



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

CORRUPTION AND MONEY LAUNDERING TYPOLOGY REPORT

JULY 2021

TABLE OF CONTENTS

1. DEFINITIONS.....	3
SECTION A	4
2. EXECUTIVE SUMMARY	4
3. OBJECTIVES OF THIS REPORT.....	4
4. METHODOLOGY	5
5. UNDERSTANDING CORRUPTION.....	5
SECTION B	7
6. SUMMARY OF CASES AND STRs/SARs RELATED TO CORRUPTION REPORTED TO FIC	7
Chart 1: STRs received from Agency Business Types (Sectors) annually.....	8
Chart 2: Classification of STRs received by Agency Business Types (Sectors)	9
5.1 Level of prioritization of reports from AIs and RIs	9
Chart 3: Spontaneous Disclosures to the Anti-Corruption Commission (ACC)	10
Chart 4: Potential corruption related monetary values per annum	11
SECTION C	12
7. MOST COMMON IDENTIFIABLE POTENTIAL CORRUPTION INDICATORS	12
7.1 Potential indicators from cases under FIC domain and general potential indicators	12
7.2 Unexplained wealth or income	15
7.3 Corruption in public procurement	16
SECTION D	17
8. SAMPLED CASE STUDIES	17
Case Study 1: Potential corruption and bribery	17
Case Study 2: Potential employee fraud, corruption and theft.....	19
Case Study 3: Potential fraud/forgery and corruption	21
Case Study 4: Potential fraudulent and corruption	23
9. CONCLUSION.....	24

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; 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.”

¹ FATF Recommendation 7

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, corruption 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 corruption identified in cases within the domain of the FIC. It is hoped that this report will help enhance sectoral understanding of corrupt practices and result in the implementation of enhanced control measures within the sectors.

3. OBJECTIVES OF THIS REPORT

The objectives of this typology report are to:

- a) highlight the nature and level of corruption 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 corruption;

- c) enhance understanding of the *modus operandi* employed by corrupt 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 corruption.

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 corruption which potentially leads to ML/TF/PF activities. The information contained in this report was derived from STRs/SARs data filed with the FIC by various AIs and RIs.

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

- i. Sanitised 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. UNDERSTANDING CORRUPTION

Generally, corruption can be defined as the abuse of position, standing or advantage to undermine legitimate public (or general social) interests for the illicit benefit of a few or participants in such acts. In other words, a public officer commits an offence through, directly or indirectly, corruptly uses his or her office or position in a public body to obtain

any gratification, whether for the benefit of himself or herself or any other person².

Corruption often takes many forms and perpetrators continue to develop innovative ways to advance their corrupt activities. Generally, corruption can be said to take the following forms:

- **Bribery:** constitutes a crime and is defined as soliciting of any item of value to influence the actions of an official or other person in charge of a private or public legal duty;
- **Kickback:** is a form of negotiated bribery in which a commission is paid to the bribe-taker as an agreement for services/favors rendered. The remuneration (such as money, goods or services handed over) is usually agreed tacitly or otherwise. The purpose of the kickback is usually to encourage (coerce) the other party to cooperate in the illegal scheme;
- **Illegal gratuities:** These are items of value given to reward a decision after it has been made. The gift is usually made as a token of appreciation for something that has been done; and
- **Collusion:** An agreement between two or more individuals to commit an act designed to deceive or gain an unfair advantage.³

²Anti-Corruption Act 8 of 2003;

³ <https://www.icpak.com/wp-content/uploads/2015/09/Procurement-Fraud-and-Corruption.pdf>.

SECTION B

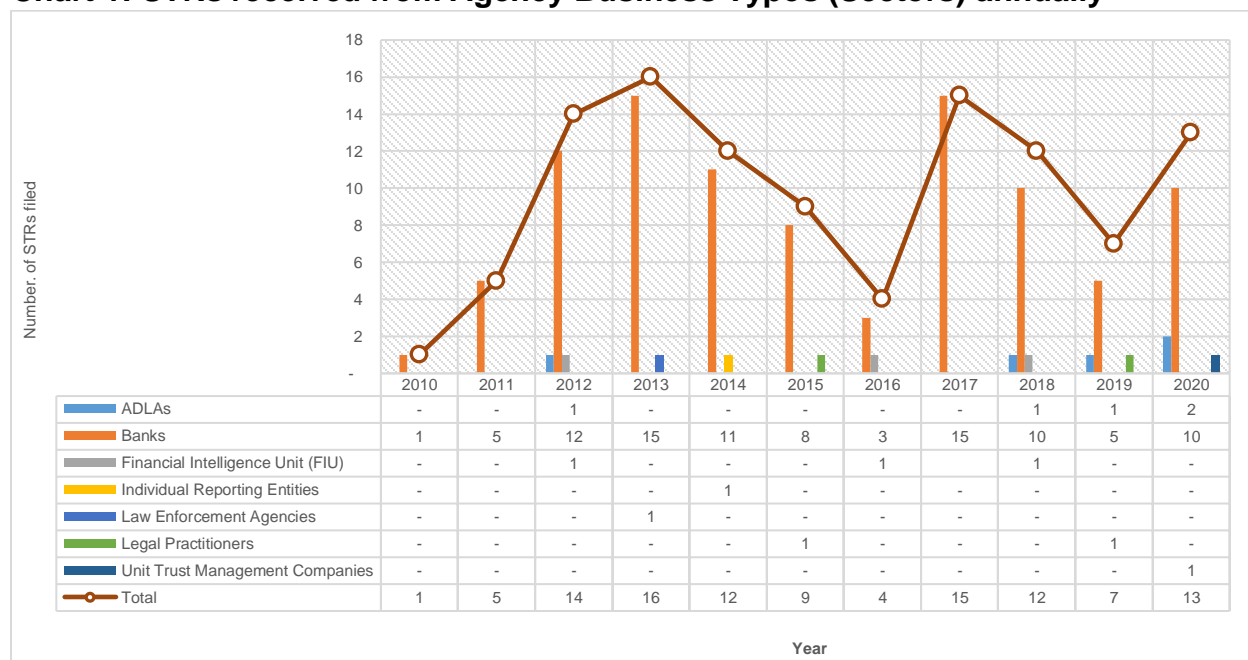
6. SUMMARY OF CASES AND STRs/SARs RELATED TO CORRUPTION REPORTED TO FIC

It is essential for combatting agencies and authorities to fully understand pressures and threats posed by this type of criminal activity in order to effectively prevent the predicate offences and related laundering activities.

This section provides an overview of STRs/cases⁴ related to possible corruption filed by AIs and RIs since the reporting obligation commenced in 2009 until **31 December 2020**. 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. Further, the section presents total number of reports escalated to cases and the total disclosures made to Law Enforcement Agencies (LEA) associated with potential corruption.

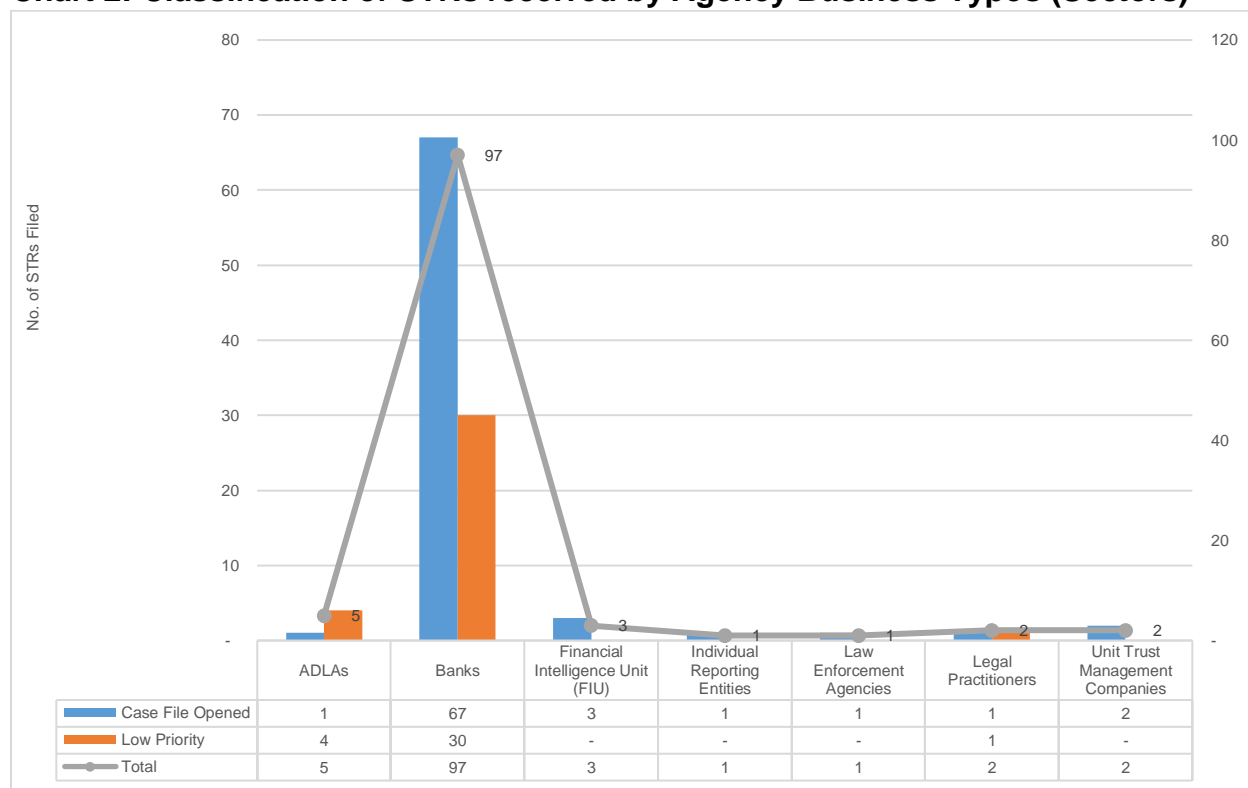
⁴ Cases within FIC domain

Chart 1: STRs received from Agency Business Types (Sectors) annually



The chart above presents a summary of STRs related to potential corruption reports received from supervised entities. The general trend over the years reflects an increase in the volume of corruption related reports reaching the FIC and being escalated to the relevant authorities. As from the date the reporting obligations commenced until 31 December 2020, the FIC received a total of 111 STRs. Such is characterized by the lowest reports of 3 STRs in 2009, to the highest number of 16 STRs in 2013 before it started levelling off in 2014. The year 2013 and 2017 saw the highest volume of reports in potential corruption offences with 16 and 15 STRs, respectively. It is worth noting that a total of 97 STRs or 87% 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 corruption as almost all other sectors make use of the banking systems.

Chart 2: Classification of STRs received by Agency Business Types (Sectors)



Overall, the FIC observed that 68% or 76 STRs were accorded “high priority” status and escalated for further analysis (case files opened) whilst a total number of 35 STRs (or 32%) were categorized as ‘low priority’. It is worth noting that a total of 67 STRs from the banking sector has been escalated for further analysis.

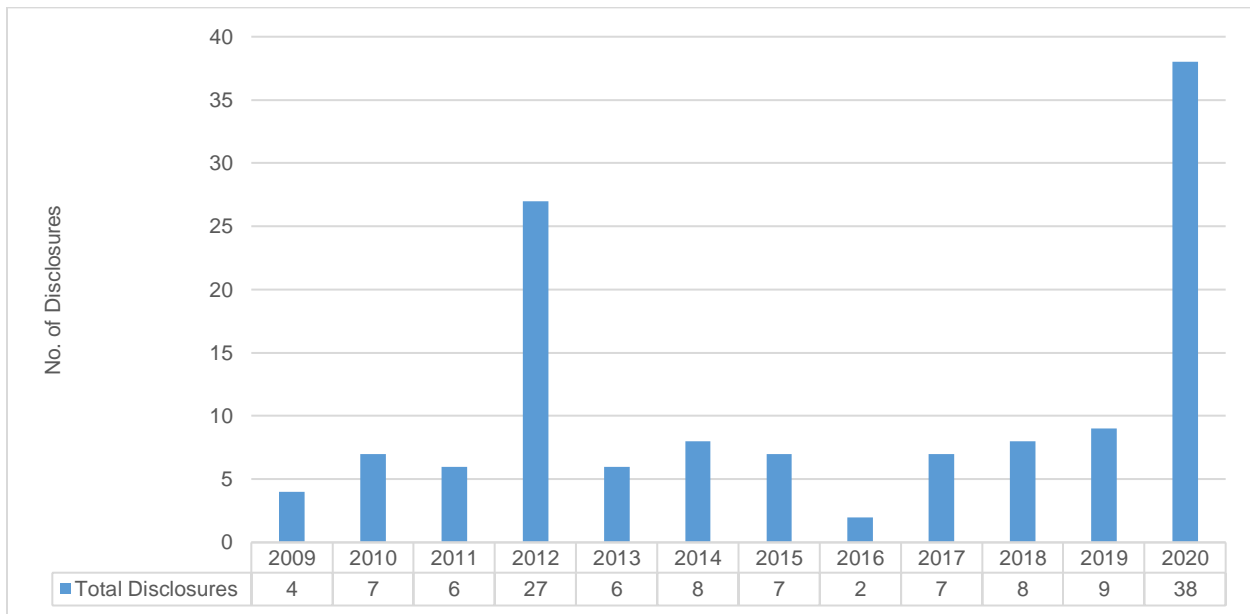
5.1 Level of prioritization of reports from AIs and RIs

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:

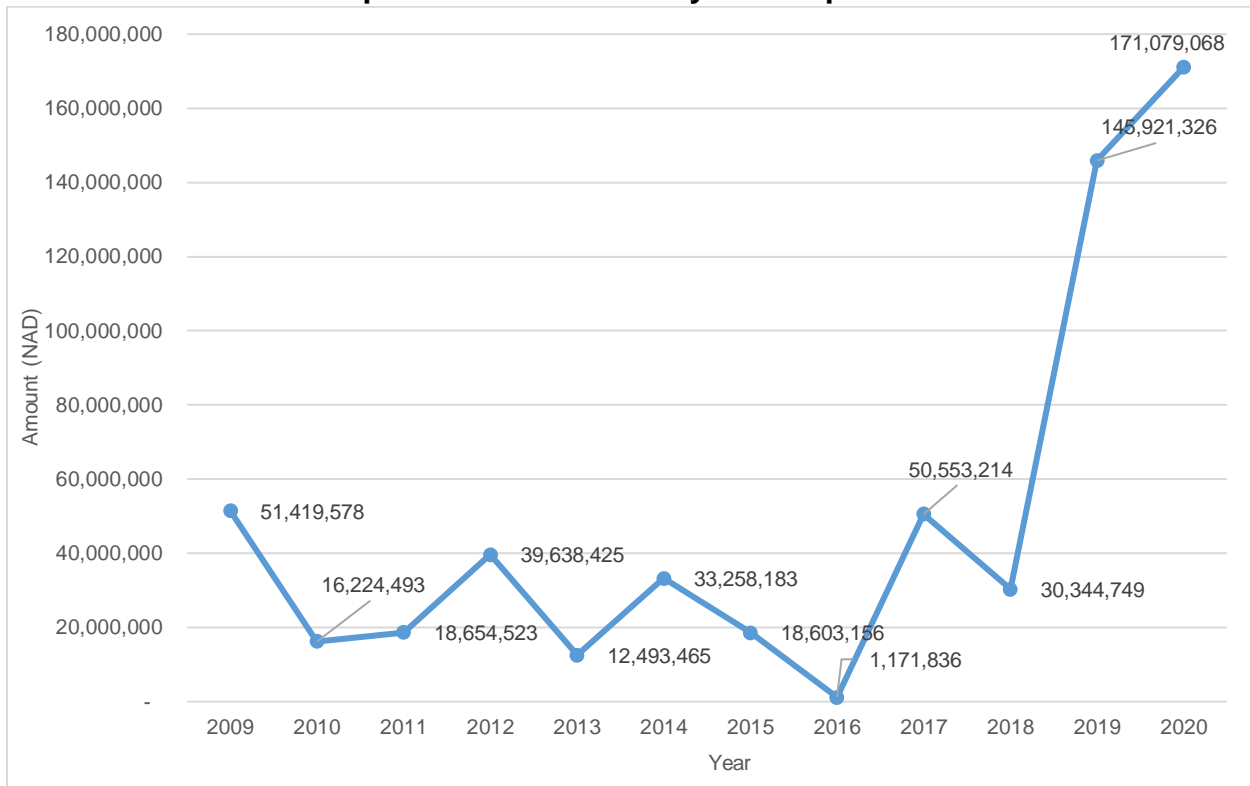
- a. Strategic priorities of LEAs, which are informed by the risk areas identified in the National Risk Assessment (NRA);
- b. Known ML, TF and/or PF indicators;
- c. Watch lists [Politically Exposed Persons (PEPs) and various sanctions lists];
- d. Prior reports on same subject/entity;
- e. Geographic 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 3: Spontaneous Disclosures to the Anti-Corruption Commission (ACC)



During the period under review, the FIC disseminated 129 Spontaneous Disclosures (SDs) to the Anti-Corruption Commission (ACC). The number of disclosures increased significantly from lowest of 4 reports in 2009, to the highest number of 38 reports in 2020. The lowest total number of reports (2) related to corruption was observed in 2016.

Chart 4: Potential corruption related monetary values per annum



It is worth noting that the potential monetary values cited above (Chart-4) emanated only from the SDs that were analyzed by the FIC and disseminated to ACC. The potential monetary value of corruption fluctuated over time since the reporting obligations commenced to 31 December 2020. The highest total potential monetary value of NAD 171,079,068.00 was recorded in 2020. Since inception, the total potential corruption monetary value of NAD 589,362,016.00 was recorded in SDs escalated to the ACC.

SECTION C

7. MOST COMMON IDENTIFIABLE POTENTIAL CORRUPTION INDICATORS

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

7.1 Potential indicators from cases under FIC domain and general potential indicators

Corruption is a predicate offence for Money Laundering. The two cannot be separated. For supervised institutions to be in a position to identify corrupt 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 corruption indicators. When each indicator is viewed in isolation, it may not readily point to potential corrupt behavior but when viewed with other indicators and relevant factors, it may highlight presence of potential corrupt practices. It is worth noting that these serve merely as a guide and therefore not exhaustive of all indicators:

Table 1: 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 dormant or inactive bank account; Significant and unusual transactions involving non-profit organizations; 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;

		<ul style="list-style-type: none"> • The subject is under investigation for potential crimes by other Law Enforcement Agencies; • An employee misappropriating investors' funds or defrauding his/her employer; • 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 apparent purpose and that are inconsistent with the client's known occupation, employment or income; • 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 citizen 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 working with managements 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 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 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 into the insurance contract and later claiming that the items added were stolen; •

Pension Fund Administrators	Potential Fraud /Corruption	<ul style="list-style-type: none"> Employee 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 constantly depositing huge amounts of money into a minor's investment plan.
	Unknown/ Potential Corruption	<ul style="list-style-type: none"> 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 fund is for entity's operations/capital or individual's benefits.

Table 2: General potential indicators of corruption

<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"> Entity which 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 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 account which are exclusively one-directional. e.g., the entity only sends but never receives EFTs, or vice versa;
<ul style="list-style-type: none"> Employee 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"> 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.

7.2 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 3: Potential indicators of unexplained wealth or income

- Representative of a public official (i.e. lawyer, secretary, accountant) opens account and purchases expensive property or luxury goods with the express intent of enabling client/public official to bypass Customer Due Diligence (CDD) processes;
- 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');
- 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;
- 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;
- Public officials receive debt relief or repayment requirements are waived by the creditor;
- 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 front man, a strawman, or legal entity established to conceal the beneficial ownership);
- Transactions that take place in accounts of public officials involving cash deposits or withdrawals in unusual frequency and amounts;
- Private or public officials receive loan guarantees from a public corporation or government body, or a loan under favorable conditions;
- 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;
- Payments by entities to Non-Profit Organizations that public officials are known to be associated with;
- 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;
- 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;
- Purchases or leases of movable or immovable assets by public officials which are not in line with the client's income;

- 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;
- Payments in favor of public officials are made to facilitate or expedite a government service;
- Public officials making cash transactions involving large amounts (e.g. currency exchange, use of cash to purchase high value goods, etc.); and
- Transaction payments of unusual amounts or frequency from public officials to lawyers, accountants, or other professional intermediaries.

7.3 Corruption in public procurement

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

Table 4: Indicators of corruption in public procurement

- Subcontractors have common director(s), beneficial owner(s) and/or are related/associated to the management of the contractor;
- 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;
- 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;
- 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;
- EFTs from public entity being cashed out and subsequently deposited or transferred to accounts of public officials or entities related to public officials;
- Funds received by a contractor of public procurements are not spent within a reasonable timeframe to fulfil the contract needs;
- 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;
- Payments based on a public procurement contract are conducted at a price higher than originally contracted;
- Services provided to state-owned companies or public institutions by companies registered in high-risk jurisdictions; and
- Receipt of commission or fees before signing of agreement for services or carrying out a function or process in relation to public procurement contract.

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: 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 business-person may have instructed **Person-C** from **Legal Practitioner-TG** (Firm) to assist them with channeling funds to certain interest including election campaigns of a certain party and other supposed interests of government.*

*Due to the fact that **Person-A** was a high-ranking office bearer in the government and **Person-H** being a known and established businessman, the law firm apparently bona fide accepted instructions henceforth. It is claimed that at the time, the **Legal practitioner-TG** had no reason to be suspicious of 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 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 a sole signatory on 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 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 as 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 shows 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. Law firm 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 ot its transacting behaviour;
-  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 farly new and received significnat 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 analysis and discovered 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 principle business of the entities involved.

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

Report source type	RFI; 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 transfers 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 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 behaviour/activities).*

Case Study 3: Potential fraud/forgery and corruption

*An STR was reported relating to a suspicious number of payouts from a **Retirement Fund (Company-X)**. The retirement fund was administered by a **Long-Term Insurance Company-G**. It appeared that a senior employee (**Person-X**) employed at **Company-X** has been defrauding the company. The preliminary investigations reveal that she defrauded the company by completing claim forms and forging signatures of members of the **Retirement Fund**.*







*This came to light when **Person-Y**, one of the members of the Retirement Fund called to inquire about the benefit available to him under the pension fund. He was told that the payout (all his benefits) had already been affected, however, he denied having submitted claims to that respect. Subsequently, other members of the fund also made similar inquiries. It was then discovered that several other claims had been made and their benefits had been paid out unknowingly. These individuals' beneficiaries denied having submitted any claims. It was reported that **Person-X** had transferred a **significant amount** into his insurance policy account. The sources of such funds were unknown.*

Analysis revealed that these claims were processed by the **Long-Term Insurance service provider** and several payments were made as authorized by the **Retirement Fund**. It appears that the claim forms and authorizations were improperly completed and/or forged. A consequent reconciliation between the names on the claim forms submitted and the bank accounts to which payments were affected revealed that the names on the claim forms did not match the names of the account holders.

There is therefore a suspicion of fraud, forgery, corruption, and irregular authorization of claims in the approval of pension benefit payouts by the **Retirement Fund**. A report was disseminated to relevant Law Enforcement and investigations are currently underway for fraud, forgery, corruption, and money laundering.

Report source type	STR
Key	Senior employee defrauded employer
Perpetrators/Involved	Individuals/Namibian
Involved sector	Long Term Insurance, banking services
Key risk controls	Amongst others, poor claim authorization and verification controls; failure to reconcile claim names and bank beneficiary accounts etc.
Designated services	Pension benefit
Instruments used	Retirement fund products, Bank transfers
Offence	Fraud/forgery and Money laundering

Red flags

-  *Subject transferred significant funds into his insurance policy account;*
-  *The source of such funds was unknown;*
-  *Subject completed claim forms and forged signatures of the beneficiaries;*
-  *The beneficiary’s pay-out (benefits) has been affected unknowingly;*
-  *No claim forms were given to the beneficiaries for their signatures and submission;*
-  *The claim forms and authorizations were improperly completed and/or forged; and*



The names on the claim forms did not match the names of the account holders.

Case Study 4: Potential fraudulent and corruption

The FIC analysed a report pertaining to suspicious state account fraudulent cheques. It is reported that a non-transferable state account cheque to the value of **NAD 60 000**, in the beneficiary name of **entity-AJ** was deposited into the account of **Person-A**. This account was held at a local bank (**Bank-G**). Upon cheque deposit, it was processed following an authorization to process same by the Branch Controller (**Person-B**) who is related to **Person-A**.

Person-A is employed as an **Accountant** at one of the government ministries. **Entity-AJ** is registered in the name of **Person-C**, who is a brother to **Person-B**. Upon analysis, the FIC has further noted non-transferable cheques in the beneficiary name of **entity-DD** that have been deposited in the same account of **Person-A**.






As such, internal investigations within the ministry indicate that certain circumstances surrounding these transactions are not in line with the internal procurement/payment rules and procedures. Such internal investigations have resulted in disciplinary measures against some of the staff members of the said Ministry. The analysis further revealed that fraudulent cheque deposits in excess of **NAD 1.8 million** and electronic funds transfers (EFTs) of about **NAD 70 000.00** were paid into the account of **Person-A**, within a period of one year and subsequently, followed by EFTs, cash withdrawals and PoS transactions.

A report was disseminated to relevant Law Enforcement and investigations were conducted.

Report source type	STR
Key	Namibian nationals defrauding Public Institution
Perpetrators/Involved	Individuals/Namibian and entities
Involved sector	Banking

Key risk controls	Amongst others, poor payment authorization and verification controls; failure to reconcile bank beneficiary accounts. Failure to detect questionable bank transactional behaviors which conflicted nature of supposed business activities
Designated services	Personal Bank accounts
Instruments used	cheques deposits, EFTs, ATMs and PoS services
Offence	tax crime, fraud, and corruption.

Red flags

-  *significant cash deposits made by individuals into their personal bank accounts;*
-  *a cheque, in the beneficiary name of entities being deposited into personal account;*
-  *cheques deposited being authorised and processed by relatives of those involved in fraudulent schemes;*
-  *frequent cash withdrawals and PoS transactions subsequent to fund deposits; and*
-  *significant inflow of funds within a short period of time.*

9. CONCLUSION

Corruption erodes trust in private/government institutions, diverts resources away from important initiatives and affects the delivery of significant services in various sectors. Generally, like other crimes, corruption is motivated by profit and greed.

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 reflect 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. It is equally worth stating that the reporting patterns are inconsistent in the sectoral reporting behavior with some of the institutions not filing any reports over the period under review. Hence, accountable and reporting institutions are encouraged to continuously ensure that interventions are timely made to enhance general FIA compliance.

This report or similar studies on potential corruption will be updated periodically when the need arises.

A handwritten signature in black ink, appearing to read "P.P. K. [unclear]". The signature is written in a cursive style.

L. DUNN
DIRECTOR: FINANCIAL INTELLIGENCE CENTRE