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

TERRORIST FINANCING AWARENESS REPORT

MAY 2023

TABLE OF CONTENTS

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 actually used for such purpose or to carry out such acts";

Law Enforcement Authorities (LEAs): Refers to law enforcement bodies like the Namibian Police;

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;

Mutual Evaluation (ME): refers to the Mutual Evaluation Report of Namibia, carried out by ESAAMLG with the report being adopted in September 2022; and

[1] FATF Recommendation 7

Vulnerabilities: When considered in a risk assessment context, this term comprises of those control weaknesses that can be exploited by threats to advance or facilitate ML, TF or PF activities.

2. INTRODUCTION

This report serves to identify and highlight threats and vulnerabilities of Money Laundering, Terrorism and Proliferation Financing (ML/TF/PF) within the operations and services accountable and reporting institutions (AIs and RIs). Equally, the report contributes to the emphasis on specified None-Profit Organisations (NPOs) which are most vulnerable to TF abuse. It is hoped that the observations herein can aid specified sectors in implementing relevant controls and place competent authorities and law enforcement agencies in positions to enhance supervisory interventions, investigations and relevant combatting activities, as per the FIA[2], PACOTPAA[3], FATF Recommendation 8, amongst other legal instruments.

The 2023 National Risk Assessment (NRA) update (to the 2020 NRA) indicates that Close Corporations (CCs) are most vulnerable to ML and TF abuse. This trend is evident in this report, with regards to overwhelming findings which suggests CCs as the most preferred vehicles employed in advancement of TF. The various risk assessments over the years have also found that Faith Based Organisations (FBOs) in general and those associated with Islamic extremism present the highest risk of potential TF in Namibia.

This report shows that although the FIC has received many reports from the sectors suggesting potential TF, many such reports were deemed 'false positives' after FIC investigations. Overall, the FIC has only escalated two intelligence reports to LEAs that had indications of potential TF. These are the two referrals that had contributed to the known potential TF cases in Namibia over the years. The high volumes of reports on TF herein and related information should thus be viewed within this context. This report equally obtained information from the Namibian Police (NamPol) on the two TF cases investigated and such are also duly considered herein. Note that the names of subjects herein have been changed for obvious reasons.

3. OBJECTIVES OF THIS REPORT

The objectives of this typology report are to:

a. identify specific types of transactions in which AIs and RIs may have been knowingly or unknowingly involved in TF;
b. identify specific products, services and delivery channels that may be vulnerable to TF;

[2] Financial Intelligence Act of 2012
[3] Prevention and Combatting of Terrorist and Proliferation Activities Act of 2014

c. rank the products, services and delivery channels in terms of their vulnerability to TF risks;
a. contribute to grounds that inform FIA Compliance Supervision and Monitoring activities in terms of the risk-based approach, including taking proactive mitigation and corrective measures for areas identified as vulnerable to TF;
b. highlight red flags or indicators that may assist in identifying and combatting TF threats; and
c. enhance understanding of the *modus operandi* employed by TF perpetrators in the sectors.

3.1 TF RELATED FINDINGS: MUTUAL EVALUATION

The report also responds to key TF observations in Namibia's Mutual Evaluation Report (MER) adopted in September 2022, particularly on Immediate Outcomes (IOs) 9 and 10. The MER, amongst others, raised the following:

a. **TF cases are not proactively/routinely identified and investigated:** There are no attempts to do such as LEAs and the FIC appears to not have measures in place to readily identify TF threats proactively. Authorities appear to only wait for reports on potential TF activities and react to such;

   The below, as noted from the MER, partly explains why LEAs are said to be understaffed to duly combat TF:

   Inadequate capacity: *The authorities mandated to investigate and prosecute TF appears to have an inadequate ability to identify and investigate TF cases even in clear instances where TF is manifested. The AML/CFT Division under Namibia's CID is currently understaffed with only one officer, the other having been transferred. This officer has undergone general criminal investigation training but no specialised training on TF. Therefore, the limited understanding of TF manifestations by the LEAs, except for NCIS and FIC, owing to severe resource constraints including trained staff hampers effective identification and investigation of potential TF incidences specifically on the financial aspects. This is the underlying reason for Namibia's inability to proactively identify, investigate and prosecute TF cases;*

b. **Limited TF knowledge:** The knowledge of terrorism is present among different LEAs but the understanding of TF in the country is not well established (save for the NCIS and the FIC)

given that different LEAs are unable to identify TF and investigate TF activities even in cases where it was evident that there are potential TF activities[4];

c. **Poor focus on TF:** TF investigation is not integrated and used to support the National CT Strategy. The NCIS is the custodian of Namibia's CT Strategy. However, the Strategy does not have dedicated pillars to deal with TF matters. Its primary focus is the offense of terrorism, with a very short and limited position on TF. This perhaps sums up Namibia's prioritization as authorities did not conduct proper TF investigations in any of the cases. From the four cases, the authorities pursued only three cases for disruption purposes. TF investigations are also hampered by deficiencies identified in Namibia's poor compliance with FATF Recommendation 5; and

d. **Misaligned TF risk:** Namibia's measures on TF and NPOs are inconsistent with the TF risk profile of the country. Though the NRA rates overall TF risk in Namibia low, the measures described by the NCIS discussed under IO9, seem to indicate some of the TF risks that Namibia might be exposed to. Additionally, some of the measures taken such as monitoring of movement of persons from some of the categorised jurisdictions, seem to show a general implementation of measures related to TF. As discussed under IO.1, apart from NCIS and FIC, the LEAs did not appear to have an adequate understanding of TF risks. Therefore, the assessors were of the view that the measures being taken are not consistent with the TF risk profile of Namibia. The inconsistent data relating to the identification and investigation of TF cases also discounts any measures that the country applies to mitigate TF risks.

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 sectors that potentially leads to TF activities. The information contained in this report was derived from STRs/SARs data filed with the FIC by various reporting institutions. Equally, information from NamPol's investigation of the few TF cases has also been obtained and incorporated herein to add value. Namibia has only had about 2 potential TF cases investigated by LEAs. Such cases have been sanitized and included herein. Most, if not all such 2 cases are related to one subject who has

[4] At the time of the ME, the FIC had disseminated 2 cases relating to terrorism and terrorism financing which resulted into LEAs initiating TF inquiry in 2017. However, this case proceeded to prosecution but was withdrawn due to lack of sufficient evidence. Other 2 potential TF cases that LEAs inquired into arose from intelligence reports and through INTERPOL.

been monitored by NamPol for several years since the risk emerged. The same case was reopened in several years suggesting 3-4 TF cases overall.

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

i. TF cases as investigated by LEAs;
ii. Sanitised intelligence emanating from reports and closed databases;
iii. Competent authorities' investigation outcomes; and
iv. Open-source research.

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

5. UNDERSTANDING TF RISK ASSESSMENT

A TF risk assessment is a product or process based on a methodology, agreed upon by relevant parties, that attempts to identify, analyse and understand TF risks and serves as a first step in addressing them. While assessments may take different forms, a TF risk assessment should generally cover the primary TF components which are: raising, moving, storing and using funds or other assets (including goods, vehicles, weapons etc.) to meet the needs of a terrorist or terrorist organisation. This should go beyond the revenue raising aspects and address terrorist resource mobilisation, procurement and terrorist facilitation networks, including Foreign Terrorist Fighters (FTFs).

FATF Recommendation 1 lays out several basic principles with regard to TF risk. It requires jurisdictions, and for this context, institutions to identify, assess and understand the TF risks they face, as well as by designating an authority (AML Compliance Officer) or mechanism to coordinate actions to assess risks. Based on such assessment, institutions should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate TF are adequate with the risks identified. The national and sectoral risk assessment outcomes as published by the FIC over the years should be used to support risk assessments at the institutional level.

5.1. Considerations for jurisdictions with no or few known TF STRs/cases

Countries must assess and continue to monitor their TF risks regardless of the absence of known threats. This approach should be similarly adopted at institutional level. The absence of known or suspected terrorists and TF cases does not necessarily mean that a jurisdiction has a low TF risk, similarly does it not suggest that institutions in such jurisdiction are not exposed to TF risks. In particular, the absence of cases does not eliminate the potential for funds or other assets to be

raised and used domestically (for a purpose other than a terrorist attack) or to be transferred abroad. Jurisdictions without TF and terrorism cases may still need to consider the likelihood of terrorist funds being raised domestically (including through willing or defrauded donors). Equally, the jurisdiction should consider the likelihood of the transfer of funds and other assets through, or out of the country in support of terrorism, and the use of funds for reasons other than a domestic terrorist attack.[5]

TF process organically involves four stages being: raising, moving, storing or using funds and other assets. Such stages are not certainly sequential or linked to a specific terrorism-related activity. Below is a breakdown of such four TF stages:

a. **Raising funds** via numerous methods including legitimate means, donations, self-funding and criminal activity;

b. **Moving funds** to an individual terrorist or a terrorist group, network or cell through a series of knowing or unknowing facilitators and/or intermediaries by means of banking and remittance sectors, informal value transfer systems, bulk cash smuggling and crypto assets, and smuggling high-value commodities such as oil, art, antiquities, agricultural products, precious metals and gems, as well as used vehicles;

c. **Storing funds** intended for an individual terrorist or a terrorist group, network or cell by similar means used in moving funds while planning for their use; and

d. **Using funds** for payment when needed to further the terrorist organisation, group, network or cell's goals, including living expenses, to purchase weapons or bombmaking equipment and/or to finance terrorism operations.

6. SUMMARY OF STRs AND SARs RELATED TO TF ACTIVITIES REPORTED TO FIC

It is essential for combatting agencies and authorities to fully understand the pressures and risks posed by terrorism and TF, in order to effectively prevent and duly investigate such offences.

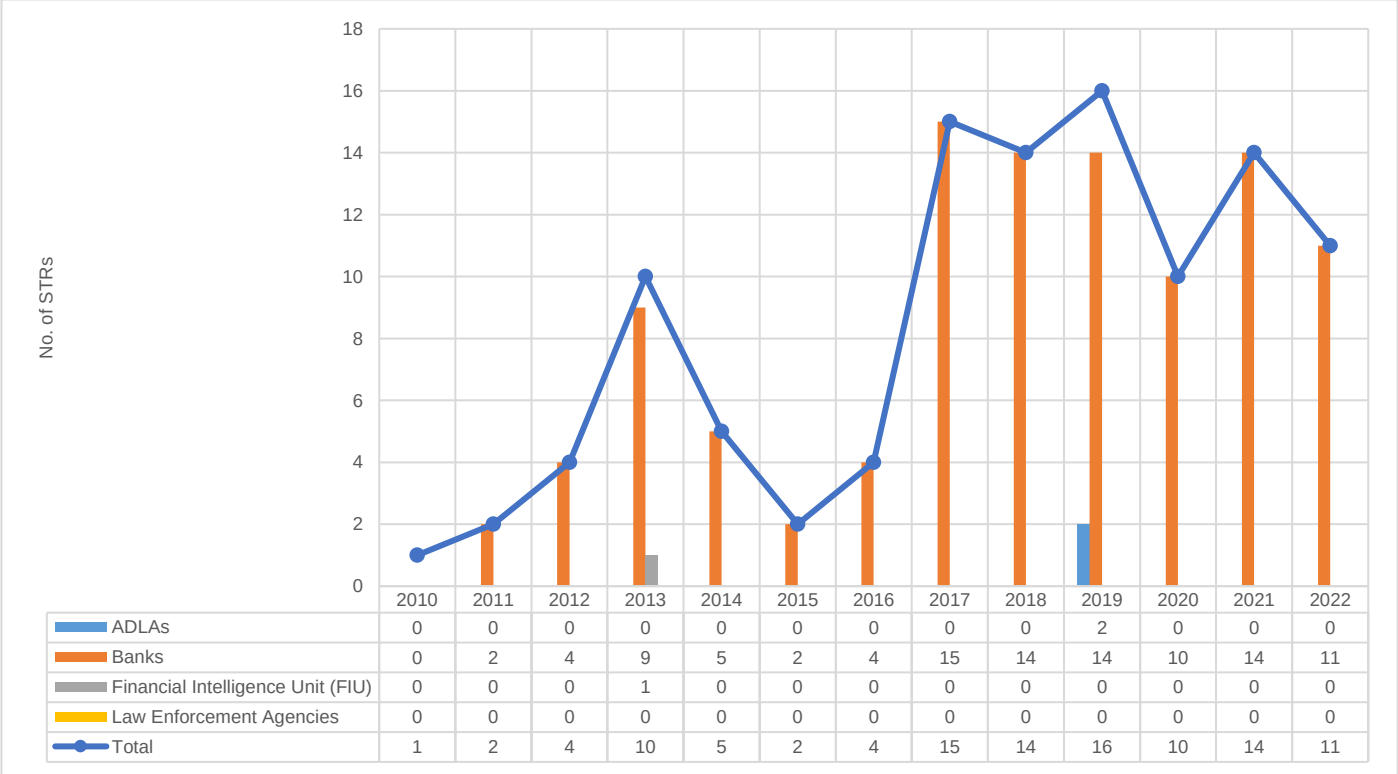
This section provides an overview of STRs/cases related to possible TF risks/threats filed by various sectors and reporting institutions since the reporting obligation commenced in 2009 until 31 December 2022. Worth noting is that when reports are received by the FIC, they are cleansed to determine each report's prioritization level. This process usually results in the decision of whether

[5] FATF Report: Terrorist Financing Risk Assessment Guidance, July 2019.

such reports should be escalated for further investigation (case files opened), or regarded as low priority. In some cases, some reports are set aside when it is concluded that there may not be merits for further investigations. Further, this section presents the total number of reports escalated for investigations based on potential TF activities.

Though the FIC has received many reports from the sectors suggesting potential TF, almost all such reports were determined to be false positives, after FIC analysis. The FIC has only escalated two intelligence reports to LEAs that had indications of potential TF. The STR-related information herein should thus be considered within this context.

Chart 1: Summary of STRs received per Sector

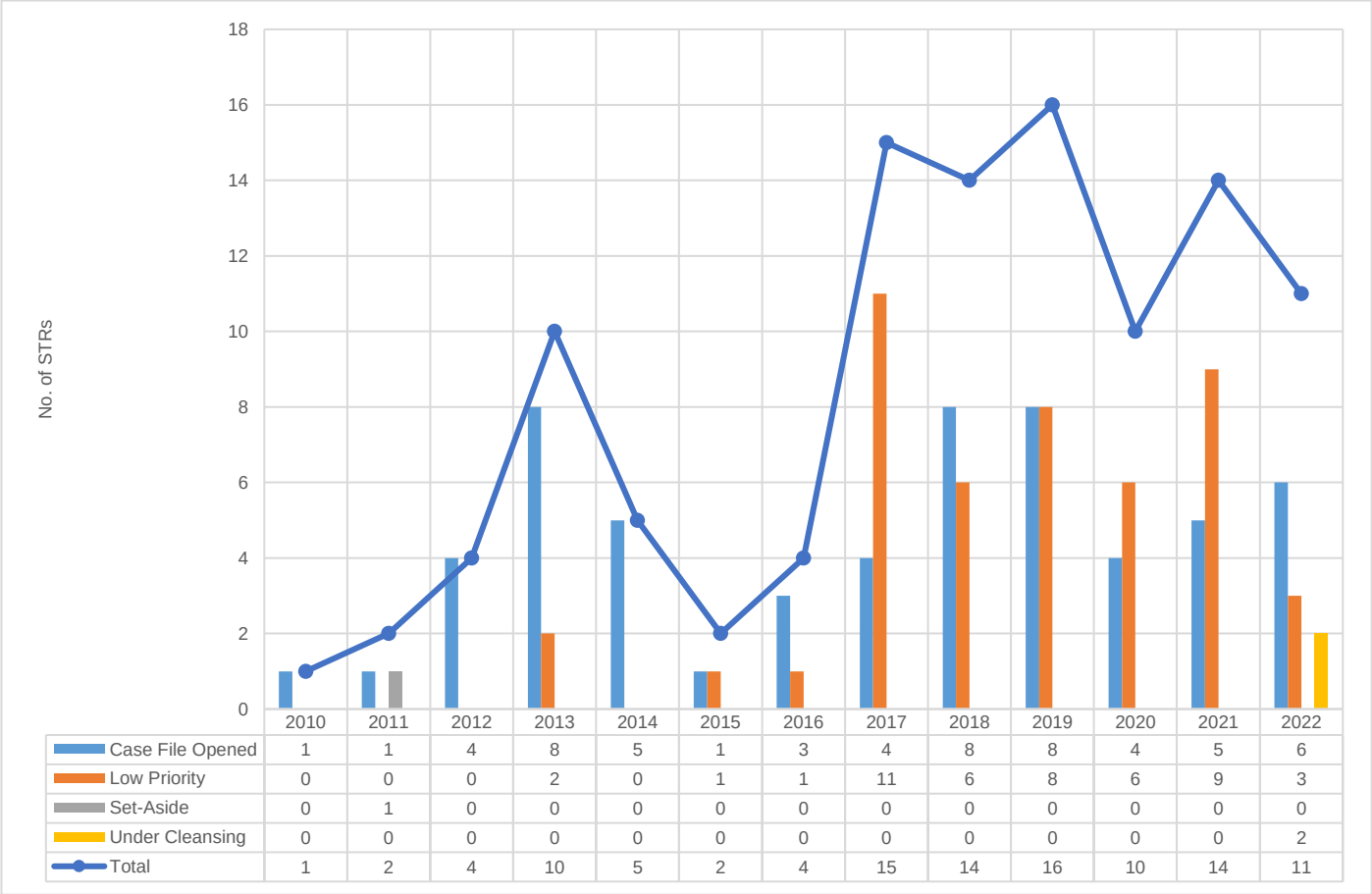


	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
ADLAs	0	0	0	0	0	0	0	0	0	2	0	0	0
Banks	0	2	4	9	5	2	4	15	14	14	10	14	11
Financial Intelligence Unit (FIU)	0	0	0	1	0	0	0	0	0	0	0	0	0
Law Enforcement Agencies	0	0	0	0	0	0	0	0	0	0	0	0	0
Total	1	2	4	10	5	2	4	15	14	16	10	14	11

Chart 1 presents a summary of STRs filed by sectors related to potential TF. The year 2019 saw the highest volume of reports related to potential TF offences with 16 STRs. It is worth noting that 96% of the reports originate from the banking sector. This reporting trend could be attributed to various factors, including the fact that 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 financial crimes as almost all other sectors make use of the banking systems.The ME, as per Immediate Outcome 4, found that TF is understood to some extent by FIs and to a negligible extent by Designated Non-Financial Businesses and Professions (DNFBPs).

As mentioned above, note that many such potential TF reports were deemed false positives within the FIC and not escalated to Law Enforcement for further investigation.

Chart 2: Classification of STRs

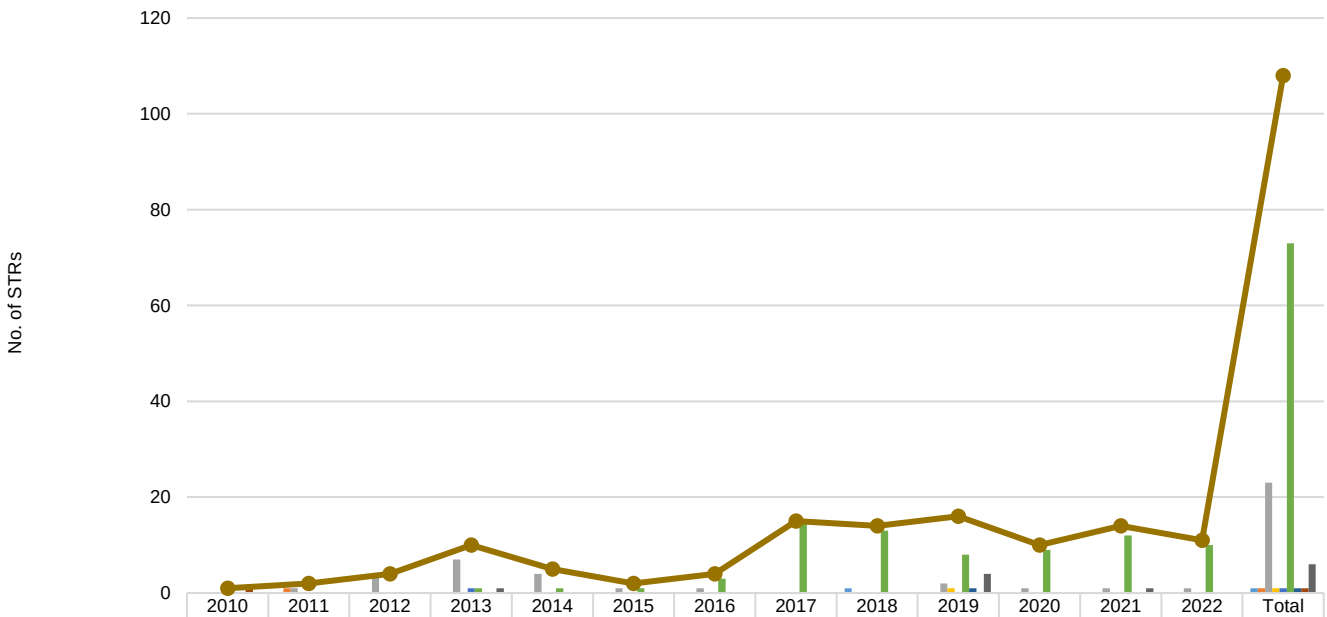


	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Case File Opened	1	1	4	8	5	1	3	4	8	8	4	5	6
Low Priority	0	0	0	2	0	1	1	11	6	8	6	9	3
Set-Aside	0	1	0	0	0	0	0	0	0	0	0	0	0
Under Cleansing	0	0	0	0	0	0	0	0	0	0	0	0	2
Total	1	2	4	10	5	2	4	15	14	16	10	14	11

Overall, the FIC observed that 54% were accorded 'high priority' status and escalated for further analysis (case files opened) whilst 44% were categorized as 'low priority'. Cases such as those involving foreign individuals and entities who transferred funds to high-risk jurisdictions were considered as possible TF. The mere remittance to a high risk jurisdiction appears to be the sole indicator of potential TF in these cases, without other additional indicators. However, NamPol (AML & CFT Division Crime Investigation Directorate) investigations eventually confirmed that such escalated reports are false positives for terrorism or TF and not investigated any further.

On the other hand, only two SARs were reported related to potential TF offenses in the period under review. Such reports were filed in 2021 by Bank-C and were categorized as 'low priority'.

Chart 3: Summary of STRs received per Reporting Entity



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	Total
Bank-A	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Bank-B	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Bank-C	0	1	4	7	4	1	1	0	0	2	1	1	1	23
ADLA-A	0	0	0	0	0	0	0	0	0	1	0	0	0	1
FIC - Namibia	0	0	0	1	0	0	0	0	0	0	0	0	0	1
Bank-D	0	0	0	1	1	1	3	15	13	8	9	12	10	73
ADLA-B	0	0	0	0	0	0	0	0	0	1	0	0	0	1
LEA-A	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Bank-E	0	0	0	1	0	0	0	0	0	4	0	1	0	6
Total	1	2	4	10	5	2	4	15	14	16	10	14	11	108

Chart 3 shows a summary of STRs related to potential TF offences reported by various reporting entities. Bank-D filed the highest volume of reports related to potential TF offences with 73 STRs. The records show that the high number of reports received from Bank-D could be attributed to various factors, including the fact that they appear to be the largest financial institution in terms of volumes of clients. Equally, through such a larger client base, Bank-D's measures aimed at detecting and reporting suspicions can be said to be aligned to the bank's risk exposure. This is based on volumes of reports and bank size. It does not replace any observations in the relevant supervisory observations around compliance.

The following are some of the two involved stages highlighted by the reporting entities amongst others:

Sources/Raising of funds:

- Subjects and entities received suspicious transactions into their bank accounts. Accounts have received funds through cash deposits and from foreign jurisdictions via EFTs;

- Significant foreign cash deposits have been paid into NPO account described as “donations”. Such deposits have been made by individuals from high-risk jurisdictions. The account is also credited with inward swifts from various individuals who appear to be from high-risk jurisdictions; and
- In most cases, the source of funds received into accounts are not known and not in line with client’s account profile.

Moving of funds:

- Funds are subsequently disbursed via cross border ATM cash withdrawals and international purchases; and
- The involved entities and subjects are primarily Close Corporations (CCs) and natural persons. A few NPOs were cited in some reports from sectors but FIC analysis could not find any potential TF in any such reports citing NPOs.

7. SAMPLED CASE STUDIES (TF CASES FROM THE FIC DOMAIN)

Mr-X a Country-L national, married to a Namibian citizen (Ms-M) has reportedly been residing in Namibia since 1996. He is the beneficial owner of at least six business entities registered in Namibia, being: Close Corporation CC-A, Company (PTY) Ltd-A, Close Corporation CC-B, Close Corporation CC-C, Close Corporation CC-D and Close Corporation CC-E. The subject and his entities have been reported in various reports to the FIC on suspicion of possibly advancing TF. Information provided by the LEAs alleged that the subject may be linked to the terrorist group *Hezbollah*. Below is a case study on the said subject with potential indicators of TF.

Case Study: A

The reported subject, Mr-X is a Country-L national, suspected of supporting, aiding or associating with potential terrorist groups. The subject was reported due to withdrawals done in Country-L from his business bank account held with Bank-D in the name of Close Corporation CC-E.

The funds received in the subject’s bank account are purported to be from business activities, however, the nature thereof cannot be ascertained. The analysis confirmed that two visa electronic cards are linked to the account of the subject. The justification made by the subject in respect of the additional card is that his family in Country-L should have access to the funds in the account for their upkeep. It is against this background that funds are withdrawn from the account at different ATMs (Automated Teller Machines) in Country-L. All debit transactions are conducted in Country-L, and

no debit transactions are conducted in Namibia, which cements the suspicion that both cards are used in Country-L.

Due to the above, the subject could expose Namibians to a TF vulnerability as making funds available in this manner presents a high risk of TF.

Open-source information suggests that Mr-X has a connection with Hezbollah, a Country-L military group referred to by the west as a terrorist group. In 2011, the subject was also suspected of human trafficking as he sent six Namibian males to Country-L who underwent labour exploitation at farm-Txx at the outskirts of Town-T of Country-B and Country-L.

Intelligence on the matter was shared with the NCIS and NamPol (AML & CFT Division Crime Investigation Directorate), however, investigations eventually confirmed that such escalated report is false positives for terrorism or TF and did not warrant them to pursue the matter further.

Case Study: B

Another case study is again of Mr-X and his six entities indicated in case study A.

The analysis conducted confirmed that the subject has channeled through his personal and business account a total of NAD 9,4 million to various recipients in Country-B and Country-L. The relationship between the subject and various recipients in the two conturies could not be established.

The subject transferred large amounts of money to recipients in various countries. He further, indicated to be dealing in second-hand vehicles and claims that funds channeled to these destinations are for payments for the purchase of vehicles.

The subject was also being investigated by the receiver of revenue (NamRA) for an amount of NAD 1,15Million reportedly fraudulent funds paid from the receiver of revenue to him or his business, Close Corporation CC-B of which he is the sole owner. In addition to this amount, a total of NAD 851,000.00 was paid into the account of Company (PTY) Ltd-A also owned by the subject purportedly from NamRA.

The analysis conducted concluded that the account of the subject and that of the entities may be linked or associated with funds collected and movement relating to TF. The subject is making use

of business accounts to collect and then channel funds to certain foreign individuals and businesses potentially associated with terrorist activity.

Except for one entity which is a Proprietary Limited Company, all his other businesses, especially the ones where suspicions were noted, are Close Corporations (CCs). This ties in with the 2023 National Risk Assessment update (to the 2020 NRA) which indicates that CCs are most vulnerable to ML and TF abuse. The various risk assessments have equally found that Faith Based Organisations (FBOs) in general present a higher risk for potential TF, with those associated with Islamic extremism most vulnerable to TF risks. The subject in this matter could be bordering on associations with extremist Islamic ideologies.

Intelligence on the matter was shared with the NCIS and NamPol , however, investigations eventually confirmed that such escalated reports are false positives for terrorism or TF and did not warrant them to pursue the matter further.

Report Source Type	STR
Perpetrators Involved	Foreign Individuals and locally registered Close Corporations
Involved sector	Banking and Motor Vehicle Dealerships
Key risk controls	Amongst others, failure to detect questionable bank transactional behavior which conflicted nature of supposed business activities.
Designated services	Personal and business bank accounts
Instruments used	EFTs, Companies, Close Corporations and Individual bank accounts, etc.
Potential Predicate Offence	Possible Terrorist Financing, Tax Evasion, Human Trafficking and Capital Flight.
Red flags/Indicators	*subject reported on various reports to the FIC to be linked to a terrorist;* *the transaction activity of the client is inconsistent based either on the client's usual pattern of activities, such as large cash payments, unexplained payments from a third party, or use of multiple or foreign accounts;* *structured foreign cash withdrawals from accounts;* *frequent transfers to high-risk jurisdictions;*

	subject is implicated in other criminal cases; *frequent international ATM activity in high-risk jurisdictions;and* *faith Based Organisations in general and those associated with Islamic extremism present the highest risk of potential TF.*

Case Study: C

The Namibian Police has Mr-JJ as a potential subject of terrorist act and terrorists funding. The profiling of the subject started during 2016 and the initial case was registered in March 2019. The subject case docket bearing Windhoek CRXXXX was registered for contravention of section 2(1) & (2)- of the Prevention and Combating of Terrorists and Proliferation Activities Act, Act No. 4 of 2014. Further, such case docket is under investigation and the subject has not yet been charged.

It was then established that the subject has been sending funds to individuals in foreign countries that are considered to be high risk in terms of terrorist activities through various foreign money exchange entities. With the information collected, it was discovered that the subject has been using Western Union and Money Gram via ADLA-A, ADLA-B, ADLA-C, and ADLA-D to send and received the money. It is further confirmed that the subject sent and received money from countries such as Country-D, Country-T, Country-M, and Country-F through the same entities. Although the subject was operating in small businesses such as: car washing and dealing in hand second-hand used car sales, as a source of income, this could not sustain him to frequently send money out of the country.

It was also established that the subject is currently venturing in the charcoal industry operating under two companies in the Grootfontein district as follows:

1. **Company: Close Corporation-XX1**

a. Mr-JJ (5%): Namibian national;

b. Mr-IM (40%): Country-K national;

c. Mr-Fx (30%):: with dual citizenship of Country-S1 and Country-S2; and

d. Mr-HJ (25%): Country-S.

2. Close Corperation-XX2

a. Mr-JJ (10%); and

b. Mr-HAA (90%): Country-KK national.

Thus far, the subject is not arrested or interviewed in relation to the matter and the case is still under investigation.

Report Source Type	NamPol (AML & CFT Division Crime Investigation Directorate)
Perpetrators Involved	Namibian National
Involved sector	ADLAs; Used Car Dealerships and Carwash.
Key risk controls	Amongst others, failure to detect questionable transactional behavior which conflicted nature of supposed activities.
Designated services	Western Union and Money Gram through money remittance and currency exchange Services
Potential Predicate Offence	Possible Terrorist Financing and Capital Flight.
Red flags/Indicators	*the above-mentioned entities in the name of the subject and other beneficiaries are exporting charcoal to foreign jurisdictions in the Middle East, but no payments are received in their local business accounts;* *as such it is suspect that, the profit is channelled to fund possible terrorist activities elsewhere;* *the subject is religiously radicalised into ISLAMIC religion which is linked to ISIS;* *funds may be generated through the exportation of charcoal, and with the available information from the banking institutions, no indications of income could be traced;* *the subject engaged himself on social media like Facebook and WhatsApp where he is sympathizing with and supported the activities of ISIS, by posting pictures;* *to date, through investigations, it is confirmed that funds are raised under the pretext of the charcoal business; and* *faith-Based Organisations in general and those associated with Islamic extremism present the highest risk of potential TF.*

Case Study: D

The FIC received a request for information on a certain subject from LEAs. The information requested was related to Mr-DD, a Namibian national, suspected of financing terrorism. The subject was suspected to have joined a Muslim guerrilla militant movement known as the Mujahideens abroad and was requesting friends and former colleagues to join the jihad. The FIC conducted a financial analysis on the Bank-D account held in the name of the involved subject. Analysis showed that for the period of 23 October 2010 to 15 May 2015, the subject was a student at WWT University in South Africa and was also for some periods employed at an entity named GHGH Limited. The analysis confirmed that the subject received a monthly salary ranging between NAD 3,000.00 and NAD 20,000.00 from such entity. Further, the analysis on the bank account confirmed that a certain lady (Ms-SS) has made regular cash deposits into the subject's bank account.

Between January 2014 and December 2014, the subject transferred an amount of NAD 40,000.00 to an account in favour of Sadaqa. It is alleged that Sadaqa is an Islamic term that means "voluntary charity"[6]. The analysis further revealed that the subject purchased an air ticket in February 2015. It is also alleged that the subject was destined for the vicinity of IISS in Country-TTk and surrounding areas. Subsequently, on 16th February 2015, an amount of NAD 25,000.00 was transferred from the Bank-D account held in the name of Mr-JN into the subject's bank account. The subject later made several cash withdrawals in Country-SAA and other structured foreign cash withdrawals in Country-TTk. This potentially represents the final stages of the subjects' journey from Namibia to Country-TTk and beyond, to join the Islamic Jihad.

Intelligence on the matter was shared with the Namibia NCIS and NamPol. It is further confirmed that the subject was reported killed abroad.

Report Source Type	RFI
Perpetrators Involved	Namibian National
Involved sector	Banking, NPO - charity (sadaqa)
Key risk controls	Amongst others, failure to detect questionable bank transactional behavior which conflicted nature of supposed activities.

[6] Sadaqa is charity given voluntarily in order to please God. Sadaqa also describes a voluntary charitable act towards others, whether through generosity, love, compassion or faith.

Designated services	Bank accounts
Instruments used	EFTs, Point of Sale (PoS) and ATM.
Potential Predicate Offence	Possible Terrorist Financing and Capital Flight.
Red flags/Indicators	*subject reported to the FIC to be linked to terrorist groupings/activities;* *subject made cash withdrawals and electronic funds transfers after funds deposits;* *the transaction activity of the client is inconsistent based either on the client's usual pattern of activities, such as large cash payments, unexplained payments from a third party, or use of multiple or foreign accounts;* *structured foreign cash withdrawals from the account;* *frequent international ATM activities in a high-risk jurisdiction; and* *faith Based Organisations (FBOs) in general and those associated with Islamic extremism present the highest risk of potential TF.*

8. COMMON POTENTIAL INDICATORS OF TF

Certain red flags point to potential TF abuse. This section presents a summary of indicators that may signal the occurrence or presence of TF potential predicate offenses. Such indicators are observable events that point to the likelihood of specific activities occurring. When each indicator is viewed in isolation, it may not readily point to TF, but when viewed with other indicators and relevant factors, it may highlight potential TF. The below are an addition to the specific indicators highlighted in some sections above and other FIC publications on the matter. It is worth noting that these serve merely as a guide and therefore not exhaustive of all possible TF indicators:

Table 1: General potential indicators of TF
• The entity applies for tax-exempt status as a charity or NPO, especially high risk and Specified NPOs such as FBOs and Charities;
• Fundraises through personal correspondence, newsletters, crowdfunding and via the organisation's website;
• Open domestic bank account(s) into which proceeds and donations are deposited;
• Transfers of funds to overseas branches, diverting some (or all) of these funds FBOs, especially those closely associated with radical or extremist ideologies;

• Significant and unusual transactions involving NPOs, especially high risk NPOs such as charities and FBOs. Changes in the objectis or activities of such NPOs;
• Payments by entities to NPOs that public officials are known to be associated with. When high risk NPOs are associated with prominent figures who subscribe to extremist ideologies;
• Frequent cash deposits and transfers into the NPO's bank accounts from high-risk jurisdictions;
• Individuals and entities transfer funds to various high-risk jurisdictions, especially those known to have active terrorism/conflict;
• Client attempts to close NPO account(s) to avoid due diligence questioning by the banks/financial institutions;
• An entity that pays other firms to perform logistical roles in countries where there is a high degree of perceived terrorism and which they could perform themselves, in order to transfer the risk to the other firm or distance themselves from CDD;
• Entity, NPOs, or persons that are closely aligned to or supporting radicalizations and extremism or terrorist organizations internationally;
• A pattern of sending or receiving international EFTs to or from foreign businesses that operate in a sector or industry unrelated to each other;
• The NPO or entity moves funds or other resources frequently to areas of conflict/active terrorism;
• Transactional patterns from NPO or entity accounts that are exclusively one-directional. e.g., the entity only sends but never receives EFTs, or vice versa;
• The NPO or 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's primary NPO objective, however, their account receives significant funds;
• Entity or NPO deals in cash or alternative remittance systems where no formal banking infrastructure exists; and
• Entity or NPO has extremely complicated financial records in which suspicious transactions are less easy to identify. It is also suspicious if the governance framework of an NPO is complex to enable the identification of those managing its affairs, its donors or recipients/beneficiaries.

8.1. How is Terrorist Financing risk different from Terrorism risk?

TF risk and terrorism risk are often, but not always, interlinked. For instance, an assessment of TF risk may require consideration of domestic and foreign terrorist threats. If a jurisdiction has active terrorist organizations operating domestically or regionally, this is likely to increase the probability of TF. A country with no active terrorist activities may wrongly assume that its risk of actual terrorism and TF are low or non-existent. However, in light of the cross-border nature of TF, a jurisdiction that faces a low terrorism risk may still face significant TF risks. A low terrorism risk implies that terrorist individuals and groups may not be using funds domestically for terrorist attacks. However, actors may still exploit vulnerabilities to raise or store funds or other assets domestically, or to move funds or other assets through the jurisdiction[7].

[7] FATF Report: Terrorist Financing Risk Assessment Guidance, July 2019.

9. KEY FINDINGS

STRs and SARs filed by the reporting institutions concerning potential TF have assisted the FIC and LEAs in pursuing and detecting criminals engaged in suspected TF. Further, clients who are legal persons essentially present higher TF risks than natural persons when the ultimate beneficial owners in such legal persons cannot be readily and reliably identified. Below is a summary of the key findings concerning the TF risks and vulnerabilities:

a. 108 STRs involving potential TF were reported to the FIC. Importantly, 54 STRs were accorded “high priority” status and escalated for further analysis and investigation with the FIC. Importantly, many such potential TF reports were deemed false positives within the FIC and not escalated to Law Enforcement for further investigation. With those escalated to NamPol, almost all were deemed false positives for terrorism or TF and not investigated any further;

b. Only 2 SARs were reported related to potential TF offenses;

c. Bank-D filed the highest volume of reports related to potential TF offenses with 73 STRs;

d. The information herein suggests banks, perhaps due to their nature of business activities and in particular, cross-border remittance services, are most vulnerable to TF-related threats. 96% of the potential TF reports originated from this sector. The banking sector has comparatively more matured AML/CFT/CPF control systems which naturally means banks can readily identify TF threats, compared to other sectors. 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 TF and other financial crimes;

e. It is worth noting that apart from banks, ADLAs (money service businesses) appear to be most vulnerable to TF-related threats as demonstrated under case study C;

f. It is generally understood that beneficial owners who may advance TF will most likely use complex ownership structures that hide their identification or representation. CCs in particular are most vulnerable for TF abuse. 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; and

g. Certain subjects (Namibian and Country-L nationals) and entities have been reported in various reports to the FIC with the possibility that they may be advancing TF activities.

10. POSSIBLE RECOMMENDATIONS

a. **Implement risk-based measures:** It is clear that sectors are implementing measures to prevent services from being abused for TF. Nevertheless, it is significant for supervised institutions to identify whether these measures are appropriate with the risks identified to target greater measures to those sectors exposed to higher risks, and not generate the unplanned effects of implementing excessive measures to sectors that are exposed to lower risks of being abused for TF;

b. **Encouraging dialog with the sector:** The outreach and involvement of the sectors, especially DNFBPs, in the risk identification and management process is very helpful to obtain all the information available and to develop strategies to mitigate and address these risks adequately;

c. **International cooperation:** Namibia should encourage the strengthening of effective mechanisms to respond to requests for information related to TF. Developing effective collaboration between countries and sectors can help identify complementary measures that are relevant and adjusted to the needs of the sectors, but also relevant to prevent misuse for both TF and other crimes; and

d. **Guidance on Targeted Financial Sanctions (TFS):** Sectors are encouraged to study Guidance Note 07 of 2023 on Targeted Financial Sanctions for guidance relating to combatting TF, through freezing, prohibition and filing the relevant reports when suspecting TF, sanctions screening name matches etc.

11. CONCLUSION

TF poses a threat to Namibia's national security including the integrity and reputation of its financial system. Besides posing a security threat, it also impacts the integrity of financial and non-financial institutions such as charities and non-profit organizations which could be exploited, often unknowingly, for the financing of terrorism. Further, terrorists and terrorist groups may use both

legitimate and illegitimate means to raise funds for personal upkeep, recruitment, and purchase of tools and equipment, amongst others.

The FIC's supervision function is currently updating the sectoral risk assessment which could help yield more information on threats and vulnerabilities within sectors. Further, a lack of awareness of TF risks and red flag indicators, especially amongst DNFBPs, reduces the likelihood that sectors would be in a position to protect their services from TF abuse. 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. Similarly, the Namibian Police are expected to note observations herein to help aid in combatting and investigating TF.

This report or similar studies on TF risks and within sectors will be updated periodically when the need arises.

Z. Barry
ACTING DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

12. ANNEXURES

Annexure 1: Spontaneous Disclosures to LAEs

No.	Subject/Entity Name	Possible Predicate Offence	Amount Involved (NAD)	LEAs Conclusion
	2011			
1	Names of subjects/enties herein have been removed for obvious reasons	Possible Terrorism Financing	9,445,838.75	No Terrorism or TF found
2	Removed	Possible Terrorism Financing	29,656,198.54	No Terrorism or TF found
	Total		**39,102,037.29**	
	2012			
1	Removed	Possible Terrorism Financing	7,539,044.11	No Terrorism or TF found
	Total		**7,539,044.11**	
	2013			
1	Removed	Possible Security Threat	N/A	No Terrorism or TF found
2	Removed	Possible Security Threat	N/A	No Terrorism or TF found
3	Removed	Possible Terrorism Financing	3,032,483.04	No Terrorism or TF found
	Total		**3,032,483.04**	
	2014			
1	Removed	Possible Money Laundering & Terrorism Financing	2,000,000.00	No Terrorism or TF found
2	Removed	Possible Terrorism Financing	1,306,880.80	No Terrorism or TF found
3	Removed	Possible Money Laundering & Terrorism Financing	1,888,428.46	No Terrorism or TF found
4	Removed	Possible Terrorism Financing	676,528.75	No Terrorism or TF found
	Total		**5,871,838.01**	
	2015			
1	Removed	Possible Terrorism Financing	397,176.12	No Terrorism or TF found
2	Removed	Possible Terrorism Financing	267,121.86	No Terrorism or TF found
3	Removed	Possible Money Laundering & National Threat	747,543.35	No Terrorism or TF found
4	Removed	Possible Money Laundering & Terrorism Financing	696,517.25	No Terrorism or TF found
5	Removed	Possible Money Laundering & Terrorism Financing	2,830,000.00	No Terrorism or TF found
6	Removed	Possible Terrorism Financing	460 182.44	No Terrorism or TF found
7	Removed	Possible Proliferation Activities	3,586,271.15	No Terrorism or TF found
8	Removed	Possible Proliferation Activities	13,000,000.00	No Terrorism or TF found
9	Removed	Possible Terrorism Financing	535,947.50	No Terrorism or TF found

10	Removed	Possible Terrorism Financing	1 943 819.43	No Terrorism or TF found
	Total		**22,060,577.23**	
	2016			
1	Removed	Possible Terrorism Financing	0.00	No Terrorism or TF found
2	Removed	Possible Proliferation activities	3,305,792.00	No Terrorism or TF found
3	Removed	Possible Proliferation activities	21,000,000.00	No Terrorism or TF found
4	Removed	Possible Terrorism Financing	0.00	No Terrorism or TF found
5	Removed	Possible Terrorism Financing	56,916.08	No Terrorism or TF found
6	Removed	Possible Proliferation Activities	322,816.00	No Terrorism or TF found
7	Removed	Possible Proliferation Activities	0.00	No Terrorism or TF found
	Total		**24,685,524.08**	
	2017			
1	Removed	Possible Terrorism Financing	1,856,890.00	No Terrorism or TF found
	Total		**1,856,890.00**	
	2018			
1	Removed	Possible Terrorism Financing	861,468.82	No Terrorism or TF found
4	Removed	Possible Terrorism Financing	45,722.30	No Terrorism or TF found
2	**Total**		**907,191.12**	
	2020			
1	Removed	Possible Terrorism Financing	0.00	No Terrorism or TF found
2	Removed	Possible Terrorism Financing	8,843,535.26	No Terrorism or TF found
	Total		**8,843,535.26**	
	2021			
1	Removed	Possible Terrorism Financing	90,836.33	Under investigation
	Total		**90,836.33**	
	2022			
1	Abdullah Abdul-Jabbar ABDUL-HAY	Possible Terrorism Financing	0.00	No Terrorism or TF found
	Total		**0.00**	
	2023			
1	Removed	Possible National Security Threat	0.00	No Terrorism or TF found
2	Removed	Possible Terrorism Financing	0.00	No Terrorism or TF found
	Total		**0.00**	