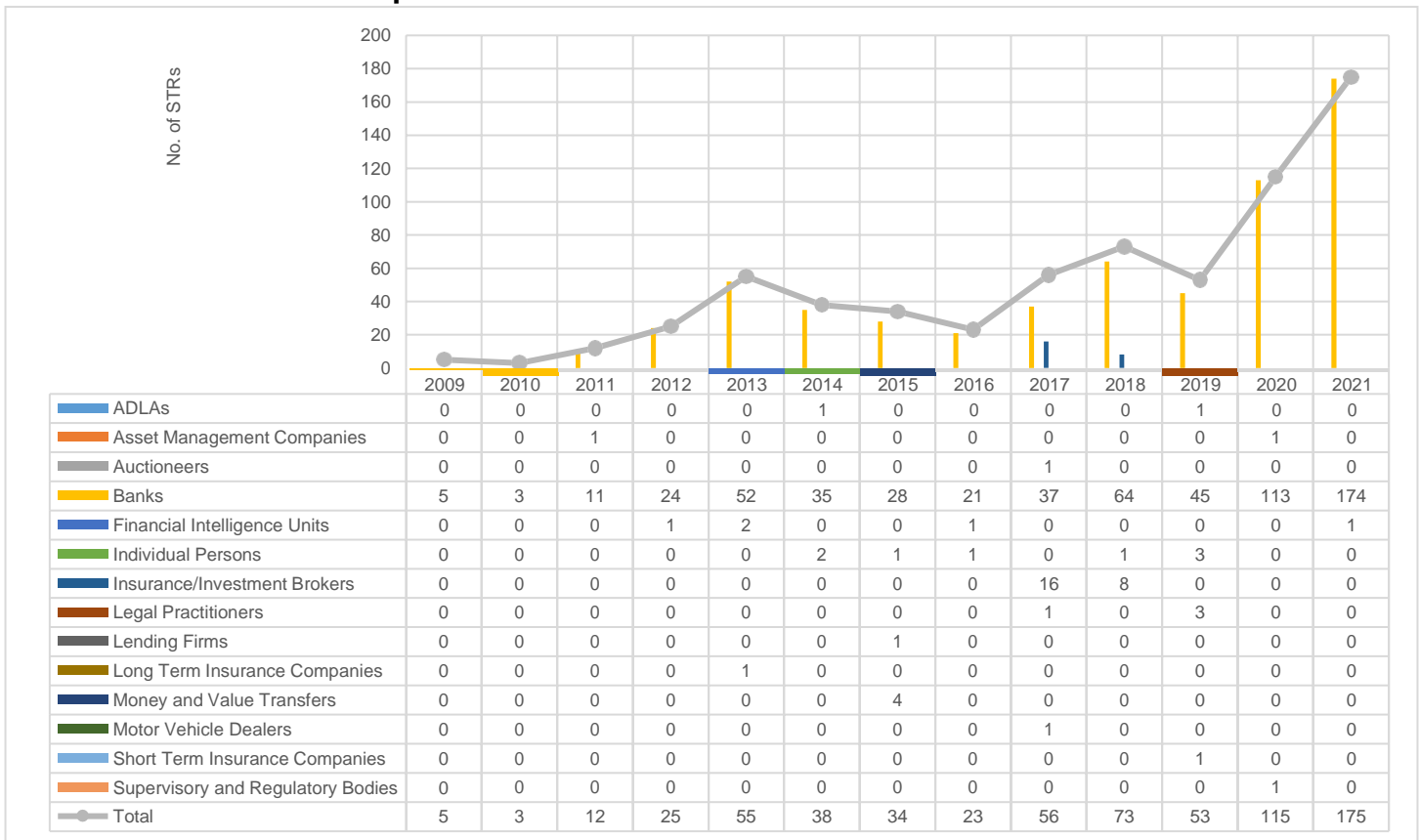
30% or 1,696 STRs involving natural persons were accorded “high priority” status and escalated for further analysis, whilst 3,970 STRs were categorized as “low priority”.

Chart 22: STRs received per Sector: Potential Tax-Related Offence



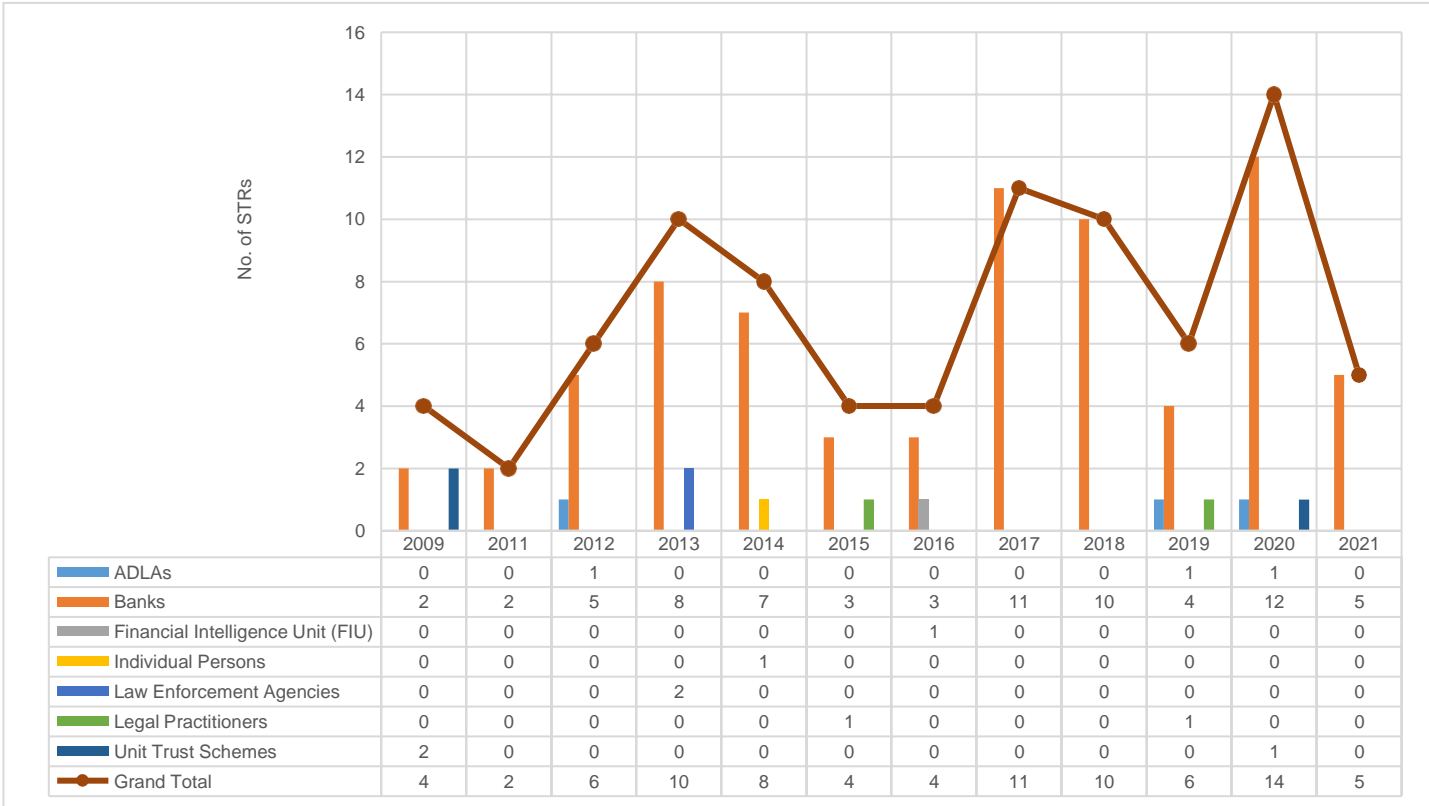
The FIC received 2,264 STRs related to potential tax offences involving individual persons. Most of these reports were filed by the banking sector during the year 2020.

Chart 23: STRs received per Sector: Potential Fraud-Related Offence



The Chart above shows a summary of STRs related to potential fraud offences involving natural persons. The FIC received 667 of such reports. The highest volume of 175 reports was recorded in 2021. The banking sector filed most of these reports.

Chart 24: STRs received from Sectors: Potential Corruption-Related Offence



The Chart above shows a summary of STRs related to potential corruption offences involving natural persons. The FIC received 84 such reports. annually, the highest volume of 14 reports was recorded in 2020. The banking sector filed most of these reports.

9. SUMMARY OF SARs RELATED TO LEGAL PERSONS AND ARRANGEMENTS

This section provides an overview of SARs/cases⁶ related to possible ML/TF threats within legal persons and arrangements filed by reporting institutions. Equally, the section presents the total number of reports escalated to cases associated with various predicate offences such as potential related tax, fraud and corruption.

⁶ Cases within FIC domain

Chart 25: Summary of SARs received by Legal Persons

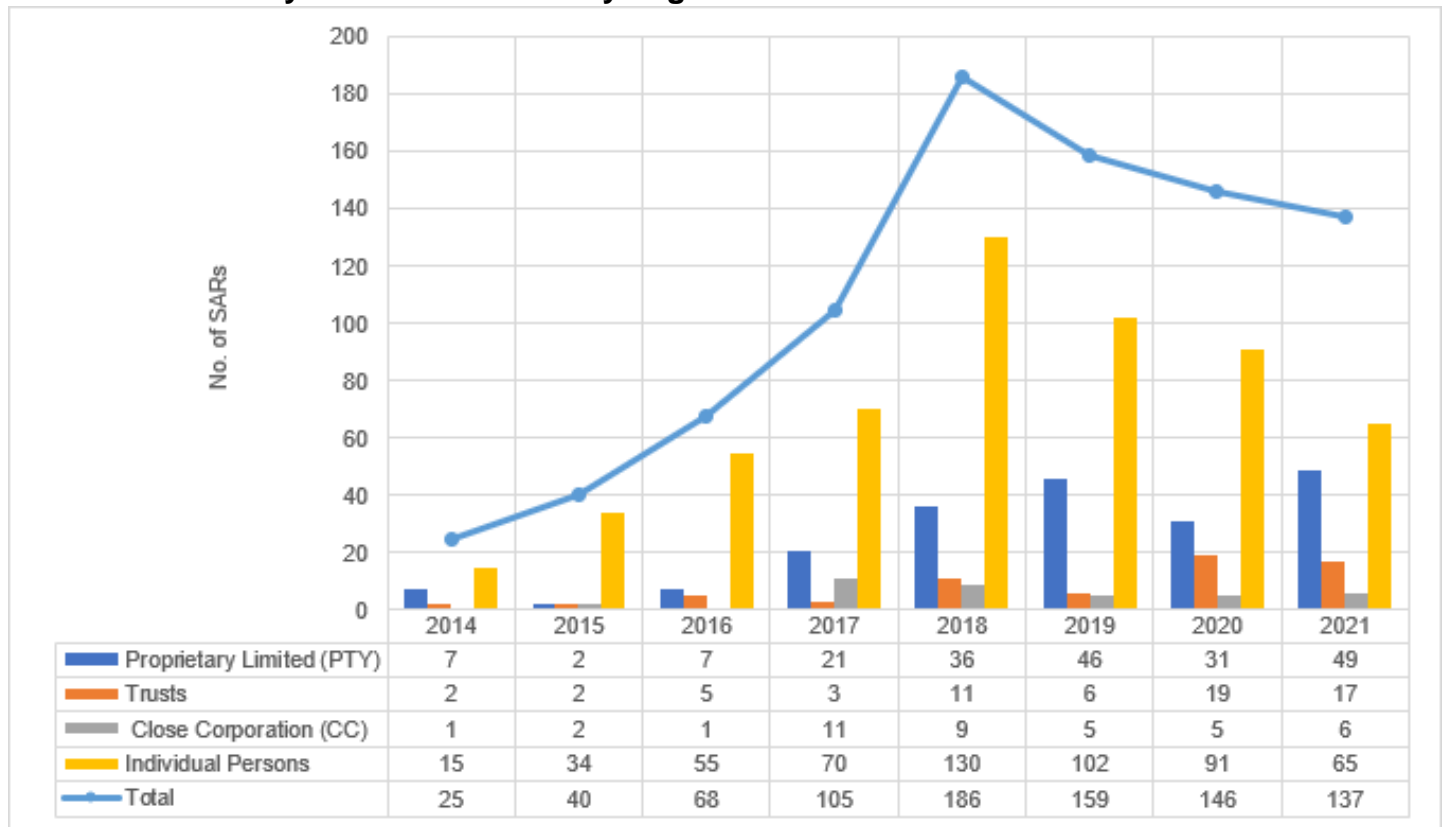
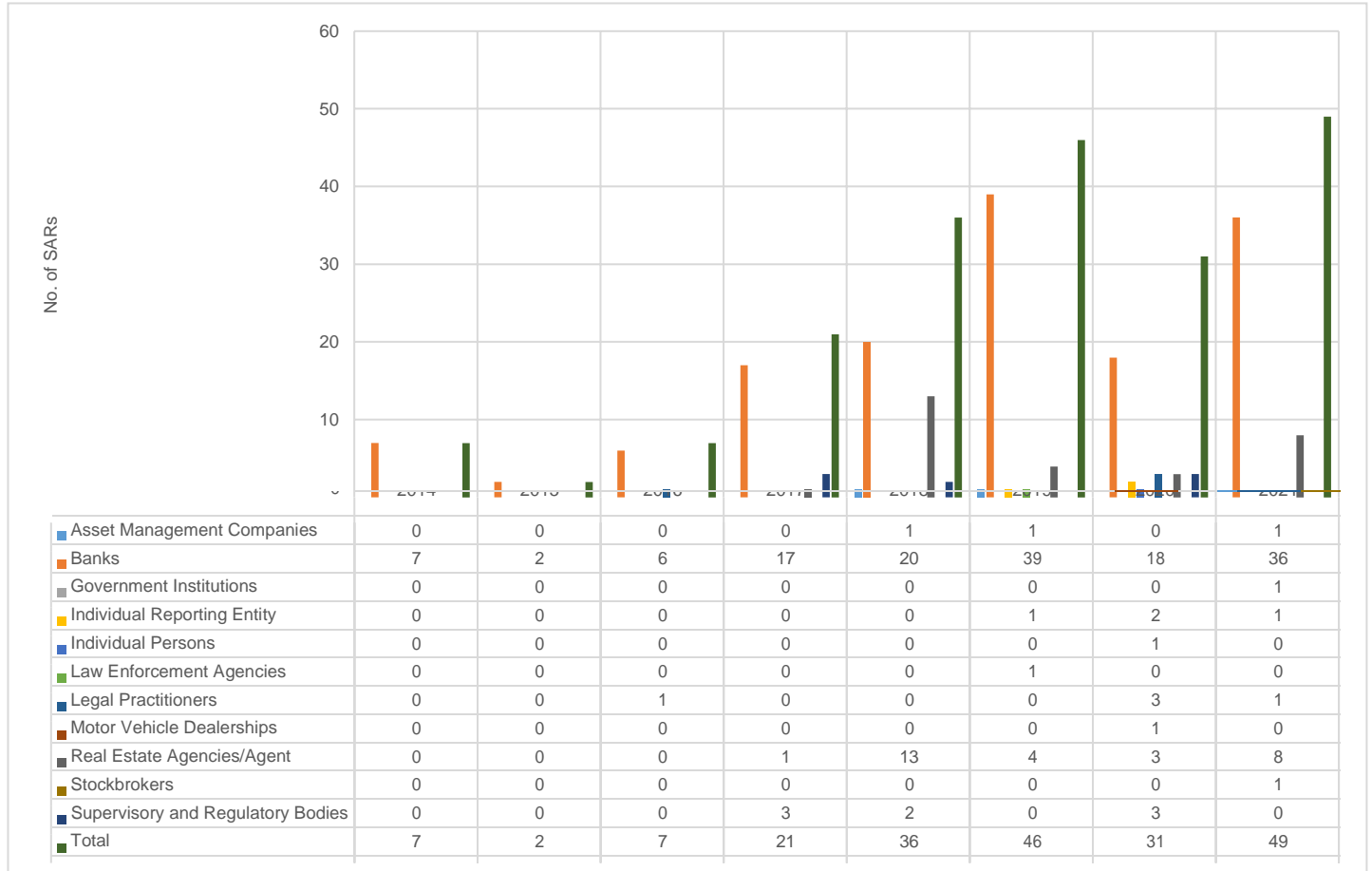


Chart 25 presents a summary of SARs filed by AIs and RIs showing the involvement of different Legal Persons. The highest volume of SARs involves Individual Persons at 65% (or 562 STRs), followed by Proprietary Limited Companies at 23% (or 141 SARs) and then Trusts at 8% (or 65 SARs).

9.1 PROPRIETARY LIMITED COMPANIES

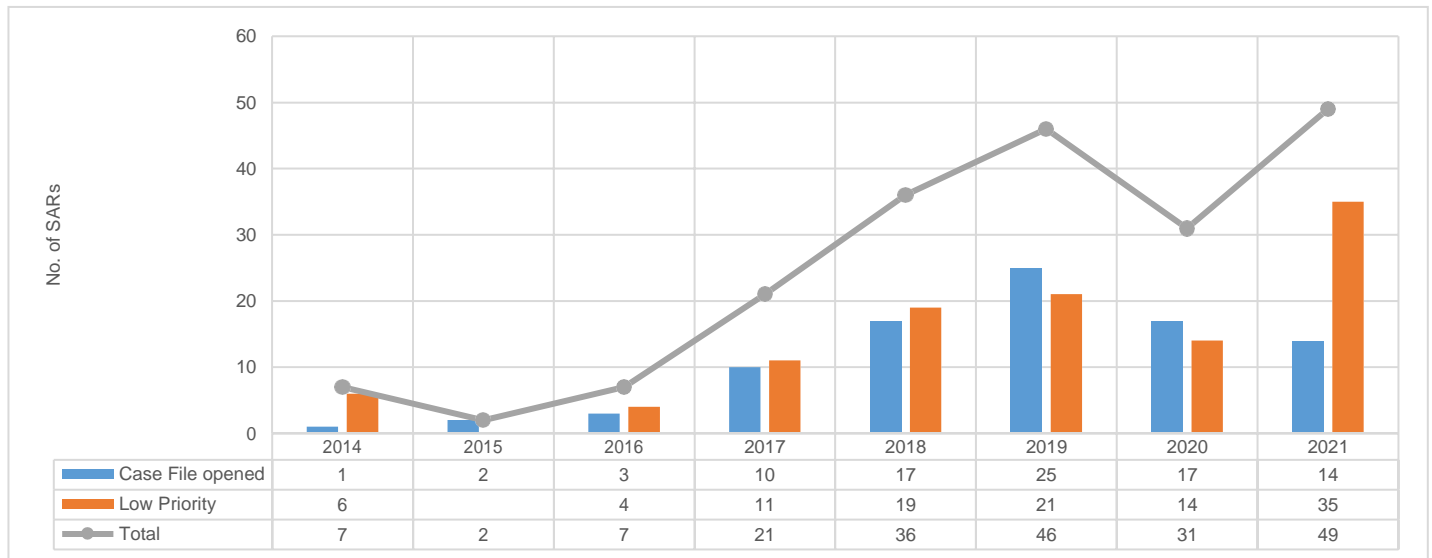
This section presents a summary of SARs involving Pty Ltd and the classification of such reports in the period under review.

Chart 26: SARs received from Sectors



The FIC received 199 SARs involving different Pty Ltd. The banking sector is leading in the reporting volumes, filing 73% of reports followed by Real Estate Agents with 29 reports. annually, the highest number of such SARs was received in 2021. It is worth noting that the following various potential predicate offences were revealed from the analysed reports: 43 tax irregularities, 26 fraudulent activities, 11 corruption-related offences and 8 bribery-related activities, amongst others.

Chart 27: Classification of SARs received

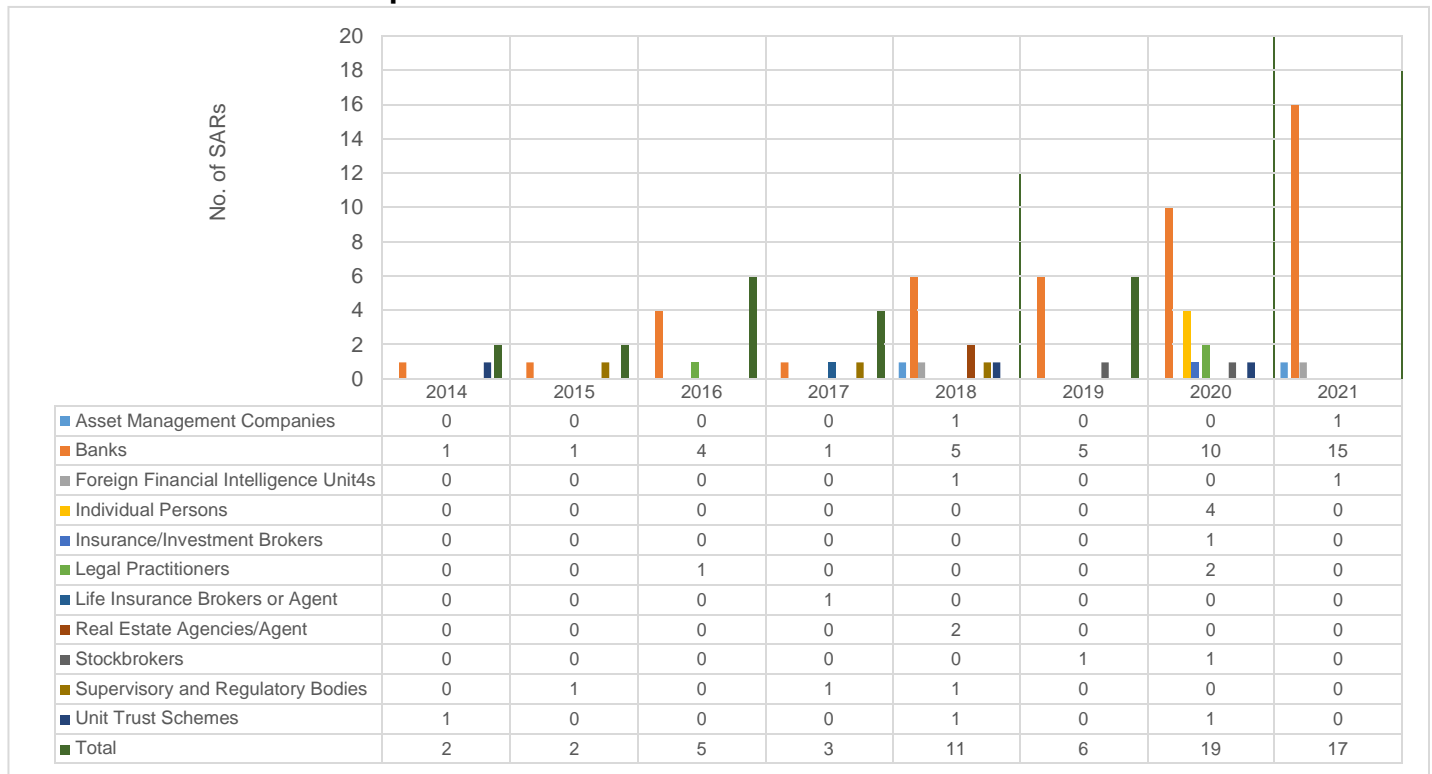


Importantly, 45% were accorded “high priority” status and escalated for further analysis, whilst 110 STRs (or 55%) were categorized as ‘low priority’.

9.2 TRUSTS

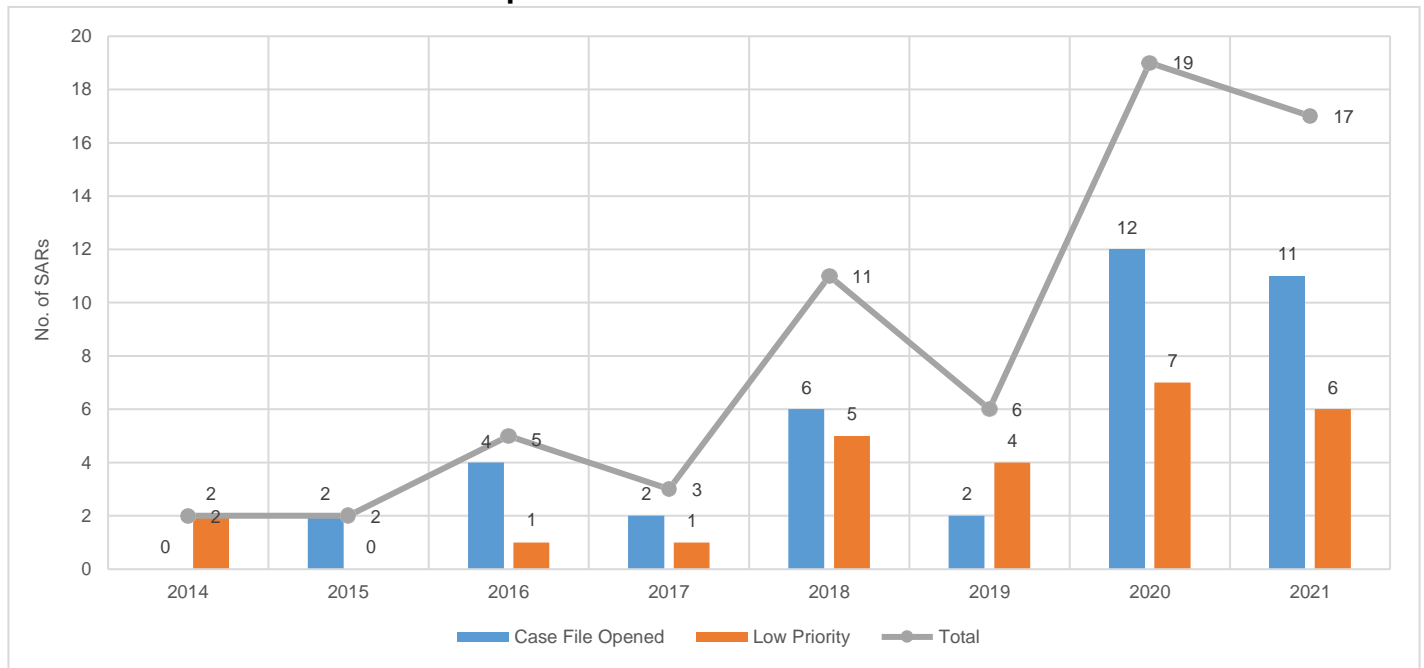
This section presents a summary of SARs involving trusts and the classification of such reports in the period under review.

Chart 28: SARs received per Sector



In the period under review, 65 SARs involving different trusts were recorded, with banks reporting the most STRs. Amongst others, most reports (7) were filed related to potential tax offences, followed by potential corruption (6), then potential fraud with 5 reports Bribery was the least predicate offence with 3 reports.

Chart 29: Classification of SARs per Sector

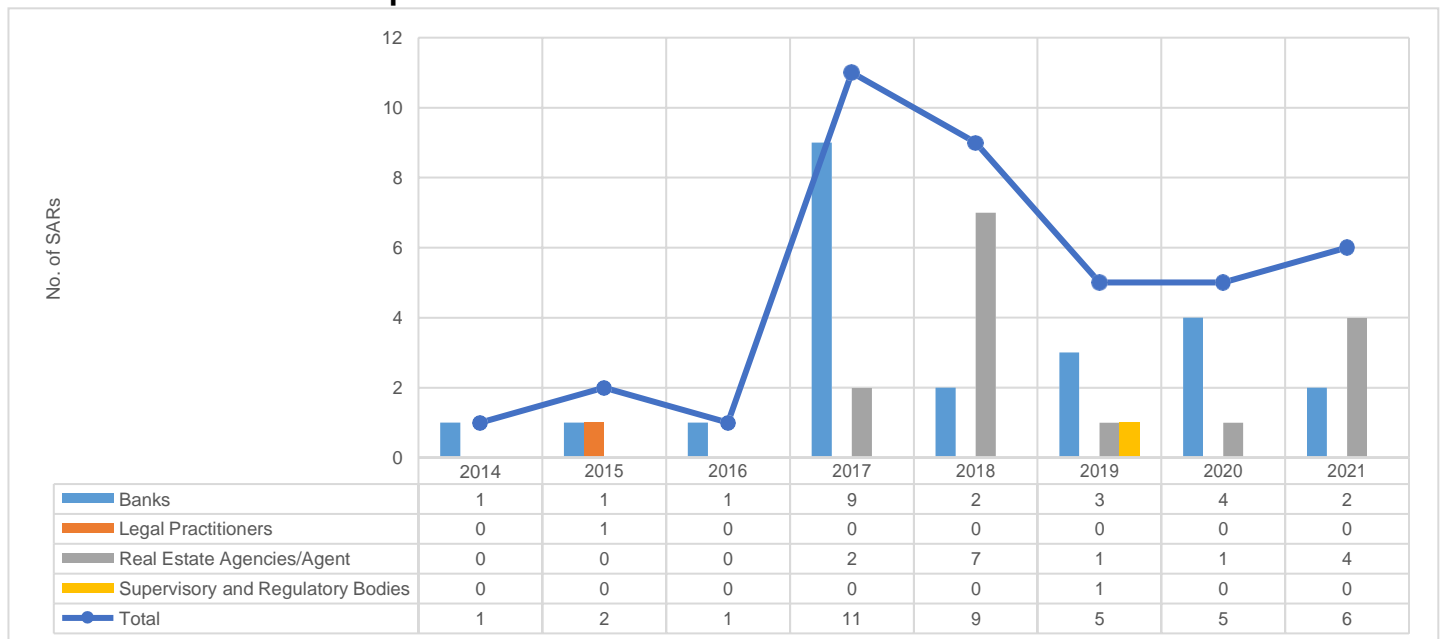


It is revealed that 60% (or 39 reports) were accorded “high priority” status and escalated for further analysis, whilst 26 reports (or 40%) were categorized as ‘low priority’.

9.3 CLOSE CORPORATIONS

This section presents a summary of SARs involving CCs and the classification of such reports in the period under review.

Chart 30: SARs received per Sector



40 SARs involving different CCs were recorded. The highest volumes of reports were filed by the banking sector. Amongst others, most reports filed relate to potential tax offences (19 reports), followed by potential fraud and corruption-related offences with 3 reports each.

Chart 31: Classification of SARs per Sector

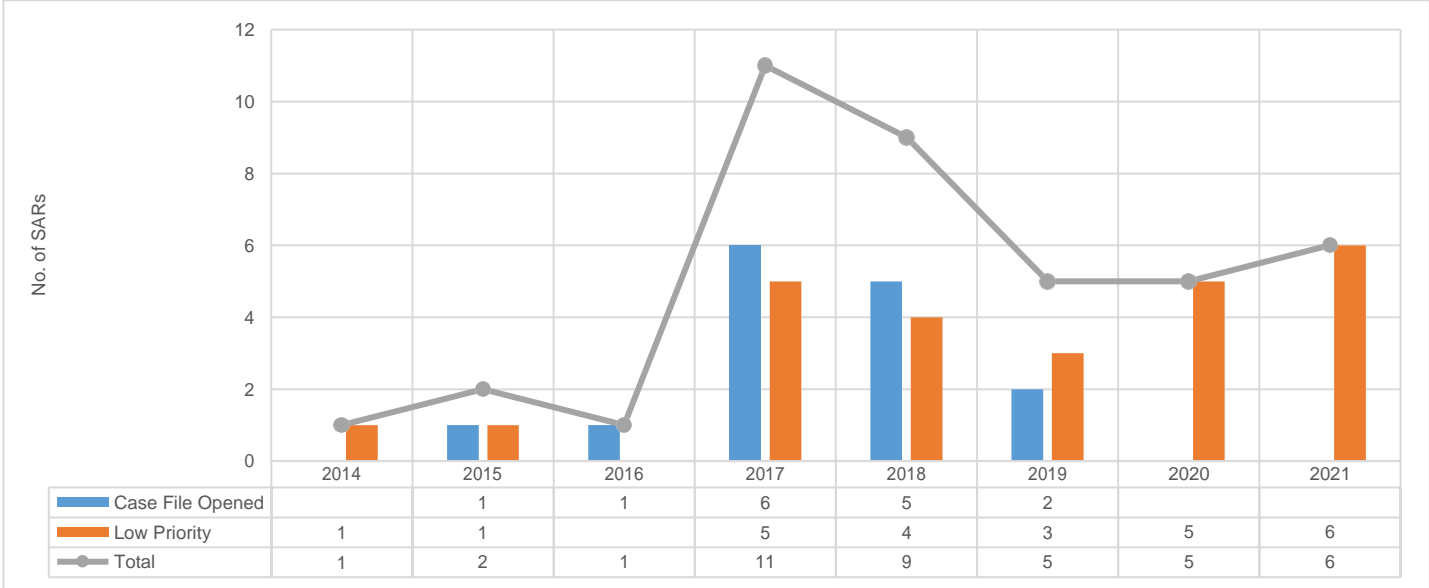


Chart 31 shows that 38% were accorded “high priority” status and escalated for further analysis, whilst 25 reports (or 62%) were categorized as ‘low priority’.

SECTION D

10. SPONTANEOUS DISCLOSURES (SDs) AND AMOUNTS INVOLVED PER LEGAL PERSON/ARRANGEMENT

Not all reports filed with the FIC are analysed and investigated. Some are set aside while those classified as low priority are not attended to immediately. If case files are opened, such enable analysis and investigations. When investigations are completed, the FIC spontaneously discloses such to the relevant Law Enforcement Authorities (LEAs). Spontaneous Disclosures thus refer to the case files referred to LEAs by the FIC for further investigations.

Table 5: Close Corporation

	No. of SDs	Amount Involved (NAD)
Anti-Corruption Commission of Namibia	24	372,091,067.06
Bank of Namibia	29	294,675,044.02
The Ministry of Home Affairs and Immigration	1	3,860,258.87
Ministry of Safety and Security	1	-
Namibia Financial Institutions Supervisory Authority	2	-
Namibian Police	109	856,793,519.58
The Namibia Revenue Agency	385	32,137,738,040.01
Namibia Central Intelligence Service	11	25,036,715.48
Office of the Prosecutor-General	48	1,117,571,515.73
Grand Total	610	34,807,766,160.75

Table 6: Proprietary Limited

	No. of SDs	Amount Involved (NAD)
Anti-Corruption Commission of Namibia	12	202,365,516.52
Bank of Namibia	17	21,866,824.08
Ministry of Finance	2	-
Namibia Financial Institutions Supervisory Authority	2	18,470,682.14
Namibian Police	23	401,730,331.36
Namibia Revenue Agency	61	7,844,694,686.70
Namibia Central Intelligence Service	5	16,132,203.38
Office of the Prosecutor-General	16	153,807,373.95
Grand Total	138	8,659,067,618.13

Table 7: Trusts Companies

Row Labels	No. of SDs	Amount Involved (NAD)
Anti-Corruption Commission of Namibia	5	56,516,585.60
Bank of Namibia	2	-
Law Society of Namibia	1	-
Ministry of Finance	1	-
Namibian Police	1	17,890.50

Namibia Revenue Agency	10	776,270,899.4
Office of the Prosecutor-General	3	-
Grand Total	23	1,613,992,815.33

Table 8: Individual Persons

	No. of SDs	Amount Involved (NAD)
Anti-Corruption Commission of Namibia	105	2,212,083,463.57
Bank of Namibia	183	854,451,830.84
City of Windhoek	1	706,927.15
Namibia High Commission	3	-
Law Society of Namibia	1	-
Ministry of Fisheries	2	-
Ministry of Environment and Tourism	4	-
The Ministry of Home Affairs and Immigration	7	4,603,239.40
Minister of Finance	6	-
Ministry of Mines and Energy	1	-
Momentum Metropolitan Namibia Ltd	2	16,605,042.03
Namibia Financial Institutions Supervisory Authority	10	536,771,393.56
Namibian Police	484	719,312,126.87
Namibia Revenue Agency	650	16,586,136,488.05
Namibia Central Intelligence Service	52	214,833,068.60
Office of the Prosecutor-General	185	2,259,215,500.74
Ministry of Safety and Security	1	-
Namibia Office of the President	1	-
Grand Total	1699	23,404,719,080.81

SECTION E

11. MOST COMMON IDENTIFIABLE POTENTIAL TAX OFFENCES, FRAUD AND CORRUPTION INDICATORS

Similar to every other crime, certain red flags point to detailed indicators. This section presents a summary of detailed indicators that may signal the occurrence or presence of various predicate offences indicated above. Such indicators are observable events that point to the likelihood of specific activities occurring.

11.1 Potential indicators from cases under the FIC domain and general potential indicators

Tax, fraud and corruption are some of the highest predicate offences for ML recorded by the FIC. For supervised institutions to be in a position to identify various predicate offence activities, the essential foundation is having an effective Anti-Money Laundering policy and procedures, as per section 39 of the Financial Intelligence Act 2012. The following have been identified as some of the most common potential indicators within the legal persons and arrangements. When each indicator is viewed in isolation, it may not readily point to a single potential predicate offence, but when viewed with other indicators and relevant factors, it may highlight the presence of various potential predicate offence practices. It is worth noting that these serve merely as a guide and therefore not exhaustive of all indicators:

Table 9: potential indicators under FIC domain

Sector	Predicator Offence	Potential Indicators
Banking	Potential Corruption	<ul style="list-style-type: none"> Banking client's legal representative/s appear in media reports, which link/s client to corruption or other financial crimes; A subject (private employee or public servant) who uses banking services is under investigation for potential economic crimes by LEAs; Sudden cash inflows into a dormant or inactive bank account; Significant and unusual transactions involving non-profit organizations; The client's account consistently receives multiple deposits from government institutions; Long-term contracts are repeatedly awarded to the same subcontractor, or a certain legal entity or legal arrangement is consistently awarded a significant value/volume of contracts by certain authorities.
	Potential Fraud/Bribe/Corruption and Tax Evasion	<ul style="list-style-type: none"> Subject refusing to provide evidence of business activities and source of the funds; The subject is under investigation for potential crimes by other Law Enforcement Agencies; An employee misappropriating investors' funds or defrauding his/her employer; The client's account receives payroll deposits out of line with the occupation or employment listed on his or her profile, or multiple deposits with no

		<p>apparent purpose and that are inconsistent with the client's known occupation, employment or income;</p> <ul style="list-style-type: none"> • Large financial transactions carried out on behalf of minors, incapacitated persons or other persons who may not be included in these categories. Transactions on accounts whose holders appear to lack such financial capacity to make such transactions; • A certain legal entity or arrangement, which is a contractor to a state-owned company, usually receives payments of higher amounts for goods or services which normally should cost less (when compared to the normal market prices for equivalent products or services); • Payments made in favor of public officials originate from accounts of persons that benefited from public procurements/funds, without reasonable justification; • Payments made by contractors for consultancy services, particularly in industries with a higher risk to corruption, where the amount paid appears to be outside the normal price range for such consultancy services.
	Unknown/Potential Corruption	<ul style="list-style-type: none"> • A subject placing funds into an investment account shortly after being de-risked from another commercial bank; • Foreign citizens opening an investment account online and transferring a significant amount of money without proof of source of funds; • Frequent termination of business or investment accounts by individuals; • Significant multiple transfers followed by suspicious cash withdrawals; and • Transactions that take place in accounts of public officials involving cash deposits or withdrawals in unusual frequency.
ADLAs	Unknown/Potential Corruption	<ul style="list-style-type: none"> • A client receiving significant funds as a gift from his relative/associate in a high financial crime risk jurisdiction; and • A client appears in media reports which link the client to corruption or other financial crimes.
Individual Reporting Entities	Potential Corruption/Bribe	<ul style="list-style-type: none"> • An employee responsible for a certain project in a government institution reportedly works with the management of the institution by corruptly allocating tenders and receiving funds via his/her accounts (kickbacks) in return.
Financial Intelligence Unit (FIU)	Unknown/Potential Corruption	<ul style="list-style-type: none"> • A councilor of a traditional authority is reportedly involved in corrupt activities by claiming or applying funds from the authority under false pretenses.
Legal Practitioners		<ul style="list-style-type: none"> • A client who repeatedly appears in the media for suspected corruption allegations approached the legal practitioner to buy property in cash.
Unit Trust Schemes	Unknown/ Potential Corruption/Fraud	<ul style="list-style-type: none"> • A customer conducting transactions that appear to be inconsistent with their profile and/or transaction history; and • Client refusing to provide evidence of business activity and proof of source of income.
	Potential Corruption	<ul style="list-style-type: none"> • A client appears in media reports which link the client to corruption or other financial crimes; and
Insurance/Investment Brokers	Potential Fraud/Theft/Corruption	<ul style="list-style-type: none"> • A subject defrauding an insurance company by continuously adding items to the insurance contract and later claiming that the items added were stolen;
Pension Fund Administrators	Potential Fraud /Corruption	<ul style="list-style-type: none"> • Employees abusing the funds for their own gains, making payments without proper authorization;
Short term Insurances	Potential Tax Evasion/ Corruption	<ul style="list-style-type: none"> • Subject is constantly depositing huge amounts of money into a minor's investment plan;
	Unknown/ Potential Corruption	<ul style="list-style-type: none"> • The subject is constantly adding vehicles to the existing policy contract (vehicles are bought in cash);
Stockbrokers	Unknown/ Potential Corruption	<ul style="list-style-type: none"> • A subject placing funds into an investment account and dis-investing within a very short period of time, source of funds not known;

Supervisory & Regulatory Bodies	Potential Fraud/Corruption	<ul style="list-style-type: none"> Employee making payments to suppliers that appear to be fictitious; and
	Unknown/Potential Corruption	<ul style="list-style-type: none"> Entity reportedly receiving funds from an unknown source. It is not known if such a fund is for entity's operations/capital or individual's benefits.

Table 10: General potential indicators of tax, fraud, corruption, and bribe
<ul style="list-style-type: none"> Transactions inconsistent with customers' financial profiles or behavioral patterns;
<ul style="list-style-type: none"> The ownership structure of a company appears unusual or excessively complex given the nature of the business' activities;
<ul style="list-style-type: none"> Client purchases personal property through his or her entity when this type of transaction is inconsistent with the client's ordinary business practice or personal profile;
<ul style="list-style-type: none"> Close family members or associates of public officials are appointed as senior management officials in private companies without meeting the necessary requirements for taking up the position. At times, the high salary or compensation package accorded is not commensurate with market conditions;
<ul style="list-style-type: none"> Significant and unusual transactions involving non-profit organizations;
<ul style="list-style-type: none"> Explanations for transactions may include the use of words and phrases often used as euphemisms for bribes (for example consultation fees, commission, marketing fees, surcharge, etc.);
<ul style="list-style-type: none"> Client attempts to close an account(s) to avoid due diligence questioning by the banks/financial institutions;
<ul style="list-style-type: none"> An entity that pays other firms to perform logistical roles in countries where there is a high degree of perceived corruption and which they could perform themselves, in order to transfer the risk to the other firm;
<ul style="list-style-type: none"> Unusual cash withdrawals from government or public entity's account;
<ul style="list-style-type: none"> A pattern of sending or receiving international EFTs to or from foreign businesses that operate in a sector or industry unrelated to each other;
<ul style="list-style-type: none"> Frequent amendment of business account holders/owners;
<ul style="list-style-type: none"> Transactional patterns from entity accounts that are exclusively one-directional. e.g., the entity only sends but never receives EFTs, or vice versa;
<ul style="list-style-type: none"> Employees abusing the funds for their own gains, making payments without proper authorization;
<ul style="list-style-type: none"> The entity has business activities or a business model that is outside the norm of its sector or conducts no business activities in Namibia. It may also be difficult to confirm the exact nature of the business, however, their account receives significant funds;
<ul style="list-style-type: none"> Employees making payments to suppliers that appear to be fictitious;
<ul style="list-style-type: none"> The client receives large deposits or multiple electronic funds transfers and then orders multiple outgoing cheques and drafts to multiple third-party individuals and companies; and
<ul style="list-style-type: none"> Individuals transacting but appearing to be more concerned by the speed of transaction completion than the transaction cost or risk involved.

11.2 Unexplained wealth or income

These sections speak to observations around persons who may have wealth or income that cannot be legitimately traced to lawful sources or logically explained. Table 3 below illustrates some notable potential indicators of unexplained wealth or income, which may be derived from corrupt activities:

Table 11: Potential indicators of unexplained wealth or income

<ul style="list-style-type: none">• Representative of a public official (i.e. lawyer, secretary, accountant) opens an account and purchases expensive property or luxury goods with the express intent of enabling client/public official to bypass Customer Due Diligence (CDD) processes;
<ul style="list-style-type: none">• Incoming transactions from foreign jurisdictions (specifically from high-risk jurisdictions) on accounts of public officials, which are intended for real estate purchases or purchases of high-value or luxury goods. They typically contain no additional information about the transaction itself and the necessary remittance information is vague (e.g. refers to 'consultancy fees');
<ul style="list-style-type: none">• The stated source of wealth of funds received to an account of a public official may be inconsistent with the client's stated career history, expertise or age. In this regard, a mismatch may exist between the applicant's stated career history and their total net worth;
<ul style="list-style-type: none">• Public officials receive large amounts of money for their attendance in workshops, conferences or as consultants to projects, in order to disguise the origin of the funds from being seen as a payment for corrupt practices;
<ul style="list-style-type: none">• Public officials receive debt relief or repayment requirements are waived by the creditor;
<ul style="list-style-type: none">• Funds received in accounts of persons, legal entities, or legal arrangements with no visible connection to public officials, but known to be controlled by such, or persons related to them (a frontman, a strawman, or a legal entity established to conceal the beneficial ownership);
<ul style="list-style-type: none">• Transactions that take place in accounts of public officials involving cash deposits or withdrawals in unusual frequency and amounts;
<ul style="list-style-type: none">• Private or public officials receive loan guarantees from a public corporation or government body, or a loan under favorable conditions;
<ul style="list-style-type: none">• Financial flows, which reveal complex financial mechanisms and intervention by foreign legal entities or arrangements, are received in an account in another jurisdiction, where the account is related to a public official;
<ul style="list-style-type: none">• Payments by entities to Non-Profit Organizations that public officials are known to be associated with;
<ul style="list-style-type: none">• A transaction or financial activity, which involves foreign nationals with no significant link (apart from the financial) to the country where the transactions took place. These foreign nationals are known to be active consultants or employees of lobbying organizations and are sometimes reluctant to explain the source of wealth/funds or give unsatisfactory explanations;
<ul style="list-style-type: none">• Misrepresentation and/or inconsistency between the declared source of wealth of public officials through their sworn asset declarations, and those established during the due diligence process;
<ul style="list-style-type: none">• Purchases or leases of movable or immovable assets by public officials which are not in line with the client's income;
<ul style="list-style-type: none">• Fixed Term Deposit Certificates made by companies with the main purpose that the capital and interest generated from the investment should be transferred immediately to designated accounts;
<ul style="list-style-type: none">• Payments in favor of public officials are made to facilitate or expedite a government service;
<ul style="list-style-type: none">• Public officials making cash transactions involving large amounts (e.g. currency exchange, use of cash to purchase high-value goods, etc.); and
<ul style="list-style-type: none">• Transaction payments of unusual amounts or frequency from public officials to lawyers, accountants, or other professional intermediaries.

11.3 Corruption in public procurement

Public procurement activities are significantly exposed to corruption. Several factors contribute to this vulnerability. Table 4 below highlights potential indicators of corruption in public procurement activities:

Table 12: Indicators of Corruption in public procurement

- | |
|--|
| <ul style="list-style-type: none">• Subcontractors have a common director(s), beneficial owner(s) and/or are related/associated to the management of the contractor; |
|--|

<ul style="list-style-type: none"> • Procurement projects which are funded through loan agreements by governing bodies such as development institutions but where the eventual tender price put out is significantly higher than the loan amount requested;
<ul style="list-style-type: none"> • Payments are conducted to the accounts of providers of goods, works and services, which are opened in countries different from where such goods, works and services are originated or provided;
<ul style="list-style-type: none"> • Legal entities with little or limited experience receiving highly complex and technical government contracts/projects (not compatible with the known size or expertise of the entity) or receiving government contracts/projects that are not related to their field of business;
<ul style="list-style-type: none"> • EFTs from the public entity being cashed out and subsequently deposited or transferred to accounts of public officials or entities related to public officials;
<ul style="list-style-type: none"> • Funds received by a contractor of public procurements are not spent within a reasonable timeframe to fulfill the contract needs;
<ul style="list-style-type: none"> • The contracting party issues commercial cards to individuals that are not employees of contracting party and are used to purchase luxury goods, make payments for high-cost services or other transactions that are not in the norm of such business expenses. At times, procurement officials are simply availed company bank cards with which they execute purchases. That way, it is not easy to detect the bribes as expenses could be said to have been incurred by the company or its associates;
<ul style="list-style-type: none"> • Payments based on a public procurement contract are conducted at a price higher than originally contracted;
<ul style="list-style-type: none"> • Services provided to state-owned companies or public institutions by companies registered in high-risk jurisdictions; and
<ul style="list-style-type: none"> • Receipt of commission or fees before the signing of an agreement for services or carrying out a function or process in relation to public procurement contract.

SECTION F

12. SAMPLED CASE STUDIES

The FIC observed that in Money Laundering activities, perpetrators continue to explore and find new methods of hiding or concealing the illicit origins of the funds they launder. It is therefore crucial that accountable and reporting institutions constantly conduct risk assessments on their products, services, and customers, in order to enable a proactive approach to combatting ML/TF/PF threats. Below are sample case studies to help understand certain common or notable trends from the reports analyzed.

Case Study 1: Potential Corruption and Bribery

*The FIC analysed a report on Politically Exposed Persons (PEPs) possibly reflecting potential corrupt behavior. It appears that some years ago, **Person-A** who was a minister at that time and **Person-H**, a businessperson may have instructed **Person-C** from **Legal Practitioner-TG** (Firm) to assist them with channeling funds to certain interests including election campaigns of a certain party and other supposed interests of the government.*

*Since **Person-A** was a high-ranking office bearer in the government and **Person-H** was a known and established businessman, the law firm bona fide accepted instructions henceforth. It is claimed that at the time, the **Legal practitioner-TG** had no reason to be suspicious of the instructions and/or motives of both **Person-A** and **Person-H**. It is further purported that, as a result of the sensitivity of the matter, **Person-A** and **Person-H** allegedly advised **Person-C** that the project should always be kept confidential and anonymous. In the advancement of such confidentiality, **Person-A** and **Person-H** allegedly instructed **Person-C** to register and establish a company. It is further noted that **Person-C** was the sole signatory on the account held at Commercial **Bank-T** for this newly established company. By so doing, the actual beneficial owners of the company were hidden from banking and other institutions.*

*On the face of it, at all relevant times thereto, **Person-C** was the only director and held shares in **Company-TY (Pty) Ltd** as a nominee for **Person-A** and **Person-H**. This was apparently done to further ensure the anonymity of the two and keep the process confidential. Over time, numerous large “donations” in form of EFTs were made into the law firm’s trust account from **Company-X and W** subsidiaries whose parent/holding company is based in a foreign country, for the purposes*



mentioned above. The total credits received during the period under review in the trust account for the benefit of **Company-TY (Pty) Ltd** exceeded **NAD 70 million** and distributions were made by the **Legal Practitioner-TG** thereafter to various individuals and entities on apparent instructions of **Person-A** and **Person-H**.









All funds paid into the account of such **company-TY (PTY) Ltd** emanated from a government entity involved in one of the major extractive industries. The **Company-TY (Pty) Ltd** is registered for income tax however, it has declared a nil return since it was established. Additionally, transfers to various entities and individuals who have benefited from such funds show that such beneficiaries did not declare such benefit to the Receiver of Revenue for tax purpose.

Reports were disseminated to relevant law enforcement agencies and investigations are currently underway.

Report source type	STR
Key	Namibian nationals
Perpetrators/Involved	Individuals/Namibian and entities
Involved sector	Banking and Legal Practitioners
Key risk controls	Amongst others, poor payment authorization and verification controls; failure to reconcile bank beneficiary accounts. Failure to detect questionable bank transactional behavior which conflicted nature of supposed business activities. The law firms failed to detect structured business arrangements to undermine beneficial ownership identification.
Designated services	Personal and business bank accounts
Instruments used	EFTs, banks accounts, trust accounts etc.
Offence	Possible corruption and bribery.

Red flags

-  a PEP and businessman instructed a individual from Legal Practitioner to establish and register a business on their behalf;
-  involved subjects requested such business to be kept strictly confidential and anonymous;

-  *the person who established the entity was the only sole director and sole shareholder, for all intends and purposes relating to its transacting behavior;*
-  *frequent large deposits (EFTs) not in line with the account profile;*
-  *notable deposits with a common payment description/reference made into the bank account by various individuals and entities;*
-  *the account is fairly new and received significant funds in no time;*
-  *large electronic fund transfers subsequent to fund deposit;*
-  *bank account transactions not consistent with profile of the business;*
-  *the business is registered for income tax, however, it has declared a nil return since it was established; and*
-  *the entities and individuals who have benefited from such funds did not declare income to the Receiver of Revenue for tax purposes.*

Case Study 2: Potential employee fraud, corruption, and theft

Joeline Joseph is employed as an accountant at **Tarnish (Pty) Ltd**. Her duties involve processing and facilitating payments on behalf of the company to its service providers. **Joeline** lives an extravagant lifestyle, which appears to be beyond the capacity of her known financial earnings. **Joeline** developed a strategy to defraud her employer by registering several close corporations in which she has 100% interest. She then approached **local banks** and opened several bank accounts under the names of the close corporations, to which she had sole signatory rights. Furthermore, **Joeline** holds personal bank accounts with four major commercial banks in Namibia. **Joeline** then used her position to fabricate fictitious invoices for “services rendered” to **Tarnish (Pty) Ltd** purportedly by her entities.








FIC performed an analysis and discovered a regular and significant flow of funds into several personal accounts in the name of **Joeline**. At times, she conducts electronic payments from the close corporation bank accounts into her personal accounts and ATM withdrawals. Funds from the personal accounts were normally disbursed through cash withdrawals, internet banking payments and point of sales purchases (PoS). Investigations revealed that such expenditure was sustaining **Joeline**'s high-end lifestyle. This high-end lifestyle was premised on cash purchases of high-value items including livestock, vehicles, household items and entertainment. To avoid detection by banks, **Joeline** would create payment descriptions that appear to be in line with her

business when moving funds from one account to another to suit the principal business of the entities involved.

A report was disseminated to relevant law enforcement and investigations were conducted.

Report source type	STR
Key	Money Laundering through Fraud, Corruption and Theft
Perpetrators/Involved	Individual and entities
Involved sector	Banking
Key risk controls	poor customer due diligence controls; failure to reconcile transacting behavior to account beneficiary/owner.
Designated services	Bank account
Instruments used	EFTs, Point of Sale (PoS) and ATM
Offence	Fraud/Corruption/Theft

Red flags

-  *frequent large cash deposits not in line with the account profile;*
-  *large cash and electronic funds transfer subsequent to funds deposits;*
-  *large volumes of transactions amongst the accounts to which the subject is signatory;*
-  *large funds withdrawals (PoS and ATMs) and strictly no withdrawing in branches to avoid detection;*
-  *bank account transactions not consistent with the profile of the business;*
-  *immediate funds transfers/withdrawals from the entities' account following fund deposits; and*
-  *a person suddenly starts living beyond her known income (sudden change in her banking behavior/activities).*






Case Study 3: Mobile Risks (Potential Tax-related offence)

A Namibian businessman registered a Close Corporation with BIPA in which he is the sole owner. The business holds a non-resident bank account in South Africa. Such businessman also holds a personal bank account with a commercial bank in Namibia.

During the period 01 March 2016 to 16 April 2017, several individuals locally made cash deposits into his personal bank account amounting to NAD 1.7 million. Thereafter, the funds were transferred to the business bank account in South Africa through ATM and Cellphone transfers. Subsequently, he traveled to South Africa where he conducted large in-branch withdrawals, ATM and PoS transactions. The only known source of income into this account was funds transferred from Namibia by the subject. It appears that the account was merely a conduit for the ease of movement of funds from Namibia to South Africa. Such funds were not duly declared, thus not subjected to relevant taxes locally.

Report source type	STR
Key	Namibians deposit cash locally and withdraw funds from a foreign jurisdiction (South Africa).
Perpetrators/Involved	Individuals/Entities, Namibian
Involved sector	Banking
Key risk controls	Account is used merely as a conduit to quickly move funds from Namibia
Designated services	ATM and Cellphone transfers
Instruments used	Bank accounts, cash deposits, ATM and PoS
Offence	Tax related offence

Red flags

-  *Sudden and frequent large cash deposits into a newly opened bank account;*
-  *Large volume of transactions amongst the accounts to which the subject is a signatory;*
-  *Large in-branch withdrawals, ATM and PoS transactions in the foreign jurisdiction;*
-  *Transacting behavior is not aligned with the known business profile of the entity; and*
-  *Significant inflow of funds within a short period of time.*

Case Study 4: Awarding of Mining License (Potential corruption and fraud offence)

A Chinese entity bought a N\$50 million lithium mining license from a company that is accused of fraudulently manipulating ownership documents with the help of two government officials.

One of the accused people in the case is Ralph Muyamba, former technical assistant to the mines minister.

Information has emerged that a company owned by Muyamba's cousin, Peter Shifwaku, is accused by the Business and Intellectual Property Authority (Bipa) of “fraudulently and dishonestly” tampering with company registration documents with the help of at least two officials from Bipa.

These officials are claimed to have tricked a certain De Klerk out of his company Karlowa Mineral Resources while he was in the hospital recovering from head injuries caused by a car accident. Three officials from the Namibia Ministry of Mines and Energy, 'Ralph' Muyamba, a former technical assistant to the mines minister, and Timoteus Mashuna, a historian in the Ministry of Defence and Veterans Affairs historian. The third official is Ndili Benyamen, a mines' ministry geologist and friend of Mashuna who are accused of playing a role in removing businessman Jacobus de Klerk from claims to a mine in Namibia to Chinese-owned Xinfeng Investments.

Shifwaku, one of the biggest beneficiaries of the N\$50 million transaction of at least N\$18 million, is being accused of removing names from the registration of another private company to enable him to sell it to a Chinese outfit. In the process, Muyamba's cousin, Peter Shifwaku, scored an N\$18 million payment in July which appears to be linked to this lithium deal.

The payment was made through his company, Orange River Mining. Court documents show that Shifwaku agreed to sell 100% of Orange River Mining to the Chinese outfit for N\$50 million on 23 June 2022.

The Chinese company also agreed to pay Shifwaku N\$6 million upon signing the agreement.

That same month, Shifwaku's mining company splashed money on eight vehicles – a Ford Ranger worth N\$1,1 million, Volkswagen Amarok valued at N\$933 400, a top-of-the-range Toyota Hilux Legend worth N\$819 000, three Volkswagen Tiguan worth N\$639 900 each, and two other Toyota Hilux Legends worth about N\$500 000. Bank statements seen by The Namibian show payments of N\$50 000 to N\$400 000 were transferred to people believed to be Muyamba's relatives.

Muyamba resigned from his position amid new revelations about the deal.

Xinfeng, which now owns the lithium mine, is developing a reputation of being on the wrong side of the law in Namibia.






The minister of mines has stopped the company from exporting lithium ore because the company had failed to honor its legal obligation to process the mineral in Namibia. The said company exported 54 000 tones of lithium ore to China, where it claims that they were test samples.

As the company imported 80 Chinese tipper trucks to transport the ore to the harbor, doubts emerged over whether the company had any intentions of building a processing plant in Namibia.

The mining commissioner Shivolo also stopped Xingfeng's mining explorations after the company started mining without an environmental clearance certificate.

Report source type	STR
Key	<i>Fraudulently manipulating company ownership documents</i>
Perpetrators/Involved	<i>Namibian and Chinese Individuals/Entities</i>
Involved sector	<i>Mining Sector</i>
Key risk controls	<i>Lack of transparency and accountability in the awarding of mining licenses</i>
Offence	<i>Corruption and Fraud</i>

Red flags

-  *fraudulently manipulating company ownership documents;*
-  *An official with influence over the selection process has a conflict of interest;*
-  *Competition is deliberately constrained in the award process;*
-  *The winning company or its owners sell out for a large profit without having done substantial work; and*
-  *resigning from the ministry while under investigation.*

SECTION G

13. KEY FINDINGS

The FIC has noted that most legal persons and arrangements seek to comply with the law and their requirements, and they have no desire to be involved in ML/TF activity. Equally, it is significant to state that the sectors are relatively regulated. Inherently, ethical obligations, professional rules and guidance on ML/TF provided by FIA Act of 2012 and other professional bodies should cause legal persons and arrangements to refuse to act for clients who seek to misuse legal services for ML/TF purposes. Importantly, STRs and SARs filed by the reporting institutions under legal persons and arrangements have assisted the FIC and law enforcement agencies (LAEs) in detecting and prosecuting criminals engaged in ML/TF activity.

Clients who are legal persons essentially present higher ML risk than natural persons when the ultimate beneficial owners in such legal persons cannot be readily and reliably identified. Inherently, the more legal persons a bank has as clients, the higher it is ML vulnerability. Below are the key finds concerning the ML threats and vulnerabilities within the sectors. The finding also signifies which type of legal persons and arrangements are more vulnerable ML/TF than the others in the context of Namibia.

13.1 STRs REPORTS

Common potential predicate offences (threats/crimes) under the Pty Ltd section

- a. A total of 232 STRs involved three (3) common potential predicate offences were reported to the FIC under the Pty Ltd section amongst others. Importantly, 115 STRs were accorded “high priority” status and escalated for further analysis. The potential tax-related offence was recorded as the highest with 141 reports, followed by the fraud-related offence with 56 reports, and then corruption-related offence with 35 reports.

The banking sector was found to carry the highest ML vulnerability levels with 98% of the reports originating from this sector. It is further imperative that almost all transactions nationally, from all sectors, pass through the banking sector. The banking sector has comparatively more matured AML/CFT/CPF control systems. Despite this, the huge volumes of clients and

transactions in the sector escalate the risks as control frameworks in banks are under strain to effectively combat ML.

It is understood that beneficial owners who may launder proceeds of crime will most likely use complex ownership structures that hide their identification or representation. From the FIA compliance assessment activities conducted in the banking sector, the FIC observed that in most cases, beneficial owners' information was not adequately obtained when business relationships were established.

According to BIPA record, only one (1) company is indicated to be locally owned. Classifications of other involved companies (local or foreign) were not provided because such information was not captured in their system. It is further significant to indicate that these companies are 61% Namibian-owned (directors/beneficiaries) whereas 31% are foreign beneficiaries. Additionally, the record show that 9 foreign beneficiaries are Chinese, 5 South African, 3 British, 2 Spanish, 1 Zimbabwean, 1 Icelander, 1 Bulgarian and 1 Russian citizen.

Common potential predicate offences (threats/crimes) under the Trust Legal Arrangements section

- b. A total of 96 STRs involved three (3) common potential predicate offences were reported to the FIC under the trust legal arrangements section. Amongst others, the potential tax-related offence was recorded as the highest with 59 reports, followed by the fraud-related offence with 23 reports, and then corruption-related potential offence with 14 reports. It is noted that 55 STRs were accorded "high priority" status and escalated for further analysis.

Generally, banks were found to carry the highest ML vulnerability levels with 92% of the reports originating from the banking sector. Significantly, the capacity of clients transacting with different persons via the banking systems also enhances ML vulnerability.

It is worth noting that the trusts highlighted in this report are all inter-vivo trusts. It is further significant to indicate that these trusts are 100% Namibian entities registered with the Namibian Master of High Court and none of them are charitable trusts. It is also revealed that about 82% of these trusts have Namibian donors and Namibian trustees, respectively. Additionally, 40% of

these trusts have foreign nationals listed as beneficiaries whereby the majority are South African citizens.

Common potential predicate offences (threats/crimes) under CCs section

- c. Overall, a total of 228 STRs involved in several CCs were reported in the period under review. Importantly, 42% or 104 STRs were accorded “high priority” status and escalated for further analysis. Similarly, the analysis underlined three (3) common types of potential predicate offences under this section. The potential tax-related offence was recorded as the highest with 66 reports, followed by fraud-related offence with 25 reports, and then corruption-related offence with 7 reports. The banking sector is leading in the reporting volumes, filing 96%.

As per BIPA records, 85% of the involved CCs are locally owned. However, the record shows that the classifications (local or foreign) of around 12% entities were not provided. The study also reveals that about 7 involved entities were not recorded or registered with BIPA. Importantly, 76% (or 69) directors/beneficiaries of involved entities are Namibian nationals. Chinese nationals become the second highest beneficiaries with 7% followed by Indian nationals with 5% then Zimbabweans with 3%. Other least nationals involved as beneficiaries are Somali, Pakistani, Swedish, Kenyan, Egyptian and Canadian.

13.2 SARs REPORTS

Common potential predicate offences (threats/crimes) under Pty Ltd section

- d. Overall, a total of 199 SARs involved four (4) common potential predicate offences were reported to the FIC under the Pty Ltd section. Further, 89 SARs were accorded “high priority” status and escalated for further analysis. Essentially, the potential tax-related offence was recorded as the highest with 43 reports, followed by the fraud-related offence with 26 reports, corruption-related offence with 11 reports and then bribe with 8 reports amongst others. The banking sector is leading in the reporting volumes, filing 73% (or 145) of reports followed by the Real Estate Agencies/Agent with 29 reports.

Common potential predicate offences (threats/crimes) under the Trust Legal Arrangements section

- e. Overall, a total of 65 SARs involved four (4) common potential predicate offences were reported to the FIC under the trust legal arrangements section. Subsequently, 60% (39 SARs) were accorded “high priority” status and escalated for further analysis. Inherently, the potential tax-related offence was recorded as the highest with 7 reports, followed by the corruption-related offence with 6 reports. The potential fraud-related offence is in the third position with 5 reports then bribe with 3 reports amongst others.

Common potential predicate offences (threats/crimes) under CCs

- f. Similarly, a total of 40 SARs involved three (3) common potential predicate offences were reported to the FIC under this section. Further, 38% (15 SARs) were accorded “high priority” status and escalated for further analysis. importantly, the potential tax-related offence was recorded as the highest with 19 reports, followed by potential fraud and corruption-related offence with 3 reports each. The banking sector was found to carry the highest ML vulnerability levels with 58% of the reports originating from this sector, followed by the Real Estate Agencies/Agents with 38% of the total reports.

14. CONCLUSION

It is significant to note that not all legal persons and arrangements are undertaking the customer due diligence (CDD) measures required by the FIC and not all the supervisory bodies have a clear understanding of information on ML/TF vulnerabilities specific to the legal sector to provide to their members. A lack of awareness and/or lack of education about ML/TF vulnerabilities and red flag indicators reduces the likelihood that legal persons and arrangements would be in a position to prevent the misuse of their services.

This typology has demonstrated that criminals are involved in the legal persons’ ML schemes. The analysis in this report considered the overall risks of the legal structures established in Namibia being misused for financial crimes. It is important that the Compliance Monitoring and Supervision Division takes effective measures to enhance report quality or value adding STRs/SARs which can lead to effective investigations, prosecutions, asset forfeitures and asset/tax recoveries. It is within this spirit that this report is shared. This report or similar studies on the vulnerability of legal persons and arrangements will be updated periodically when the need arises.

P.P K 

K HAMUTENYA

ACTING DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

15. ANNEXURES

Annexure 1. Pty Ltd STRs transactions as per GoAML Portal

Entity	No. of Transaction	Amount (NAD)
Pty Ltd-001	1	15,500.00
Pty Ltd-002	1	29,000,000.00
Pty Ltd-003	1	101,046.00
Pty Ltd-004	1	358,007.50
Pty Ltd-005	1	300,000.00
Pty Ltd-006	1	10,000,000.00
Pty Ltd-007	1	9,000,000.00
Pty Ltd-008	1	9,000,000.00
Pty Ltd-009	1	3,000,005.00
Pty Ltd-010	8	729,000.00
Pty Ltd-011	1	50,000.00
Pty Ltd-012	1	24,548,564.00
Pty Ltd-013	1	333,500.12
Pty Ltd-014	1	490,200.00
Pty Ltd-015	1	300,000.00
Pty Ltd-016	4	52,000.00
Pty Ltd-017	1	5,000,000.00
Pty Ltd-018	1	753,500.00
Pty Ltd-019	1	30,000.00
Pty Ltd-020	1	1,000,000.00
Pty Ltd-021	1	4,000,000.00
Pty Ltd-022	1	600,000.00
Pty Ltd-023	1	500,000.00
Pty Ltd-024	1	3,152,885.31
Pty Ltd-025	1	50,000.00
Pty Ltd-026	3	7,487.81
Pty Ltd-027	1	120,750.00
Pty Ltd-028	1	19,135,092.56
Pty Ltd-029	1	1,500,000.00
Pty Ltd-030	1	14,000,000.00
Pty Ltd-031	1	100,000.00
Pty Ltd-032	1	62,350.00
Pty Ltd-033	1	63,850.00
Pty Ltd-034	1	7,245.00
Pty Ltd-035	1	1,286,495.37
Pty Ltd-036	1	85,285.57
Pty Ltd-037	1	51,750.00
Pty Ltd-038	1	10,000,000.00
Pty Ltd-039	1	910,000.00
Pty Ltd-040	77	13,640,220.45
Pty Ltd-041	1	50,000.00
Pty Ltd-042	13	1,615,750.00
Total	143	165,000,484.69

Annexure 2. Trust Legal Arrangements STRs transactions as per GoAML Portal

Entity	No. of Transaction	Amount (NAD)
Trust-001	1	5,960.72
Trust-002	2	3,286.34
Trust-003	1	522,313.00
Trust-004	1	1,997,490.78
Trust-005	2	1,900,867.02
Trust-006	1	10,912.60
Trust-007	1	1,300,000.00
Trust-008	1	4,000,000.00
Trust-009	1	7,590,000.00
Trust-010	1	400,000.00
Trust-011	1	30,000,000.00
Trust-012	3	25,100.00
Trust-013	1	70,000.00
Trust-014	2	2,425,716.00
Trust-015	1	350,000.00
Trust-016	1	234,937.00
Trust-017	1	3,132,807.82
Trust-018	2	6,200,000.00
Trust-019	1	1,000,000.00
Trust-020	1	22,333,792.12
Trust-021	2	223,936.86
Trust-022	6	581,959.54
Trust-023	1	160,000.00
Trust-024	2	320,000.00
Total	37	84,789,079.80