MARCH 2026

INSURANCE FRAUD AND MONEY LAUNDERING TYPOLOGY REPORT

+264 61 285 0054

https://www.fic.na

114 Nickel Street Prosperita

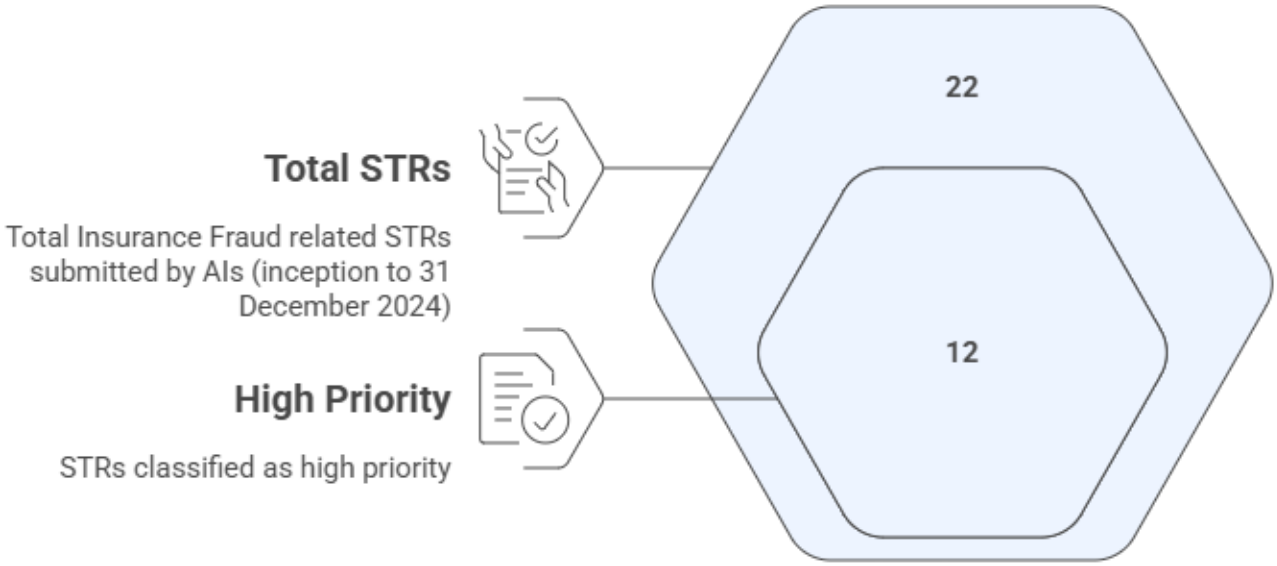
TABLE OF CONTENTS

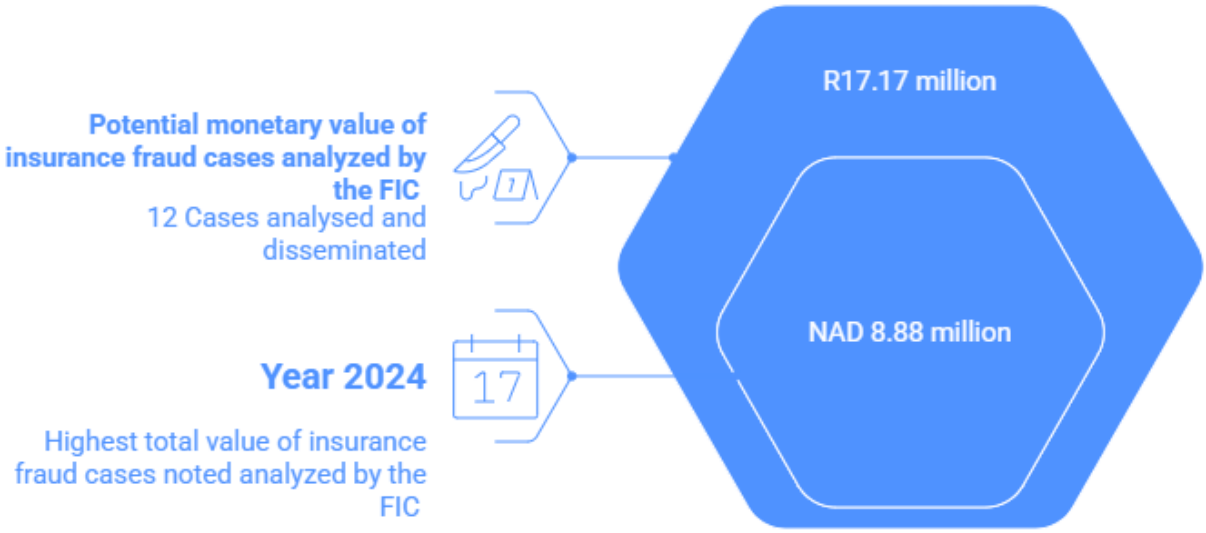
1. ACRONYMS AND DEFINITIONS

Accountable Institution (AI)	Means a person or entity listed in schedule 1 and 3 of the Act. The term "accountable and reporting institutions" in this document refers to all Authorised Dealers and Authorised Dealers with Limited Authority.
Act	Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended.
Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation framework (AML/CFT/CPF)	Refers to the national (or international) framework which combats and prevents money laundering, terrorism and proliferation financing activities.
Customer due diligence	Means a process which involves establishing the identity of a client and monitoring all transactions of the client against the client's profile.
FIA	The Financial Intelligence Act, 2012 (Act No. 13 of 2012), as amended (also referred to as the Act).
Customer due diligence	Means a process which involves establishing the identity of a client and monitoring all transactions of the client against the client's profile.
FIC	Means the Financial Intelligence Centre. It is sometimes referred to as the FIC.
PF	Refers to Proliferation Financing. "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".
ML	Money laundering (ML)" Generally, refers to the act of disguising the true source of proceeds generated from unlawful activities and presenting such in the financial system as sourced from legitimate activities. However, in terms of the Prevention of Organized Crime Act, 2004, as amended (POCA), the definition of ML is broad enough to include engagement, acquisition and concealment of proceeds of crime whether directly or indirectly.
SAR	Refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.

STR	Refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.
TF	“Terrorist financing (TF)” includes “acts which are aimed at directly or indirectly providing or collecting funds with the intention that such funds should be used, or with the knowledge that such funds are to be used, in full or in part, to carry out any act of terrorism as defined in the Organization for African Unity (OAU) Convention on the Prevention and Combating of Terrorism of 1999, irrespective of whether or not the funds are actually used for such purpose or to carry out such acts.”
	“Terrorism” Whilst no acceptable international definition on terrorism exists, it is generally described as the execution of acts of violence against persons or property, or a threat to use such violence, with the intent to intimidate or coerce a Government, the public, or any section of the public to achieve or promote any tribal, ethnic, racial, political, religious or ideological objectives .

Key Highlights:





SECTION A

2. INTRODUCTION

Insurance fraud and Money Laundering (ML) are significant and interrelated threats to the integrity of financial systems. While traditionally perceived as separate criminal activities, recent typology analyses reveal that fraud schemes in the insurance sector are increasingly being exploited as channels for laundering illicit funds. This convergence poses complex investigative challenges for insurers, regulators, and law enforcement agencies (LEAs), as fraudulent claims can disguise the movement of criminal proceeds, and legitimate insurance processes may unintentionally be misused during the layering or integration stages of money laundering.

The insurance industry's diverse products including life insurance, annuities, health insurance, and property coverage offer multiple opportunities for exploitation. Fraudulent activities may range from staged accidents and inflated claims to the deliberate misrepresentation of information to obtain policy payouts. Once obtained, illicit funds may be cycled through insurance payouts, policy loans, or early surrenders, thereby obscuring their criminal origin.

This report provides a structured analysis of common and emerging typologies that illustrate how insurance fraud is used as a predicate offense for money laundering or as a mechanism to disguise illicit funds.

In terms of the 2023 updated National Risk Assessment (NRA) outcomes and various Financial Intelligence Centre (FIC) monthly and quarterly reports, fraud remains one of the main predicate offences associated with ML in Namibia. This report avails a detailed summary of common typologies, patterns and indicators of potential insurance fraud identified in cases within the domain of the FIC. It is hoped that this report will help enhance sectoral understanding of fraudulent practices and result in the implementation of enhanced control measures within the sectors.

3. OBJECTIVES OF THIS REPORT

The objectives of this typology report are to:

4. METHODOLOGY

The FIC analysed relevant data and reports at its disposal to understand potential methodologies, trends, typologies, and associated red flags linked to insurance fraud, which may give rise to ML/TF/or PF activities. The information contained in this report was primarily derived from STRs and SARs submitted to the FIC by various AIs and RIs. Additional insights were obtained from cases escalated for further analysis by the FIC, as well as from Spontaneous Disclosures (SDs) issued to relevant Law Enforcement Agencies (LEAs).

Specifically, the sources of data and information analysed include:

a) Sanitised intelligence derived from reports and closed databases;
b) Investigation outcomes provided by competent authorities; and
c) Open-source research and publicly available information.

The findings from these sources were subject to comprehensive analysis, the results of which are summarised in this report.

5. DEFINITION OF FRAUD AND INSURANCE FRAUD

In general, fraud involves intentional misrepresentation or concealment of facts whether by withholding important information or by providing false statements for the purpose of securing a benefit that would not otherwise be granted. Likewise, depriving another individual or institution of a rightful benefit through such deceptive means also constitutes fraud.

Insurance fraud, a pervasive challenge within the financial and insurance sectors, arises when parties involved in the insurance process intentionally deceive or manipulate information to gain an unlawful financial benefit. Typically, an insurance company, agent, adjuster, or policyholder may deliberately engage in deception to obtain an unlawful financial advantage. In this instance, a fraudulent activity may occur at different stages of the insurance process, including policy purchase, underwriting, claims handling, and settlement.

Furthermore, insurance fraud may involve individuals defrauding insurance companies, or conversely, agents or company employees defrauding policyholders. In essence, beyond the direct financial harm caused to insurers, such fraudulent activity has broader consequences,

including increased premiums for consumers, reputational risk for insurance providers, and systemic vulnerabilities that may be exploited for ML and other financial crimes.

For instance, in the context of the Property and Casualty (P&C) insurance industry, common categories of fraud include:

SECTION B

6. OVERVIEW OF STRS, SARS, AND CASES RELATED TO GENERAL FRAUD AND INSURANCE FRAUD REPORTED TO FIC

This section provides an overview of STRs, SARs and Cases[1] related to possible insurance fraud filed by AIs and RIs from the commencement of reporting obligations in **2009 up to 31 December 2024**.

Upon receipt, all reports submitted to the FIC undergo a cleansing stage, during which they are reviewed to assess their relevance and quality. Reports with indicators warranting further scrutiny are escalated into active cases for detailed investigation and analysis.

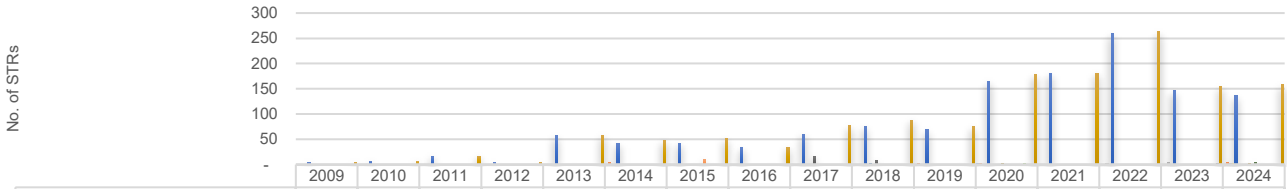
In addition, this section outlines:

1. The **total number of reports** escalated into cases related to potential general fraud and insurance fraud; and
2. The **total number of disclosures** made by the FIC to relevant LEAs in connection with these cases.

This analysis provides insight into the scale, progression, and investigative outcomes of reporting trends in insurance fraud over the period under review.

1 Cases within FIC domain

Chart 1: General Fraud related STRs received from Sectors annually

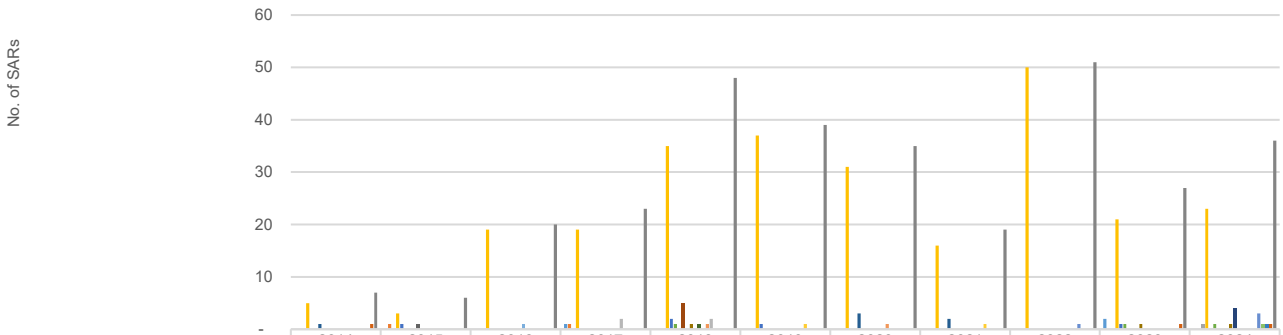


	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Accountants and Auditors	-	-	-	-	-	-	-	-	-	-	-	3	-	-	1	-
ADLAs	-	-	-	-	-	5	-	-	-	-	2	3	1	-	1	5
Asset Management Companies	-	-	1	-	-	-	-	-	-	-	-	1	-	3	4	3
Auctioneers	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
Banks	5	7	16	4	57	42	42	33	60	75	69	165	180	259	146	136
Casinos	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	1
Financial Intelligence Unit (FIUs)	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-
Natural Persons	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Insurance/Investment Brokers	-	-	-	-	-	-	-	-	16	8	-	-	-	-	-	1
Legal Practitioners	-	-	-	-	-	-	-	-	1		-	2	-	-	-	2
Lending Institutions	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-
Long Term Insurance Services	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	4
Micro Lenders	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Money and Value Transfers (MVT's)	-	-	-	-	-	-	10	-	-	-	-	-	-	-	-	-
Motor Vehicle Dealerships	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	1
Pension Fund Administrators	-	-	-	-	-	-	-	1	-	1	-	-	-	-	-	-
Short Term Insurance Services	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-
Supervisory Bodies	-	-	-	-	-	-	-	-	-	1	1	2	-	-	-	1
Trust and Loan Companies	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-
Unit Trust Schemes	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-
Virtual Assets Service Providers	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-
Total	5	7	17	4	58	47	52	34	77	88	75	178	181	263	154	158

The chart above summarizes STRs related to potential fraud received from supervised entities. Overall, the trend shows a steady increase in fraud-related reports submitted to the FIC over the years. From the commencement of reporting obligations up to 31 December 2024, a total of 1,398 STRs were filed. The year 2022 recorded the highest volume with 263 STRs.

Firstly, in terms of sectoral contributions, the banking sector accounted for 93% (1,296 reports), making it by far the largest source of fraud-related STRs. The second highest contributions came from insurance and investment brokers with 2% (25 reports). The higher volume of reports from banks can be explained by factors such as the sector's relatively mature AML/CFT/CPF control systems, which enhance their capacity to identify and report suspicious activity. Secondly, banking services remain inherently more exposed to fraud risks, as they serve as the central infrastructure for financial transactions across all other sectors.

Chart 2: General Fraud related SARs received from Sectors annually



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Accountants and Auditors	-	-	-	1	-	-	-	-	-	2	-
ADLAs	-	1	-	1	-	-	-	-	-	-	-
Auctioneers	-	-	-	-	-	-	-	-	-	-	1
Banks	5	3	19	19	35	37	31	16	50	21	23
Financial Intelligence Unit (FIUs)	-	1	-	-	2	1	-	-	-	1	-
Foreign Financial Intelligence Unit	-	-	-	-	1	-	-	-	-	1	1
Natural Person	1	-	-	-	-	-	3	2	-	-	-
Insurance/Investment Brokers	-	-	-	-	5	-	-	-	-	-	-
Law Enforcement Agencies	-	1	-	-	-	-	-	-	-	-	-
Legal Practitioners	-	-	-	-	1	-	-	-	-	1	1
Long Term Insurance Services	-	-	-	-	-	-	-	-	-	-	4
Micro Lenders	-	-	-	-	1	-	-	-	-	-	-
Money and Value Transfers (MVT's)	-	-	1	-	-	-	-	-	-	-	-
Motor Vehicle Dealerships	-	-	-	-	1	-	1	-	-	-	-
Real Estate Agencies/Agent	-	-	-	2	2	-	-	-	-	-	-
Short Term Insurance Services	-	-	-	-	-	1	-	1	-	-	-
Stock Brokers	-	-	-	-	-	-	-	-	1	-	3
Supervisory and Regulatory Bodies	-	-	-	-	-	-	-	-	-	-	1
Supervisory Bodies	-	-	-	-	-	-	-	-	-	-	1
Unit Trust Schemes	1	-	-	-	-	-	-	-	-	1	1
Total	7	6	20	23	48	39	35	19	51	27	36

Chart 2 illustrates the number of SARs related to potential fraud submitted by reporting entities from the commencement of the reporting obligation until 31 December 2024. To date, the FIC received a total of 311 SARs, with the highest number recorded in 2018 at 48 reports. The data further shows that the banking sector was the leading contributor, collectively submitting 259 SARs, which represents 83% of all reports. This was followed by submissions from natural persons and insurance/investment brokers.

6.1 Level of prioritization of reports from AIs and RIs

The FIC applies a risk-based approach to determine the prioritization level assigned to reports received. Reports that cannot be addressed immediately are classified as low priority. For example, a report may receive a low-priority designation if the suspicion raised does not align with the strategic focus areas of law enforcement or if the financial amounts involved are negligible compared to other reports under review.

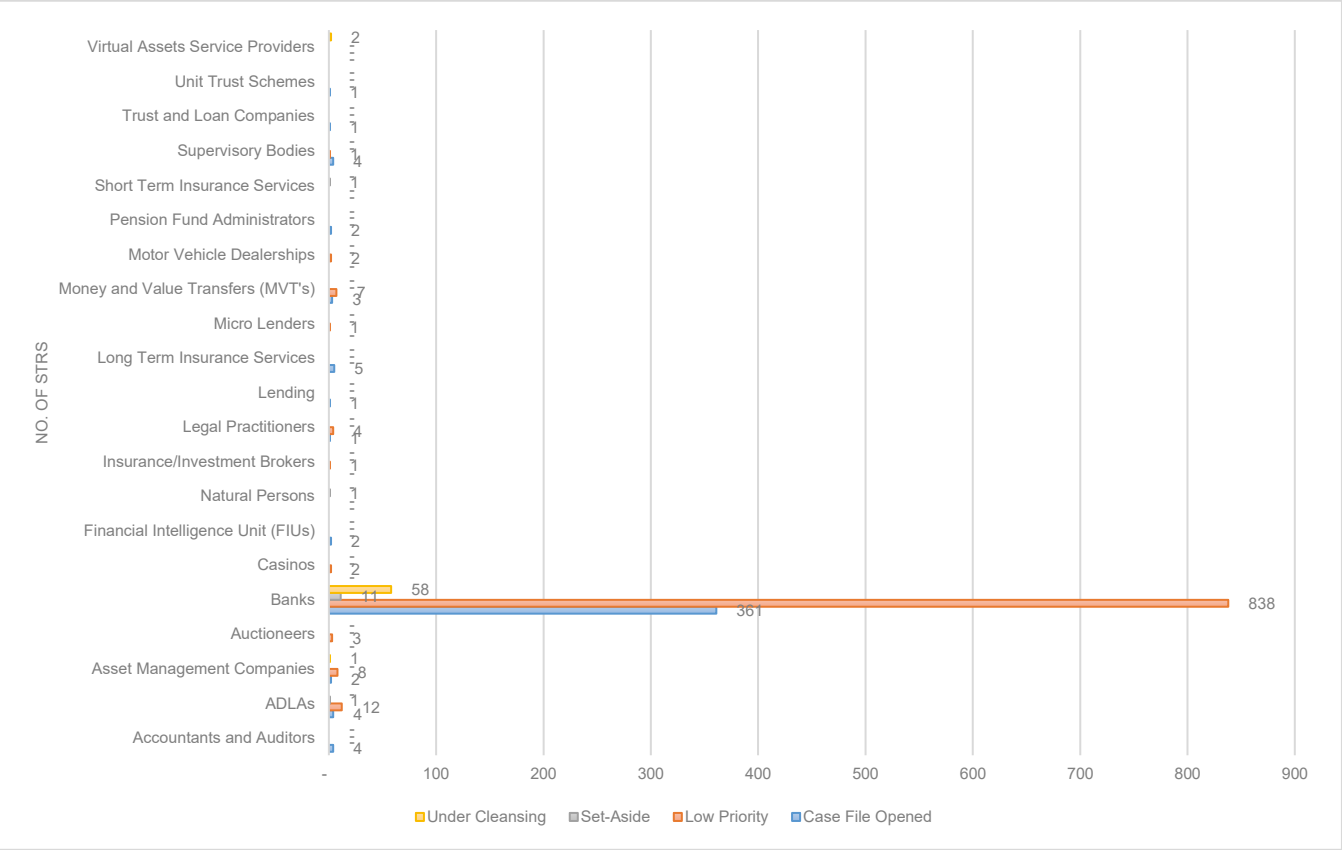
Equally, reports that meet certain criteria and exhibit significant risk indicators may be escalated for further analysis and could ultimately result in the opening of a case.

The following factors collectively inform the FIC's prioritization process:

a) Strategic priorities of Law Enforcement Agencies (LEAs), guided by risk areas identified in the National Risk Assessment (NRA);
b) Known indicators of Money Laundering (ML), Terrorist Financing (TF), and/or Proliferation Financing (PF);
c) Listings on various domestic and international sanctions lists;
d) Existence of prior reports related to the same subject or entity;
e) Geographic locations identified as high-risk areas;
f) Duplicate or erroneous filings, which may result in the STRs/SARs being set aside;
g) Risk of funds being moved beyond the reach of law enforcement; and
h) Human resource constraints within the FIC's Financial Investigations and Analysis Division.

This risk-based methodology enables the FIC to allocate its resources effectively, ensuring that investigations focus on the most significant threats to the integrity of the financial system.

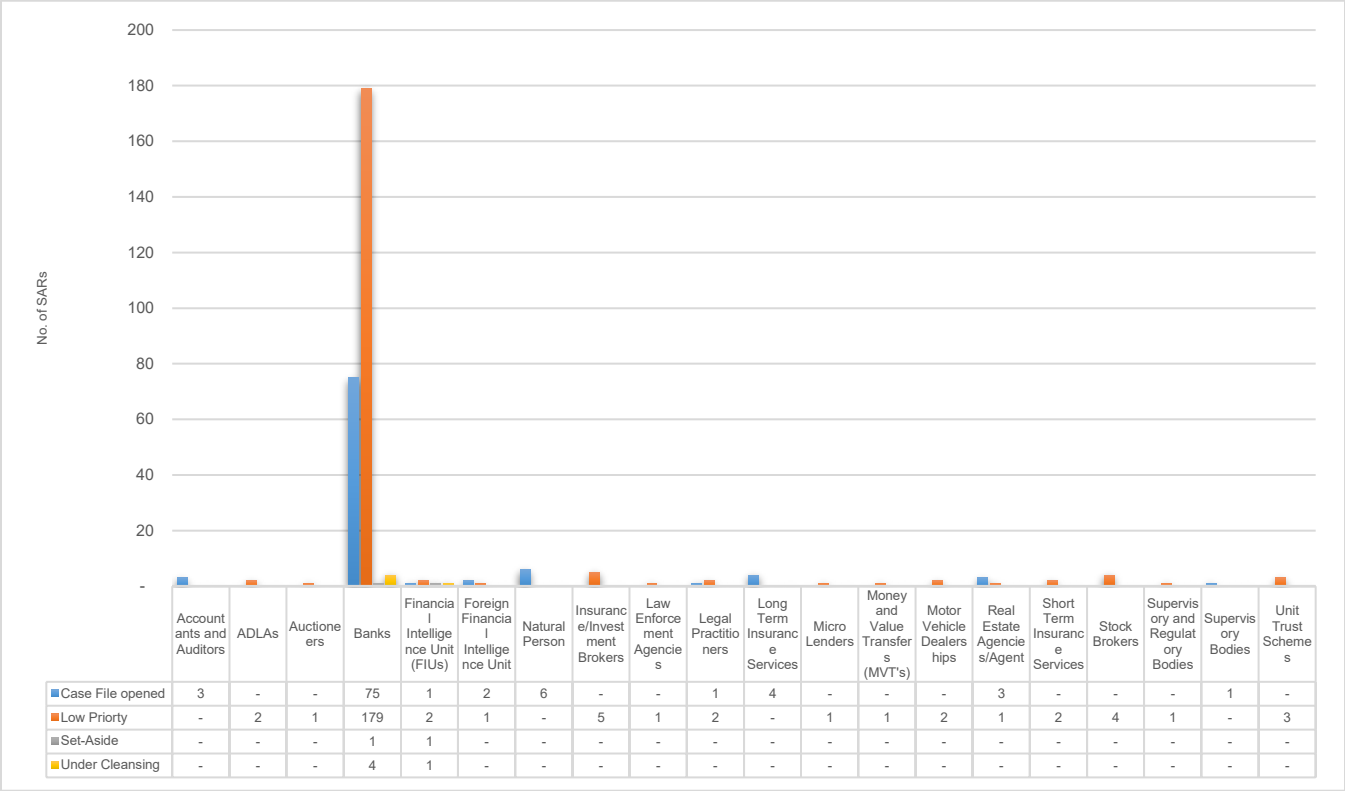
Chart 3: Classification of general Fraud Related STRs received by Sectors



Overall, the FIC observed that a total of 391 STRs were designated as high priority and escalated for further analysis, with case files opened to facilitate in-depth investigation. In contrast, 879 STRs were assessed as low priority, indicating that while they contained potentially relevant information, they posed a lower immediate risk or lacked sufficient indicators of serious financial crime.

Of particular significance, 361 of the high-priority STRs originated from the banking sector, underscoring the sector's critical role in identifying and reporting suspicious activity. The prominence of banking-sector STRs highlights both the sector's robust reporting mechanisms and its central position in the movement of funds, making it a key source of actionable intelligence for financial crime investigations.

Chart 4: Classification of general Fraud related SARs received by Sectors



	Accountants and Auditors	ADLAs	Auctioneers	Banks	Financial Intelligence Unit (FIUs)	Foreign Financial Intelligence Unit	Natural Person	Insurance/Investment Brokers	Law Enforcement Agencies	Legal Practitioners	Long Term Insurance Services	Micro Lenders	Money and Value Transfers (MVT's)	Motor Vehicle Dealerships	Real Estate Agencies/Agent	Short Term Insurance Services	Stock Brokers	Supervisory and Regulatory Bodies	Supervisory Bodies	Unit Trust Schemes
Case File opened	3	-	-	75	1	2	6	-	-	1	4	-	-	-	3	-	-	-	1	-
Low Priorty	-	2	1	179	2	1	-	5	1	2	-	1	1	2	1	2	4	1	-	3
Set-Aside	-	-	-	1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Under Cleansing	-	-	-	4	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

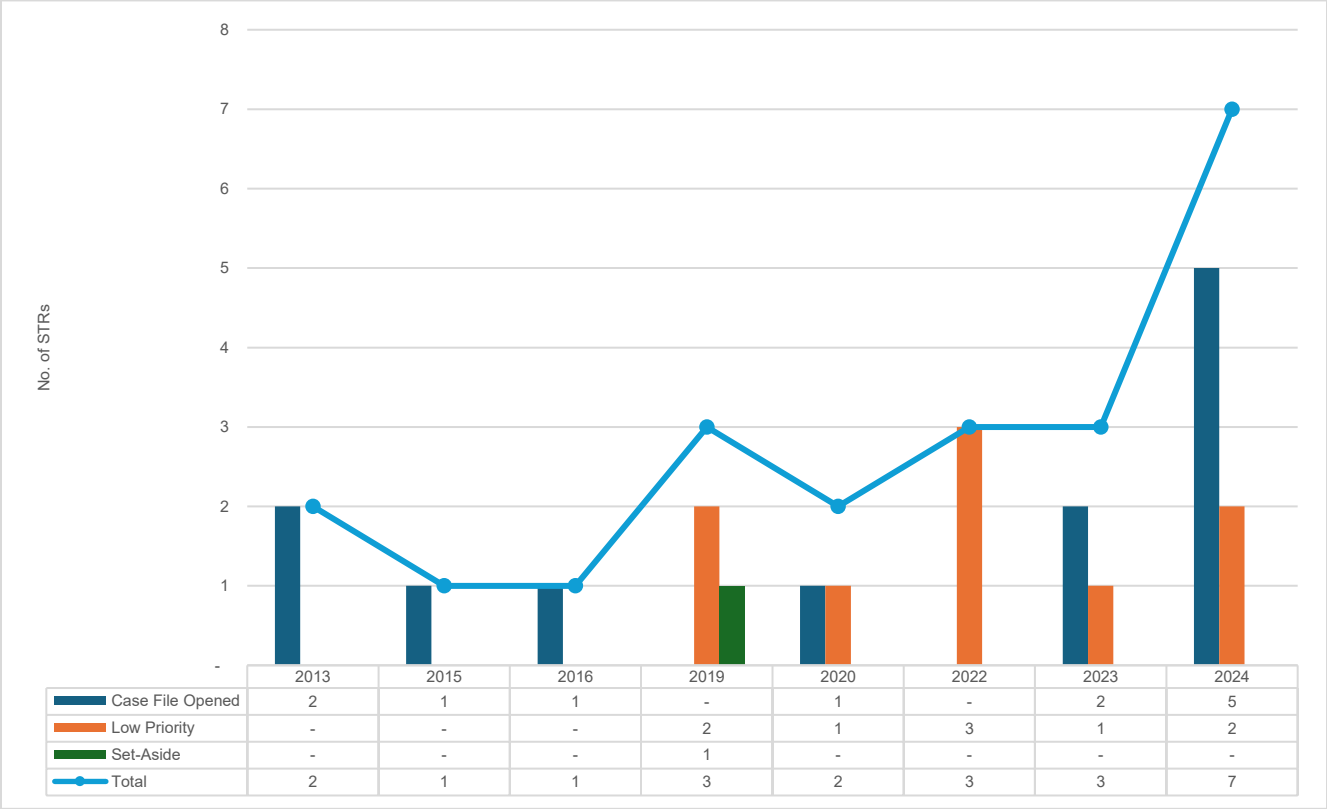
During the period under review, the FIC received a total of 311 fraud-related SARs from various reporting entities. A significant proportion of these reports, 208 SARs (67%), were assessed and categorized as *low priority*, meaning that although they contained potentially useful information, they did not present immediate or substantial indicators of financial crime risk. These reports are retained for record-keeping purposes and may be revisited should new intelligence or related cases emerge in the future.

Equally, 96 SARs (31%) were classified as *high priority* based on the severity, complexity, and potential impact of the suspicious activities reported. These SARs were escalated for further analysis, which involved the creation of case files, deeper investigative work, and potential collaboration with relevant domestic or international stakeholders. This prioritization process enables the FIC to allocate investigative resources effectively, ensuring that the most pressing threats to the financial system are addressed promptly.

6.2 OVERVIEW OF STRS, SARS, AND CASES RELATED TO INSURANCE FRAUD REPORTED TO FIC

This section provides an overview of STRs, SARs and cases related to possible insurance fraud filed by AIs and RIs. Such fraudulent practices undermine the integrity of the insurance industry, increase operational costs for insurers, and result in higher premiums for honest customers. Detecting and reporting suspicious activities through STRs and SARs helps regulatory bodies and enforcement agencies identify patterns of fraud, protect financial systems, and ensure compliance with anti-money laundering (AML) and counter-financing of terrorism (CFT) regulations.

Chart 5: Insurance fraud related STRs received from Sectors annually



	2013	2015	2016	2019	2020	2022	2023	2024
Case File Opened	2	1	1	-	1	-	2	5
Low Priority	-	-	-	2	1	3	1	2
Set-Aside	-	-	-	1	-	-	-	-
Total	2	1	1	3	2	3	3	7

It should be noted that no STRs relating to *insurance fraud* was reported prior to 2013. However, during the reporting period (2013 – 2024), 22 STRs were submitted by AIs and RIs. These STRs are formal submissions made when there is reasonable suspicion of fraudulent or illicit activities, and they form a critical part of the overall monitoring and enforcement framework.

Of the total STRs received:

a) 12 reports (more than half) were identified as being directly linked to insurance fraud. These were deemed high priority because of the seriousness, potential financial losses, and the risk they posed to the integrity of the financial system. Consequently, these cases were escalated for formal investigation or further enforcement action.
b) 9 reports were assessed as having a low risk or minimal impact. These were still documented and reviewed but did not meet the criteria for escalation. They may be monitored for patterns or future developments.
c) 1 report was set aside. This likely means that, after review, there was insufficient evidence or grounds to pursue the matter further, though it may still be kept on record for reference.

This distribution highlights that the majority of STRs in this period were actionable and insurance-related, underlining the sector's vulnerability to fraudulent schemes and the need for enhanced oversight. It also demonstrates that the review process includes prioritization, ensuring resources are focused on the highest-risk cases.

There were no SARs relating to insurance fraud reported during the period under review.

Table 1: Potential monetary values of related insurance fraud per annum

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Amount (NAD)	700,000.00	0.00	30,000.00	650.00	0.00	0.00	1,175,669.00	2,833,041.00	0.00	948,438.00	2,596,900	8,880,400.00

The figures presented in table 1 above are based on STRs and Spontaneous Disclosures (SDs) that were submitted to authorities in connection with suspected insurance fraud. These reports are part of the broader regulatory framework that obliges financial institutions and other reporting entities to flag potentially illicit activities for review.

The monetary values cited represent the potential financial impact of insurance fraud, as estimated in these reports. Over time, the reported values of these suspected fraudulent activities have fluctuated. This variation is due to factors such as the number of reports submitted each year, the complexity of the cases, and the monetary size of the transactions or claims being investigated. The FIC disseminated 12 Spontaneous Disclosure to Law Enforcement Agencies during the period under review.

In 2024, the highest total potential monetary value was recorded, amounting to NAD 8,8 million. This indicates that during that reporting year, insurance fraud cases either increased in number or involved larger amounts of money compared to previous years.

Since the introduction of reporting obligations up until 31 December 2024, the cumulative total potential monetary value of insurance fraud reported in SDs reached NAD 17,17 million. These SDs were subsequently escalated to relevant Law Enforcement Agencies (LEAs), notably the Namibia Police and the Office of the Prosecutor General (OPG) for further investigation and potential prosecution.

This shows the growing significance of SDs and STRs in identifying high-value insurance fraud risks and demonstrates how regulatory reporting serves as a key source of intelligence for law enforcement in Namibia’s financial crime prevention efforts.

SECTION C

7. TYPICAL REASONS FOR REPORTING TRANSACTIONS AS SUSPICIOUS

Reporting entities are expected to provide 'grounds for suspicion' when submitting STRs or SARs to the FIC. These grounds should reflect the offense or crime they suspect. The purpose of explaining why they find transactions or activities suspicious is to assist the FIC during analysis of such STRs. In the process of establishing such 'grounds for suspicion', institutions take into consideration various elements (red flags, modus operandi, indicators etc.) that collectively inform the formulation of a suspicious transaction or activity to be reported. Below are detailed list of typical red flags or indicators of insurance fraud in transactions. These indicators are widely used in compliance, auditing, and fraud detection programs to spot potentially suspicious activities in insurance sector.

Table 2: General potential indicators

🔍 **General Transaction-Related Red Flags**
a) **Frequent or Large Cash Payments**
4.3 Premiums or claim settlements made primarily in cash rather than traceable bank transactions.
4.4 Large cash amounts are inconsistent with the customer's known income or occupation.
b) **Multiple Premium Payments in Short Periods**
○ Several lump-sum payments or overpayments followed by refund requests.
○ Frequent policy upgrades or add-ons with little to no explanation.
c) **Premium Payments by Third Parties**
○ Payments made by someone unrelated to the policyholder, beneficiary, or insured party.
○ Multiple third parties pay for different policies on the same insured person.
d) **Overpayments and Refund Requests**
○ Policyholders deliberately overpay and request a refund, often to another account.
○ Frequent changes in payment method or beneficiary details.

e) **Unusual Payment Channels**

- Use of cryptocurrency, offshore accounts, prepaid debit cards, or money orders for premium or claim payments.

📄 **Policy Application Red Flags**

- **Inconsistent or Suspicious Personal Details**
  - Multiple policies under slightly different names, addresses, or IDs.
  - Fake or unverifiable contact information (phone numbers, emails, etc.).
- **High-Value Policies with No Clear Need**
  - Large coverage amounts are disproportionate to the applicant's income or lifestyle.
- **Rapid Policy Purchases**
  - Multiple policies purchased quickly, sometimes from different companies, without a clear financial rationale.
- **Last-Minute Policy Changes**
  - Frequent beneficiary changes shortly before a claim.
  - Sudden addition of riders or upgrades before a triggering event.

🚨 **Claims Submission Red Flags**

1. **Multiple Claims in a Short Period**
   a. Filing multiple claims across different insurers for similar or identical incidents.
2. **Claim Timing Concerns**
   - Claims filed very soon after policy issuance or just before expiry.
   - Sudden increase in claim activity after a premium increase or policy lapse warning.
3. **Inflated or Exaggerated Claims**
   a. Claim amounts that far exceed typical losses or damages for similar events.
   b. Extensive "soft tissue" injuries with minimal medical documentation.

4. **Missing or Inconsistent Documentation**

    a. Handwritten invoices, unverifiable repair receipts, or suspicious medical reports.

    b. Repeated submission of incomplete claim forms.

🏢 **Insured Asset or Incident Red Flags**

- **Over-Insured Assets**

    a. Coverage far beyond the asset's actual market value.

    b. Multiple overlapping policies for the same property or life.

- **Frequent Policy Cancellations**

    a. Canceling policies after making claims or obtaining refunds.

- **Unverifiable Incident Details**

3.1 Lack of police reports, witness statements, or supporting evidence for incidents.

3.2 Damage or loss reported long after the alleged incident occurred.

👥 **Behavioral and Customer-Interaction Red Flags**

1. **Evasive or Defensive Behavior**

    a. Policyholders avoid providing documentation or pressure for fast payouts.

2. **Excessive Knowledge of Insurance Processes**

    a. Customers demonstrate insider-level knowledge of claims processes, possibly indicating organized fraud.

3. **Suspicious Relationships Between Parties**

    8.1 Same address or contact information across multiple unrelated policies.

    8.2 Collusion suspected between insured, medical providers, repair shops, or agents.

🕵️ **Broker/Agent Red Flags**

1. **High Volume of Suspicious Business from One Agent**

    - Disproportionate number of early claims from policies sold by a single broker.

2. **Agent Involvement in Beneficiary or Payout Discussions**

○ Broker influencing claims or payout processes beyond normal responsibilities.
🧩 **Transaction Pattern Red Flags (AML/CFT Overlap)**
a. **Structuring Payments**
○ Premiums or settlements broken into smaller transactions to avoid reporting thresholds.
b. **Cross-Border Transactions**
○ Unnecessary use of offshore or foreign bank accounts for claim payments.
c. **Round-Tripping Funds**
a. Premiums paid from a third party's account and claim payouts going back to the same party.

It is worth noting that red flags do not confirm fraud on their own but help insurers, auditors, and investigators trigger enhanced due diligence. Typically, investigators look for patterns, such as:

1. Early or frequent high-value claims.
2. Untraceable or third-party payments.
3. Complex ownership structures or connections between insured and service providers.

SECTION D

8. SAMPLED CASE STUDIES

The FIC observed that in ML activities, perpetrators continue to explore and exploit new methods of hiding or concealing the illicit origins of funds. Insurance products, due to their dual nature of providing both financial protection and investment opportunities, have become increasingly vulnerable to misuse by criminals. Fraudulent activities within the insurance sector can weaken financial integrity and may create avenues for ML and TF.

It is therefore crucial that accountable and reporting institutions in the insurance sector consistently conduct thorough risk assessments of their products, services, distribution channels, and customers. Such assessments should inform the development of strong internal controls, tailored monitoring systems, and enhanced due diligence measures. A proactive, risk-based approach is necessary to effectively combat ML/TF/PF threats within the insurance industry.

The following case studies, drawn from open source and analyzed reports, highlight notable insurance-related ML and fraud typologies:

Case Study 1: Syndicate Defrauding Insurance Companies through Fake Death Claims

A Suspicious Transaction Report (STR) filed by Bank-C revealed what appears to be a prevailing fraud syndicate targeting insurance companies through life and funeral policies by faking the deaths of unsuspecting individuals.

In this matter, the subject Mr. N took out several funeral covers on his alleged fiancée (Ms. F) during October 2023. On 01 April 2024, Mr. N submitted a claim, stating that Ms. F had died in a motor vehicle accident on the same date.

The claimant submitted all the required documentation. However, information within our domain suggests that these documents may have been forged, and that the identity card used to open the policies may have been stolen.

Modus Operandi

- The perpetrators take out life/funeral policies covering alleged relatives, where the perpetrator is listed as the beneficiary.
- A bank account is opened in the name of the beneficiary, from which monthly premiums are consistently paid throughout the grace period (normally six (6) months).
- Shortly after the grace period, the covered relative is declared dead, often due to a motor vehicle accident.
- The beneficiary then submits the required documents to initiate the insurance claim, including:
    - Death certificate
    - Certified copy of the deceased's ID
    - Certified copy of the beneficiary's ID
    - Medical certificate of cause of death
    - Medico-legal postmortem examination report
    - Namibia road accident report form

Affected Companies

The analysis indicates that the following insurance companies have fallen victim to the scheme:

i. Company-A Namibia (Pty) Ltd
ii. Company-B Namibia (Pty) Ltd
iii. Company-C Namibia (Pty) Ltd

Analysis suggests that multiple insurers could have been exposed to this fraud.

Suspected Syndicate Members

The scheme suggests collusion among multiple actors, including professionals whose roles provide access to critical documents and processes **(e.g., medical, civil registration, financial, or insurance officials)**. These roles, if exploited, may enable fraudulent claims:

- Police officers and doctors, who falsely declare deaths
- Home Affairs officials, who issue fraudulent death certificates
- Insurance company staff involved in processing claims
- The insured person themselves, in some cases
- Bank officials, who may facilitate fraudulent account openings

Outcome of Analysis

- The analysis of STR filed with FIC shows strong indicators of fraud.
- Account 00000285 held at Bank-C in the name of Mr. N (Beneficiary) was restricted.
- Intelligence was shared with law enforcement agencies.
- After engagement with the FIC, Company-A Namibia (Pty) Ltd reviewed both new and old motor vehicle accident claims. This led to:
  - Four (4) suspicious reports filed.
  - Seven (7) criminal investigations initiated with the Namibian Police.
- The Prosecutor General (PG) successfully secured a Preservation Order amounting to NAD 438,632.18.

Red Flags Observed

The following red-flag indicators were noted during the investigation:

- New bank accounts opened almost at the same time as the policies.
- Limited accounts' activity, with transactions mostly consisting of monthly premium payments.
- After claims were paid, no funeral-related expenditures were observed.
- Withdrawals via ATMs only, raising suspicion that accounts may have been opened with stolen identity cards.
- Inter-bank transfers with vague or concealed descriptions to hide the source of funds.

- ❖ Each claim involves different accounts, individuals, and/or banks, making it challenging to link all role players directly.

Analytical Insight

- This case demonstrates how weaknesses in civil registration systems (identity documents, death certificates) and limited verification by insurers can be systematically exploited.
- The collusion of multiple actors; including police, health officials, and insurance staff, highlights the interconnected vulnerabilities across both public and private institutions.
- From an AML/CFT perspective, the absence of funeral-related expenditures and the use of ATMs for withdrawals are strong indicators of layering attempts.
- This typology suggests that fraudulent claims should not be viewed in isolation but as part of broader syndicate operations that can move significant sums through the financial system undetected.
- Strengthening cross-agency data validation and enhancing insurer due diligence on death claims would reduce exposure to both fraud and money laundering risks.

Case Study 2: Early Policy Surrender (Laundering via Life Insurance)

A policyholder purchased a single premium life insurance product worth N$500,000, paid entirely in cash. Within three months, the policy was surrendered, and the customer willingly accepted a 15% penalty on the surrender value. The payout of approximately N$425,000 was transferred into the customer's bank account, giving the impression that the funds originated from a reputable insurer.

- **Indicators:** Large cash payment for policy; early surrender without financial necessity; acceptance of penalties.

Analytical Insight

- The policyholder purchased a single-premium life insurance product valued at N$500,000, paid entirely in cash — an immediate red flag, given the high amount and lack of financing traceability.
- The policy was surrendered within three months, far earlier than would be typical for a legitimate investment or protection purpose.

- The customer accepted a 15% early surrender penalty, indicating a willingness to incur financial loss, which is inconsistent with rational investment behavior.
- The surrender proceeds (N$425,000) were transferred to the customer's bank account by a reputable insurer, effectively converting the initial cash into what appears to be legitimate funds.
- This activity likely forms part of the layering stage, where illicit funds are moved through legitimate financial products to disguise their origin. The surrender payout from the insurer serves as a "cleansed" source of funds, enhancing the appearance of legitimacy when reintroduced into the banking system.

Case Study 3: Overpayment of Premiums and Refunds

An insurance company detected multiple cases where a client consistently overpaid their policy premiums by significant margins (sometimes double or triple the required amount). After each overpayment, the client requested a refund, which was issued via electronic funds transfer into a different bank account than the one originally used. This process disguised the true origin of funds and allowed the client to "clean" illicit money through refunds.

- **Indicators:** Pattern of repeated overpayments; refund requests to unrelated bank accounts; customer unwilling to explain overpayment.

Analytical Insight

- The client's pattern of consistent overpayment and subsequent refund requests indicates possible money laundering activity.
- The overpayments serve as a method to introduce illicit funds into the insurance system under the guise of premium payments.
- Requesting refunds to different bank accounts suggests an intentional effort to obscure the money trail and change the apparent source of funds.
- The refunds processed via EFT from a reputable insurer create the illusion of legitimate proceeds.
- The repetitive nature of the transactions strengthens suspicion of deliberate misuse of insurance processes for layering purposes.

- This behavior is inconsistent with normal policyholder conduct, as genuine clients rarely overpay premiums repeatedly.
- The activity reflects a typical layering technique, converting suspicious cash or illicit funds into traceable, “clean” electronic transfers.

Case Study 4: Misuse of Insurance Brokers

An intermediary was found to be assisting clients in obtaining high-value insurance policies using falsified identity documents. These policies were later used as collateral for bank loans. Once the loans were disbursed, the policyholders defaulted, leaving insurers and banks exposed while successfully introducing illicit funds into the financial system. Investigations revealed that the broker received unusually high commissions and was connected to multiple high-risk clients.

- **Indicators:** Broker involved with numerous suspicious customers; irregularities in identification; use of policies as collateral followed by default.

Analytical Insight

- The intermediary facilitated insurance policy acquisitions using falsified identities, indicating possible fraud and money laundering.
- The use of fake documents suggests deliberate concealment of the true identity and source of funds.
- Policies were used as collateral for bank loans, enabling clients to access and integrate illicit money into the financial system.
- Following disbursement, the clients defaulted on the loans, causing losses to both insurers and banks.
- This pattern shows collusion between the broker and clients to exploit insurance and banking channels.
- The broker’s unusually high commissions and links to high-risk clients reinforce suspicions of active involvement.

The conduct reflects a complex layering and integration scheme, using insurance products and loans to legitimize illicit proceeds.

Case Study 5: Fraudulent Claims

A policyholder insured a vehicle valued at N$250,000 and reported its theft less than three months later. Investigations revealed that the theft was staged, and the vehicle had been deliberately sold outside the country. The insurance payout was used to purchase real estate, integrating illicit funds into legitimate assets.

- Indicators: Claim made soon after policy inception; staged or unverifiable incident; immediate reinvestment of payouts into high-value assets.

Analytical Insight

- The policyholder's actions indicate a fraudulent insurance claim intended to facilitate money laundering.
- The vehicle theft was staged, showing deliberate deception to obtain insurance proceeds.
- Evidence confirmed the vehicle was illegally sold outside the country, generating illicit income.
- The insurance payout provided a legitimate cover for these illegal proceeds.
- Funds were then used to purchase real estate, a common integration method in money laundering.
- The short period between policy inception and claim submission raises strong suspicion of premeditated fraud.
- The activity demonstrates misuse of insurance for criminal gain and conversion of illicit funds into legitimate assets.

Case Study 6: Cross-Border Policy Purchases

A Namibian citizen purchased multiple life insurance policies from providers in neighboring countries, paying premiums in U.S. dollars. Beneficiaries were listed in high-risk jurisdictions with no clear relationship with the policyholder. Upon surrender, the payout was remitted

abroad, effectively transferring illicit funds across borders under the guise of legitimate insurance transactions.

- **Indicators:** Cross-border policies without clear rationale; use of foreign currencies; beneficiaries in high-risk countries.

Analytical Insight

- The policyholder's actions indicate possible cross-border money laundering through misuse of life insurance products.
- Purchasing multiple foreign policies and paying in U.S. dollars suggests an intent to move funds offshore.
- Listing beneficiaries in high-risk jurisdictions with no clear relationship raises serious red flags.
- The foreign surrender payouts facilitated the transfer of illicit funds abroad under the appearance of legitimacy.
- This pattern reflects layering and integration stages of money laundering.
- The use of multiple insurers and foreign currencies demonstrates efforts to obscure fund origins and evade detection.
- The case shows exploitation of regulatory gaps between jurisdictions for laundering purposes

Case Study 7: Integration through High-Value Annuities

An individual invested N$2 million in a lump-sum annuity, funded through multiple cash deposits made just below reporting thresholds. The product was structured to pay out monthly income over 10 years. Investigations suggested the funds originated from illicit activities, but once integrated into regular annuity payouts, the funds appeared legitimate.

- **Indicators:** Structured cash deposits below thresholds; large lump-sum contributions inconsistent with income profile; annuity payments used to justify lifestyle.

Analytical Insight

- The client's behavior indicates structuring and money laundering through an annuity product.
- The multiple cash deposits below reporting thresholds suggest deliberate avoidance of detection.
- The lump-sum annuity investment served to introduce illicit cash into the financial system.
- By converting the funds into monthly income payouts, the client effectively legitimized illicit proceeds.
- The annuity structure provides a steady stream of "clean" income, masking the criminal origin of the funds.
- The pattern of deposits and investment timing is inconsistent with normal financial planning behavior.
- This case reflects the stage of integration of money laundering, where illegal funds are absorbed into legitimate assets.

9. LESSONS AND RECOMMENDATIONS

Insurance products can be misused as tools for money laundering and fraud. Criminals exploit life policies, annuities, and claim processes to introduce, layer, and integrate illicit funds under the guise of legitimate transactions. Common red flags include early policy surrenders, overpayments and refunds, use of falsified identities, cross-border premium payments, and claims involving staged events. These schemes not only distort the integrity of the insurance sector but also expose insurers to regulatory, financial, and reputational risks. Below are key lessons and possible recommendations:

Key Lessons

a. **Early detection saves millions** — proactive analytics and pattern recognition are more effective than post-event investigations.

b. **Timely filing of Suspicious Transaction and Activity Reports** is crucial. Delays in filing can allow criminals to move funds beyond reach.
c. Criminals **exploit** both legitimate policy benefits (surrenders, claims, annuities) and **operational weaknesses** such as complexity in policy terms, claims processes, and weak verification systems as well as brokers, refunds) to launder illicit funds.
d. **Multiple policies** taken out shortly before a claim event.
e. Identify and verify premiums paid in cash or from **unrelated third parties**.
f. Identify and verify beneficiaries with **no apparent connection** to the insured.
g. There is a **direct link between insurance fraud and other financial crimes** — including money laundering and corruption (e.g. using claims to legitimize illicit funds).
h. **Inter-agency collaboration** between FIC, Insurers, and Law Enforcement enhances prevention through timely sharing of intelligence.

Recommendations:

a. **Insurance institutions must strengthen KYC/CDD Measures:** Verify clients' identities, sources of funds, and beneficial ownership before policy issuance or payout and report suspicious activities promptly to the FIC.
b. **Implement Transaction Monitoring:** Detect unusual patterns such as early surrenders, frequent overpayments, or premium payments from unrelated parties.
c. **Train Staff Regularly:** Ensure employees understand insurance-related ML/TF typologies and can identify suspicious indicators.
d. **Strengthen Intermediary Oversight:** Monitor brokers and agents for irregular commission structures or links to high-risk clients.
e. **Collaborate with Regulators and FIUs:** Share intelligence on emerging typologies and suspicious activities for coordinated responses.
f. **File STRs Promptly:** Report any suspicious transactions or activities in line with AML/CFT requirements.
g. **Consider** central tools such as **data analytics and technology**.
h. **Public awareness** campaigns can deter opportunistic fraud and encourage whistleblowing.

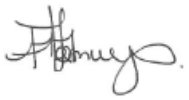
10. CONCLUSION

The analysis of sampled cases demonstrates that the insurance sector remains vulnerable to exploitation by criminals seeking to launder illicit proceeds or commit fraudulent activities for personal gain. Typologies such as early policy surrenders, overpayments and refunds, misuse of intermediaries, fraudulent claims, and cross-border policy purchases reveal the diverse methods used to disguise, move, and integrate illicit funds into the financial system.

Insurance fraud poses risks to the stability and credibility of the sector and may lead to financial, reputational, and regulatory challenges for reporting institutions. Addressing these challenges requires more than just compliance it demands a proactive, risk-based approach that incorporates robust customer due diligence, enhanced transaction monitoring, strict oversight of intermediaries, and timely reporting of suspicious activities to the FIC.

Ultimately, the effective detection and prevention of insurance-related ML and fraud rely on collaboration among insurers, regulators, LEAs, and the FIC. By strengthening awareness, enhancing institutional capacity, and fostering cooperation, Namibia's insurance sector can be better protected against financial crime threats, thereby safeguarding the integrity of the broader financial system.

This report is produced by the FIC's Strategic Analysis Section. For inquiries and communication, please contact helpdesk@fic.na. Similar studies on potential insurance fraud-related offences will be updated periodically when the need arises.



Ms. Melintha Fleermuys
Acting General Manager: Analysis and Law Enforcement Department