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

FRAUD AND MONEY LAUNDERING TYPOLOGY REPORT

October 2020

TABLE OF CONTENTS

1. DEFINITIONS

“Accountable Institution (AI)” means a person or entity listed in schedule 1 and 3 of the Act. The term “accountable and reporting institutions” in this document refers to all Authorised Dealers and Authorised Dealers with Limited Authority.

“Act” refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

“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;

“Customer due diligence” means a process which involves establishing the identity of a client and monitoring all transactions of the client against the client’s profile.

“FIA” the Financial Intelligence Act, 2012 (Act No. 13 of 2012), as amended (also referred to as the Act).

“FIC” means the Financial Intelligence Centre. It is sometimes referred to as the Centre.

“PF” refers to Proliferation Financing.

“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];

[1] FATF Recommendation 7

“ML” refers to Money laundering.

“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;

“SAR” refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.

“TF” refers to Terrorist Financing; and

“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 actually used for such purpose or to carry out such acts.”

“Terrorism” Whilst no acceptable international definition on terrorism exists, it is generally described as the execution of acts of violence against persons or property, or a threat to use such violence, with the intent to intimidate or coerce a Government, the public, or any section of the public to achieve or promote any tribal, ethnic, racial, political, religious or ideological objectives[2].

[2] See full definition of “terrorist activity” as provided for in section 1 of the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) (PACOTPAA)

SECTION A

2. EXECUTIVE SUMMARY

The primary object of the Financial Intelligence Centre (FIC) is to coordinate Namibia's Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) framework. In the advancement of such object, the FIC works with relevant stakeholders such as regulatory and supervisory bodies, private sector, Law Enforcement Authorities (LEAs) and the Office of the Prosecutor General, amongst others. In furtherance of this, the FIC, receives and analyses data, which is used to identify proceeds of predicate offences to ML/TF and PF. The outcomes of the FIC's analytical work is availed to Competent Authorities (CA) in the form of intelligence disclosures. Such are used in investigations, prosecutions and asset forfeiture activities relating to ML/TF and PF. As a supervisory body, the FIC also plays a significant role in presenting trends, case studies and guidelines to Accountable and Reporting Institutions (AIs/RIs) to enhance the managing of relevant risks.

In terms of the 2012 National Risk Assessment (NRA) outcomes and various FIC monthly and quarterly reports, Fraud remains one of the main predicate offences associated with Money Laundering in Namibia. This report avails a detailed summary of common typologies, patterns and indicators of fraud identified in cases within the domain of the FIC. It is hoped that this report will help enhance sectoral understanding of fraudulent practices and result in the implementation of enhanced control measures within the sectors.

As noted from the various ML/TF/PF NRA activities over the years, there are no threats emanating from or associated with TF and PF activities. This report is thus limited to ML related threats in potential fraud offences.

3. OBJECTIVES OF THIS REPORT

The objectives of this typology report are to:

a) highlight the nature and level of fraud related to potential ML/TF/PF within the FIC regulated sectors;

b) provide notable trends and typologies in the flow of proceeds/finances related to Fraud;

c) enhance understanding of the *modus operandi* employed by fraud perpetrators in sectors;

d) provide valuable sources of information for consideration in conducting Sectoral Risk Assessments, trends and typology studies, guiding control enhancement activities at sectoral and entity level;

e) identify vulnerable areas within the sector frameworks that may need improvement; and

f) highlight red flags or indicators that may assist in combatting fraud.

4. METHODOLOGY

The FIC analysed relevant data, and various reports at its disposal in an effort to understand potential methodologies, trends, typologies, and other related red flags associated with fraud which potentially leads to ML/TF/PF activities. The information contained in this report was derived from STRs and SARs data filed with the FIC by various AIs and RIs. Additional information was sourced from the Cases escalated for further analysis by the Centre and from the Spontaneous Disclosures issued to relevant Law Enforcement Agencies.

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

a) Sanitised intelligence emanating from reports and closed databases;
b) Competent Authorities' investigation outcomes; and
c) Open source research.

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

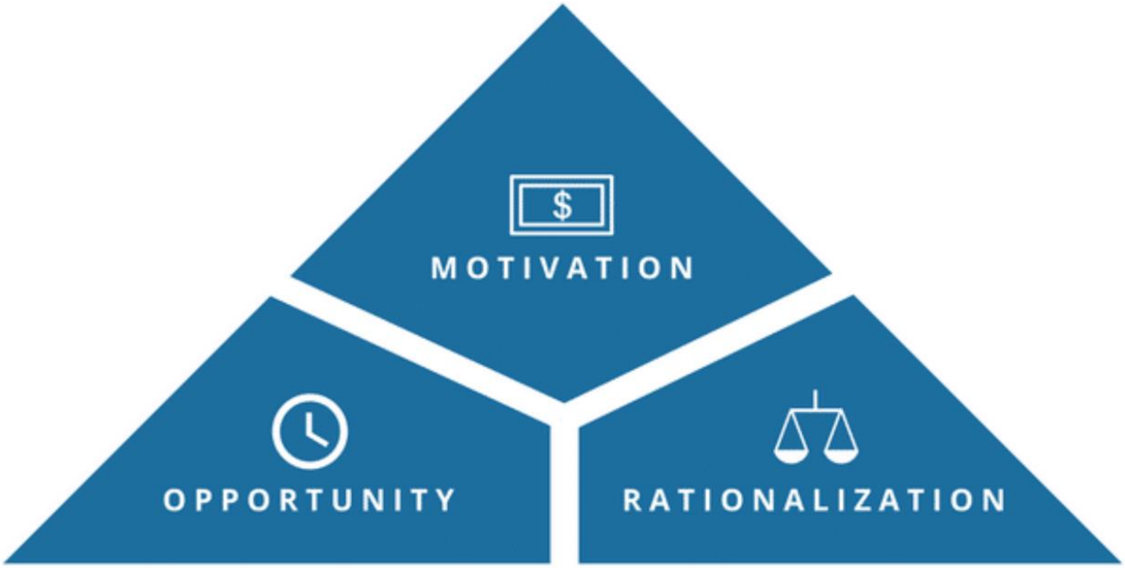
5. UNDERSTANDING FRAUD

Fraud refers to any deliberate false representation, including failure to declare information or abuse of position that is carried out for personal gain, cause loss, or expose another to the risk of loss. Fraud is used to describe acts such as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, and collusion, etc.

Generally, fraud involves the false representation of facts, whether by intentionally withholding important information or providing false statements to another party for the specific purpose of gaining something that may not have been provided without the deception. Depriving another person or the institution of a benefit to which he/she/it is entitled by using any of the means described above also constitutes fraud.

Fraud occurs because of a combination of opportunity, motivation, and rationalization. This is referred to as the Fraud Triangle Theory. The fraud triangle is a framework commonly used in auditing to explain the reason behind an individual's decision to commit fraud. The fraud triangle outlines three components that contribute to increasing the risk of fraud. See Chart 1 below:

Chart 1: Fraud Triangle



i. **Opportunity** refers to circumstances that allow fraud to occur;

ii. **Motivation** refers to an employee’s mindset towards committing fraud; and

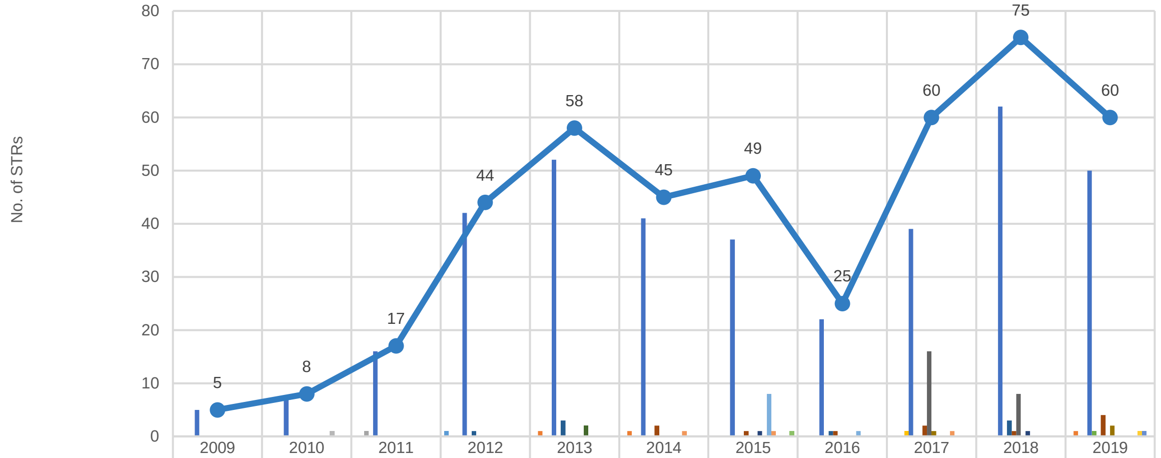
iii. **Rationalization** refers to an individual’s justification for committing fraud.

SECTION B

6. SUMMARY OF CASES AND STRs/SARs RELATED TO FRAUD REPORTED TO FIC

This section provides an overview of STRs/SARs/Cases[3] related to possible Fraud filed by AIs and RIs since the reporting obligation commenced in **2009** until **31 December 2019**. When reports are received by the FIC, they go through the cleansing stage whereby they are assessed to determine if they can be escalated for further investigations/analysis. If such is required, the reports are then turned into active cases for investigation/analysis. Further, the section presents total number of reports escalated to cases and the total disclosures made to Law Enforcement Agencies (LEA) associated with potential Fraud.

Chart 2: STRs received from Agency Business Type (Sectors) annually

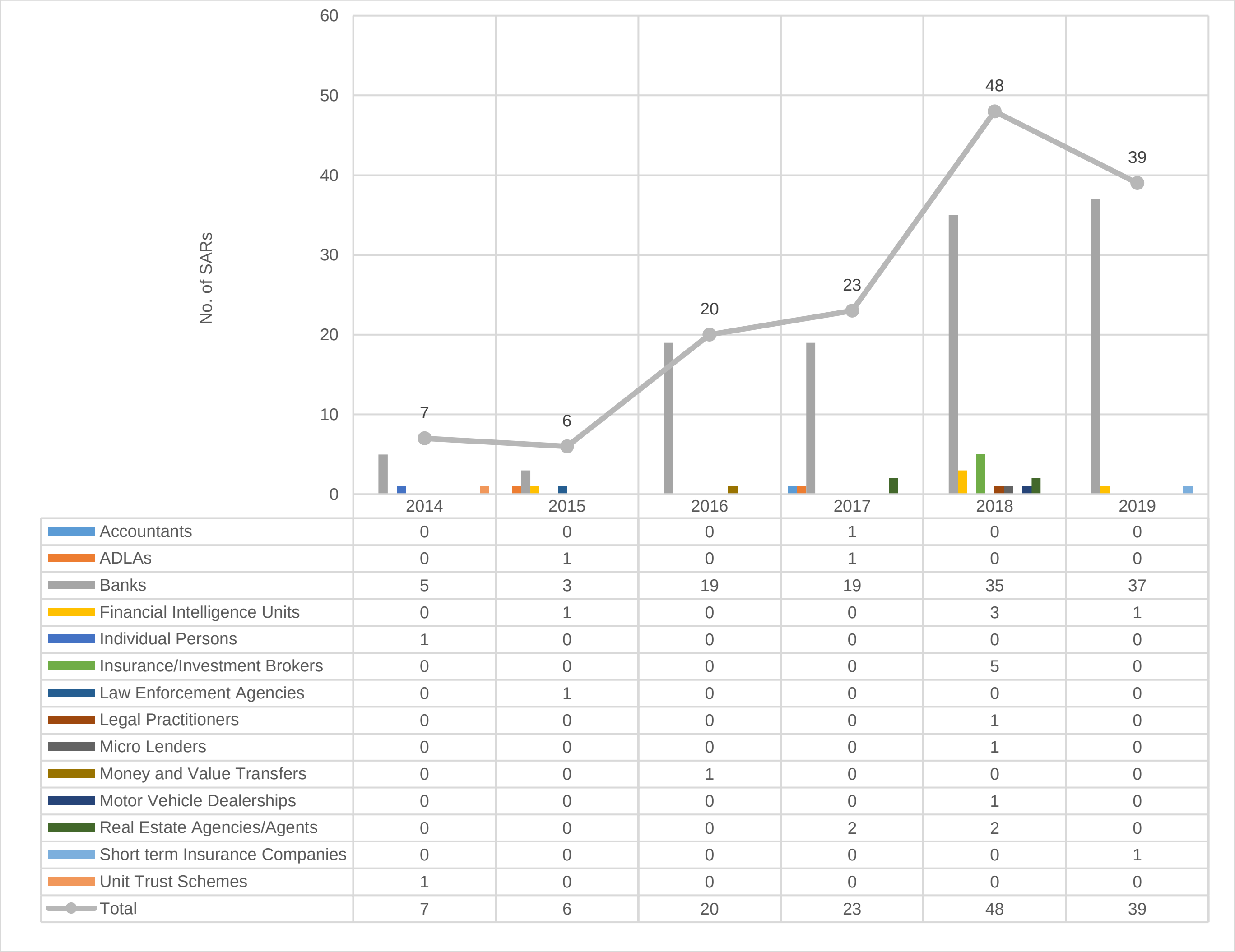


	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Accountants	0	0	0	1	0	0	0	0	0	0	0
ADLAs	0	0	0	0	1	1	0	0	0	0	1
Asset Management Companies	0	0	1	0	0	0	0	0	0	0	0
Auctioneers	0	0	0	0	0	0	0	0	1	0	0
Banks	5	7	16	42	52	41	37	22	39	62	50
Casinos	0	0	0	0	0	0	0	0	0	0	1
Financial Intelligence Units	0	0	0	1	3	0	0	1	0	3	0
Individual Persons	0	0	0	0	0	2	1	1	2	1	4
Insurance/Investment Brokers	0	0	0	0	0	0	0	0	16	8	0
Legal Practitioners	0	0	0	0	0	0	0	0	1	0	2
Lending Firms	0	0	0	0	0	0	1	0	0	1	0
Long Term Insurance Companies	0	0	0	0	2	0	0	0	0	0	0
Money and Value Transfers	0	0	0	0	0	0	8	1	0	0	0
Motor Vehicle Dealership	0	0	0	0	0	1	1	0	1	0	0
Regional Government	0	1	0	0	0	0	0	0	0	0	0
Short term Insurance	0	0	0	0	0	0	0	0	0	0	1
Trust and Loan Company	0	0	0	0	0	0	0	0	0	0	1
Unit Trust Schemes	0	0	0	0	0	0	1	0	0	0	0
Total	5	8	17	44	58	45	49	25	60	75	60

[3] Cases within FIC domain

The chart above presents a summary of STRs related to potential Fraud reports received from supervised entities. The general trend over the years reflects an increase in the volume of Fraud related reports reaching the FIC. Overall, as from the date the reporting obligations commenced until 31 December 2019, the FIC received a total of 446 such STRs. Whereby the highest volume of 75 STRs was received in 2018. The banking sector submitted the most reports during the period under review, filing 84% (or 373 reports) followed by the Insurance/Investment Brokers filling 5% (or 24 reports). The high number of reports filled by banking sector could be attributed to various factors, including the fact that the banks appear to have the most matured AML/CFT/CPF control systems (enhanced ability to detect and report). It can also be argued that banking services are generally exposed to a higher risk of abuse for Fraud as almost all other sectors make use of the banking systems.

Chart 3: SARs received from Agency Business Type (Sectors) annually



	2014	2015	2016	2017	2018	2019
Accountants	0	0	0	1	0	0
ADLAs	0	1	0	1	0	0
Banks	5	3	19	19	35	37
Financial Intelligence Units	0	1	0	0	3	1
Individual Persons	1	0	0	0	0	0
Insurance/Investment Brokers	0	0	0	0	5	0
Law Enforcement Agencies	0	1	0	0	0	0
Legal Practitioners	0	0	0	0	1	0
Micro Lenders	0	0	0	0	1	0
Money and Value Transfers	0	0	1	0	0	0
Motor Vehicle Dealerships	0	0	0	0	1	0
Real Estate Agencies/Agents	0	0	0	2	2	0
Short term Insurance Companies	0	0	0	0	0	1
Unit Trust Schemes	1	0	0	0	0	0
Total	7	6	20	23	48	39

The chart above shows the number of SARs filed by the reporting entities since the reporting obligation commenced until 31 December 2019. The FIC received a total of 143 such SARs whereby the highest number of SARs were received in the year 2018, a record high of 48 SARs. It further shows that the banking sector collectively submitted a total of 118 SARs, which represents 82% of the total reports, followed by Insurance/Investment Brokers and Financial Intelligence Units.

6.1 Level of prioritization of reports from AIs and RIs

The FIC applies a risk-based approach in determining the prioritization level to assign to reports received. Some reports that cannot be attended to immediately are accorded a “low priority” status. Amongst others, a report could be classified as low priority when the observed suspicion does not fall within law enforcement’s priority areas of investigation. At times, when the financial values involved are negligible (or insignificant) in comparison to amounts in other reports, this could also contribute towards a lower prioritization level. On the other hand, a report which meets certain requirements could eventually result in a case. Factors which collectively inform prioritization levels include, but are not limited to:

a. Strategic priorities of LEAs, which are informed by the risk areas identified in the National Risk Assessment (NRA);

b. Known ML, TF and/or PF indicators;

c. Various sanctions lists;

d. Prior reports on same subject/entity;

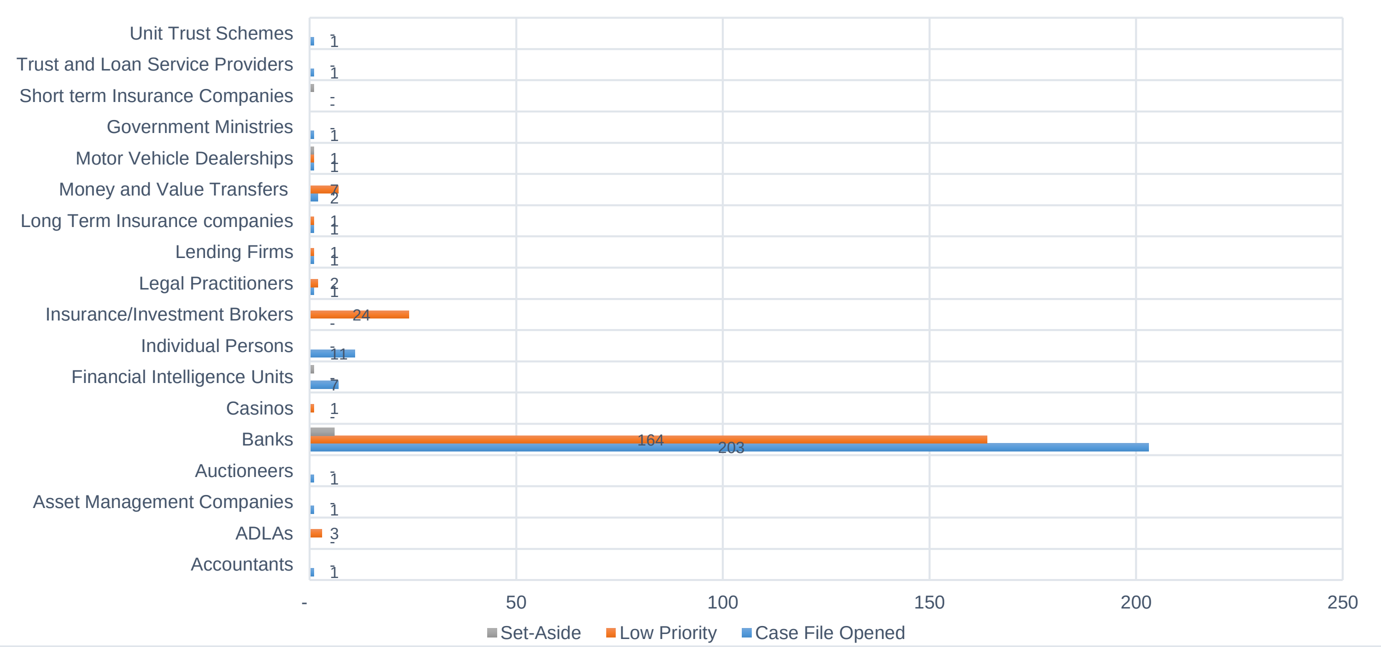
e. Geographic risk areas involved;

f. Duplicate/erroneous filing (which may lead to the STRs/SARs being set-aside);

g. Risk of funds being placed out of reach of law enforcement; and

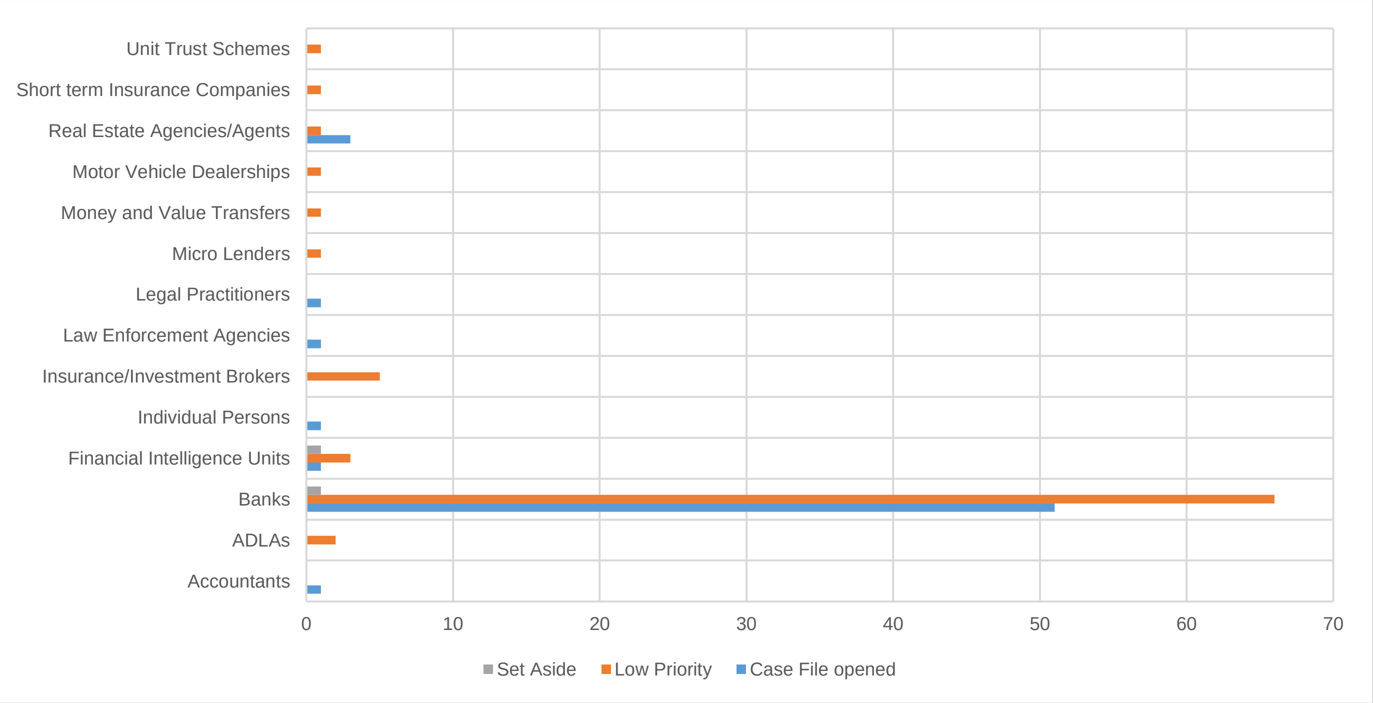
h. Human Resource constraints within FIC’s Financial Investigations and Analyses Division.

Chart 4: Classification of STRs received by Agency Business Type (Sectors)



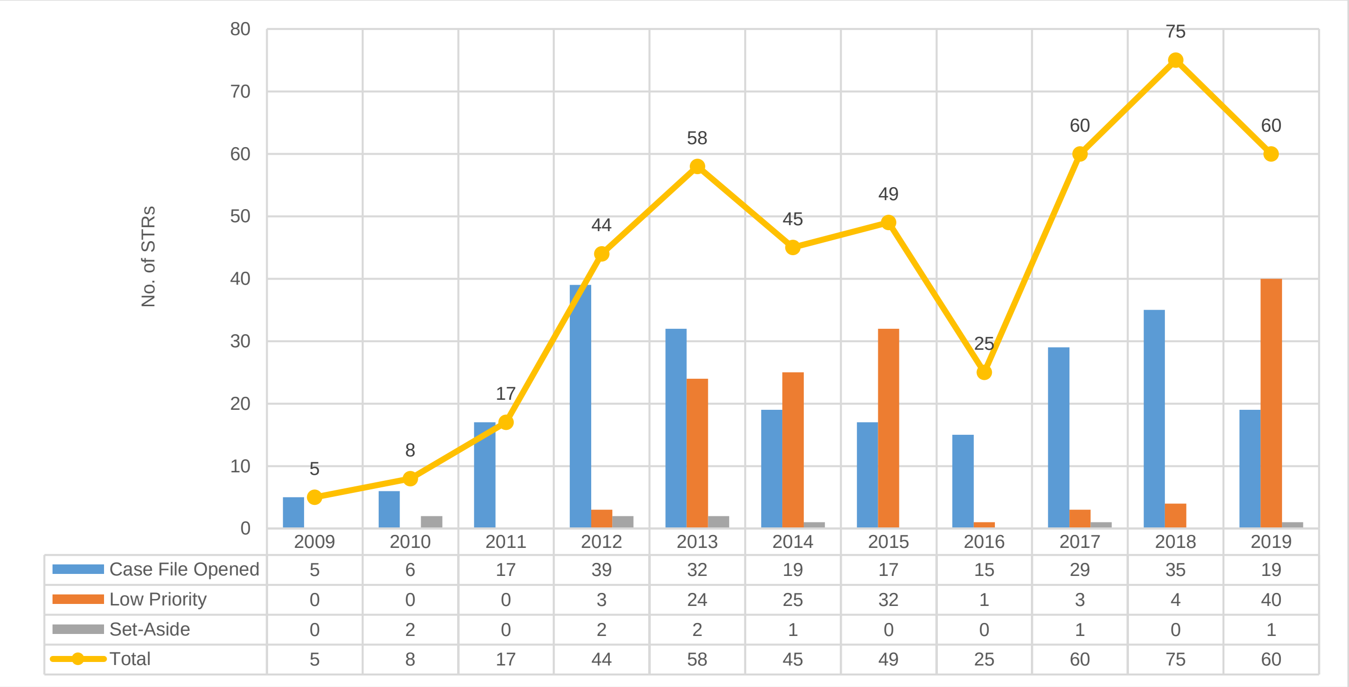
Overall, the FIC observed that 52% or 233 STRs were accorded "high priority" status and escalated for further analysis (case files opened) whilst a total number of 204 STRs (or 46%) were categorized as 'low priority'. It is worth noting that a total of 203 STRs (or 54%) from the banking sector has been escalated for further analysis.

Chart 5: Classification of SARs received by Agency Business Type (Sectors)



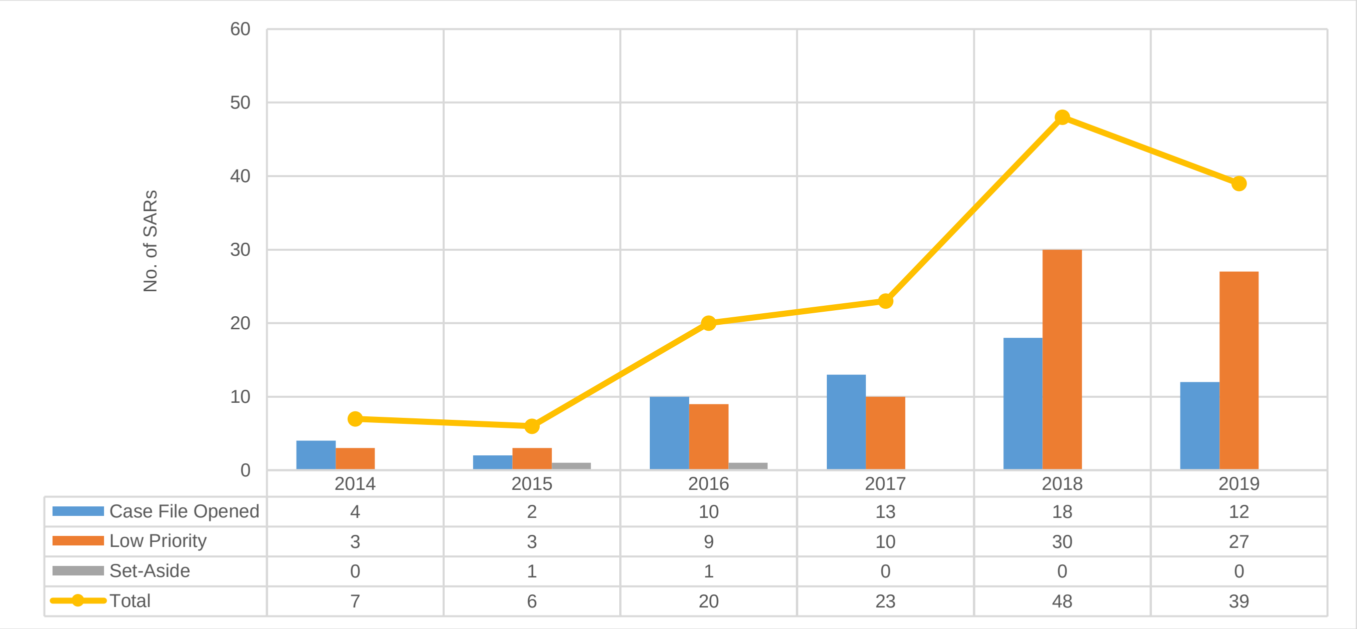
During the period under review, the Centre received a total of 143 fraud related SARs. Whereby 82 SARs (or 57%) were categorized as ‘low priority’, whilst 59 SARs (or 41%) were accorded high priority status and escalated for further analysis. The banks filed the majority of these reports a total of 118 SARs.

Chart 6: Categorization of STRs received per annum



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Case File Opened	5	6	17	39	32	19	17	15	29	35	19
Low Priority	0	0	0	3	24	25	32	1	3	4	40
Set-Aside	0	2	0	2	2	1	0	0	1	0	1
Total	5	8	17	44	58	45	49	25	60	75	60

Chart 7: Categorization of SARs received per annum



	2014	2015	2016	2017	2018	2019
Case File Opened	4	2	10	13	18	12
Low Priority	3	3	9	10	30	27
Set-Aside	0	1	1	0	0	0
Total	7	6	20	23	48	39

Chart 8: Categorization of STRs by Reporting Entities

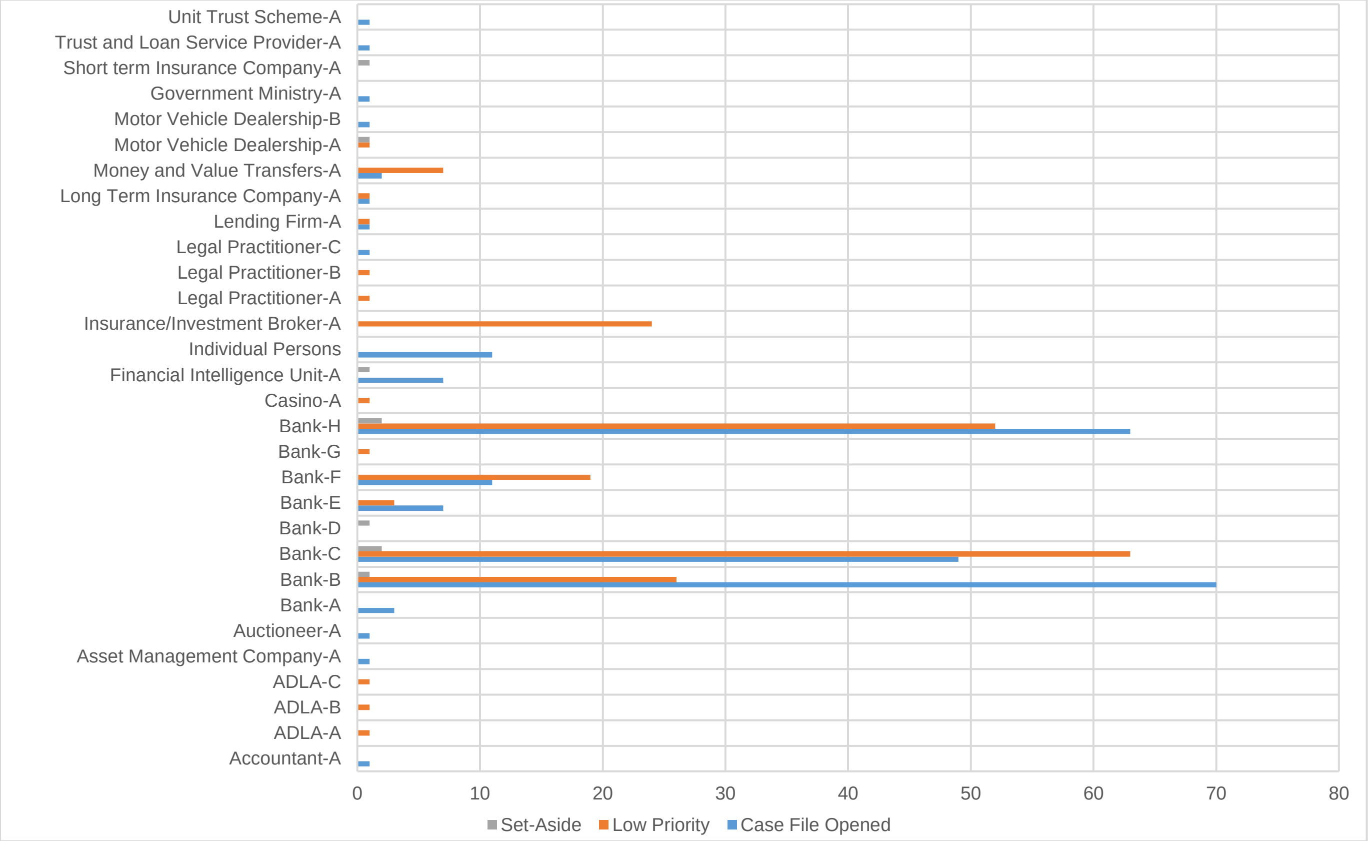


Chart 9: Categorization of SARs by Reporting Entities

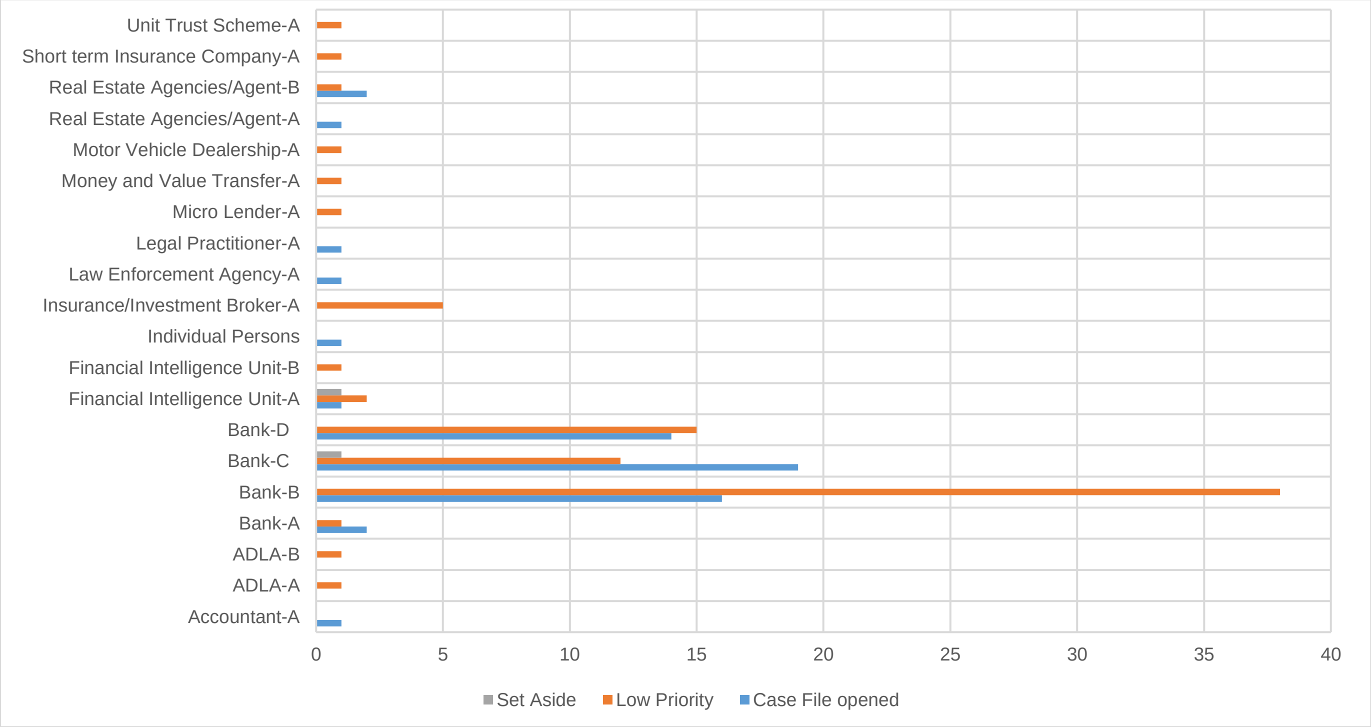
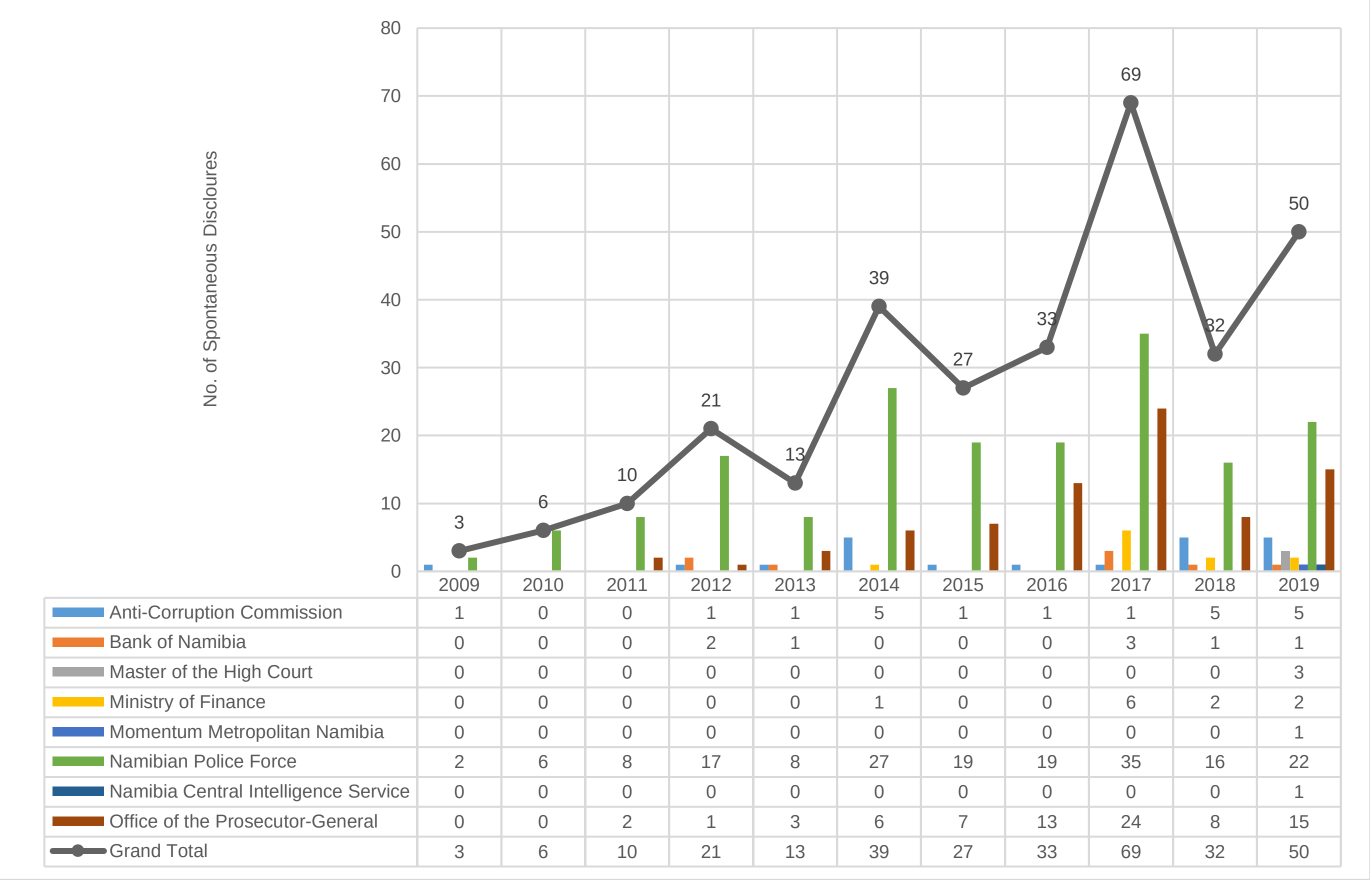


Chart 7 above shows that during the period under review, Bank-H filed the majority of STRs (a total of 117 STRs). This was followed by Bank-C and Bank-B, filing a total of 114 and 97 STRs respectively. Worth noting is that Bank-B filed the most STRs that were accorded ‘high priority’ status (a total of 70 STRs).

According to Chart 8 above Bank-B filed the majority of the SARs (a total of 54 SARs), followed by Bank-C and Bank-D in third place. Bank-C filed the majority of the SARs that were accorded high priority status (a total of 19 SARs)

Chart 9: Fraud related Spontaneous Disclosures disseminated to LEA’s per annum



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Anti-Corruption Commission	1	0	0	1	1	5	1	1	1	5	5
Bank of Namibia	0	0	0	2	1	0	0	0	3	1	1
Master of the High Court	0	0	0	0	0	0	0	0	0	0	3
Ministry of Finance	0	0	0	0	0	1	0	0	6	2	2
Momentum Metropolitan Namibia	0	0	0	0	0	0	0	0	0	0	1
Namibian Police Force	2	6	8	17	8	27	19	19	35	16	22
Namibia Central Intelligence Service	0	0	0	0	0	0	0	0	0	0	1
Office of the Prosecutor-General	0	0	2	1	3	6	7	13	24	8	15
Grand Total	3	6	10	21	13	39	27	33	69	32	50

During the period under review, the FIC disseminated 303 Spontaneous Disclosures (SDs) to Law Enforcement Agencies were Fraud featured as the potential predicate offense. The number of disclosures increased significantly over the years with a record low of 3 reports recorded in 2009, and a record high of 69 reports recorded in 2017. The Namibian police force received the highest number of such disclosures about 59% (or 179 SDs).

Table 1: Potential monetary values of Fraud related Spontaneous Disclosures disseminated to LEA's per annum in Millions NAD

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total
Anti-Corruption Commission	4.50	-	-	30.23	2.51	7.59	-	-	1.27	27.63	143.60	**217.32**
Bank of Namibia	-	-	-	1.50	1.58	-	-	-	224.87	-	-	**227.95**
Ministry of Finance	-	-	-	-	-	0.07	-	-	26.18	838.44	37.78	**902.46**
Momentum Metropolitan Namibia	-	-	-	-	-	-	-	-	-	-	16.61	**16.61**
Namibian Police Force	0.10	0.84	154.52	39.89	11.92	58.11	10.79	14.85	217.51	94.47	12.77	**615.77**
Office of the Prosecutor-General	-	-	-	-	20.38	2.19	57.05	17.74	46.76	33.31	1,110.77	**1,288.20**
Total	**4.60**	**0.84**	**154.52**	**71.61**	**36.39**	**67.96**	**67.84**	**32.59**	**516.59**	**993.84**	**1,321.53**	**3,268.31**

It is worth noting that the potential monetary values cited in the table above emanated only from the SDs that featured Fraud as the potential predicate offense. The potential monetary value of such SDs fluctuated over time since the reporting obligations commenced to 31 December 2019. The highest total potential monetary value of NAD 1,321,530,000.00 was recorded in 2019. Since inception, the total potential fraud monetary value of NAD 3,268,310,000.00 was recorded in SDs escalated to the LEA's.

SECTION C

7. TYPICAL REASONS FOR REPORTING TRANSACTIONS AS SUSPICIOUS

Reporting entities are expected to provide ‘grounds for suspicion’ when submitting STRs or SARs to the FIC. These grounds should reflect the offense or crime they suspect. The purpose for explaining why they find transactions or activities suspicious is to assist the FIC during analysis of such STRs. In the process of establishing such ‘grounds for suspicions’, institutions take into consideration various elements (red flags, modus operandi, indicators etc.) that collectively inform the formulation of a suspicious transaction or activity to be reported. Below are observations from typical case studies and a list of the prominent methods employed to advance fraud in the period under review:

Table 2: Potential indicators of Fraud from STRs/SARs

• Transactions inconsistent with customers’ financial profiles or behavioral patterns;
• The ownership structure of a company appears unusual or excessively complex given the nature of the business’ activities;
• 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;
• 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;
• Significant and unusual transactions involving foreign companies or nationals;
• Explanations for transactions may include the use of words and phrases often used as euphemisms for fraud (for example consultation fees, commission, marketing fees, surcharge, etc.);
• Client attempts to close an account(s) immediately upon receiving and withdrawing funds;
• Unusual cash withdrawals from government or public entity’s account;
• A pattern of sending or receiving international EFTs to or from foreign businesses that operate in sector or industry unrelated to each other;
• Frequent amendment of business account holders/owners;

• Transactional patterns from entity account which are exclusively one-directional. e.g., the entity only sends but never receives EFTs, or vice versa;
• 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;
• Employee making payments to suppliers that appear to be fictitious;
• 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
• Individuals transacting but appearing to be more concerned by the speed of transaction completion than the transaction cost or risk involved.
• a person suddenly starts living beyond her known income; and
• sudden change in her banking behavior/activities.
• frequent ATM withdrawals and strictly no in branch-withdrawals to avoid detection;
• Refusal to take vacations
• Control issues, unwillingness to share duties
• Subjects running Pyramid and Ponzi schemes
• Subject presenting fraudulent documents
• Identity theft to gain access to the victims online banking account
• Banking card cloning
• Employee abusing the funds for their own gains, making payments without proper authorization;

SECTION D

8. 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. The below are sampled case studies to help understand certain common or notable trends from reports analyzed.

Case Study 1: Employee Fraud

Person-A *is employed as an accountant at* ***Company-X****, a position he held for many years. His duties involve issuing and facilitating payments for the company. Person-A developed a strategy to defraud his employer by registering several close corporations to which he has 100% ownership. He then approached a couple of local banks and opened several bank accounts under the names of the entities, to which he had sole signatory rights. Furthermore, he also has personal bank accounts with four different commercial banks in Namibia. He used his position to fabricate fictitious invoices for "catering services rendered" to* ***Company-X****, purportedly by his entities. He then processes and facilitates electronic payments to the "service providers". Person-A lives an extravagant lifestyle.*

The flow of regular and significant flow of funds was discovered amongst Person-A personal accounts. The funds were transferred from several close corporation's bank accounts that he owns. The funds were normally disbursed through cash withdrawals, internet banking payments, and point of sales. It was spent to sustain his high-end lifestyle, i.e. cash purchases of high-value items including livestock, vehicles, household items and entertainment. To avoid detection by banks, ***Person-A*** *would create payment description that appears business-like when moving funds from one account to another to suits the principal business of the entities involved.*

Law enforcement arrested the suspects. The charge raised is Fraud/ Alternative theft. Three vehicles and a large cash amount were forfeited to the state.

Report source type	**STR**
Perpetrators/Involved	Individuals and entities
Involved sector	Banking
Key risk controls	Amongst others, poor payment authorization and verification controls; Failure to conduct beneficial ownership identification; Poor customer due diligence controls; failure to reconcile transacting behavior to account beneficiary/owner.
Designated services	Personal and business bank accounts
Instruments used	EFTs, banks accounts etc.
Offence	Fraud/Alternative theft.

Red flags

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

Case Study 2: Card Cloning

The Centre received several reports of card cloning through fake tourist bookings. The perpetrators were in possession of cloned credit card details belonging to various individuals in foreign jurisdictions. The perpetrators claiming to be a booking agent for the tourist's advanced booking intentions with the targeted Namibian lodge.

***Lodge-Y** is a Namibian registered enterprise, whose main business activities include the provision of Lodging and camping facilities. The lodge received the booking requests from the alleged booking agent (perpetrators) from overseas. The lodge then complied and honour the booking requests as well as initiate necessary charges by processing the cloned credit card information provided for tour and accommodation purposes. Upon successful receipt, the perpetrators cancel the booking and request to be refunded. However, the perpetrators request that the refunds are then transferred back to another recipient account instead of the accounts that made the initial payments.*

This scam cost the used commercial bank over NAD3 million as a result of making unauthorized payments from the bank account of actual cardholders. As most of the funds were paid and immediately transferred from jurisdictions to jurisdictions in an effort to frustrate any tracking efforts.

Report source type	**STR**
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	Electronic Fund transfers, Point of Sale (PoS) and Bank Accounts
Offence	Fraud

Red flags

- *Spontaneous disclosure of a list of credit card information by a third party;*
- *Immediate booking cancellation upon processing of the information;*
- *Request to refund the funds to a different account from the one that made the payment;*

9. CONCLUSION

The information contained in this report is essentially intended to provide a general overview of analysis to stakeholders with regard to typologies related to potential fraud offences within the relevant sectors, as derived from the reports within the FIC domain. It is hoped that the information contained herein is helpful in guiding other related supervision activities in the AML/CFT/CPF space.

It is therefore essential that reports of such nature submitted to the FIC are relevant, timely and meet quality expectations. The examples of indicators highlighted herein are not complete. It is the FIC's view that when considered as a whole, effective measures can be implemented by various institutions charged with combatting laundering activities. The use of indicators individually or in isolation is not ideal as they need to be used with other relevant considerations. Also, such indicators are not intended to be comprehensive, and although they are considered to be helpful, they may not be relevant in all circumstances.

The FIC appreciates relevant institutions' continuous efforts geared towards ensuring that they continuously contribute to ML/TF/PF prevention and combatting. It is equally worth noting that reporting behavior of sectors reflects the effectiveness of controls in such sectors and the level of compliance with the provisions of the FIA. Such reporting impacts overall combatting efforts. Whilst encouraging the volumes of reports, it is important to enhance an appreciation for reporting quality or value-adding STRs/SARs which can lead to effective investigations, prosecutions, asset forfeitures and asset/tax recoveries etc.

This report or similar studies on potential fraud-related offences will be updated periodically when the need arises

P.P K

L. DUNN

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE