



Q4

QUARTERLY STATISTICS REPORT

OCTOBER - DECEMBER 2023

Financial Intelligence Agency

Bermuda

QUARTERLY REPORT

October 1st to December 30th, 2023

1.0 Table of Contents

1.0 Introduction	4
2.0 Incoming Reports & Requests	4
3.0 SARs/STRs Reporting.....	4
3.1 SARs / STRs by Reporting Sector.....	4
3.2 SARs/STRs by Monetary values.....	5
3.3 SARs/STRs by Suspected Offences.....	5
4.0 International and Domestic Cooperation.....	5
4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs).....	5
4.2 Outgoing Requests for Information (Domestic & International)	6
5.0 Consent Letters.....	6
6.0 Intelligence Reports (Response / Spontaneous Disclosures).....	6
6.1 Outgoing Disclosures.....	6
7.0 Reporting Sector Filing Breakdown.....	7
7.1 Reporting Sector: Banks	7
Classification: Fraud.....	7
7.2 Reporting Sector: Digital Asset Businesses	9
7.3 Reporting Sector: Fund Administrator	9
7.4 Reporting Sector: Money Service Businesses	10
7.5 Reporting Sector: Real Estate	10
7.6 Reporting Sector: Securities: Investment Businesses	10
7.7 Reporting Sector: Long Term Insurers	11
7.8 Reporting Sector: Insurance Company.....	11
8.0 Key Report Indicators	11

KEY STATISTICS

Total Incoming Reports

245

Highest Reporting Sector

DABs

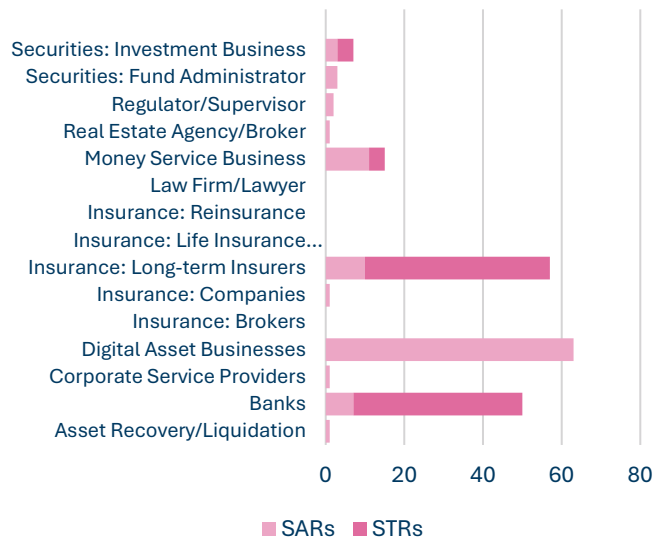
Total Monetary Values

\$24,912,081.00

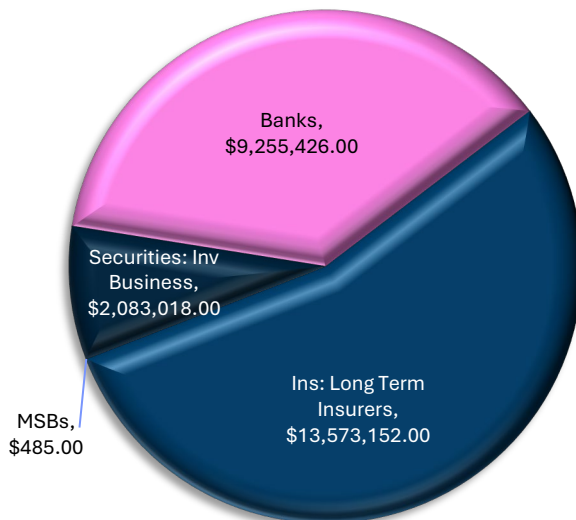
Q4 2023 Reporting (Q3 Comparison)

●	AIFs		▼	-100%
●	C-SARs			
●	C_STRs			
●	CTRs	1	▲	n/a
●	IRIs	14	▼	-18%
●	SARs	103	▼	-4%
●	STRs	98	▼	-6%
●	UIRs	29	▼	-29%

Largest Reporting Sectors



Highest Monetary Values



Glossary

ACRONYM	MEANING
AIF	Additional Information Files
C-SAR	Consent SAR Requests
C-STR	Consent STRs
DAB	Digital Asset Business
IRI	Incoming Requests for Information
LTI	Long Term Insurers
ORI	Outgoing Requests - International
ORD	Outgoing Requests - Domestic
NRA	National Risk Assessment
S16	Section 16 Requests
SAR	Suspicious Activity Reports
STR	Suspicious Transaction Reports
UIR	Unsolicited Intelligence Reports

1.0 Introduction

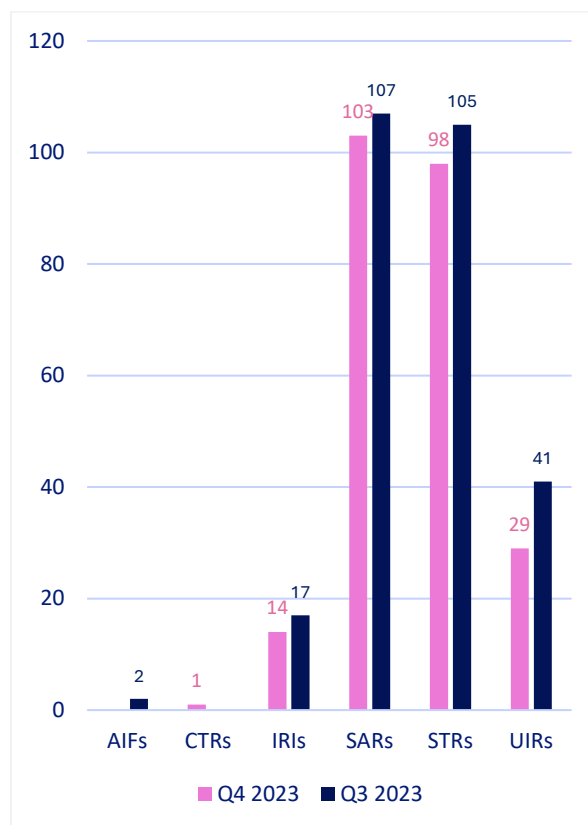
The FIA Bermuda presents its Q4 2023 quarterly report. For this period, the FIA received a total of 245 incoming reports, reflecting a moderate decline in overall volumes compared to Q3 but continued robust reporting across key sectors. Digital Asset Businesses (DABs) remained the highest filing sector, while Long-Term Insurers (LTIs) and banks together accounted for the bulk of reported monetary values, contributing to a combined total of \$24,912,081.00. Although SARs, STRs, IRIs and UIRs all decreased quarter-on-quarter, reporting activity continued to highlight significant financial crime risks, with sanctions-related matters, money laundering (including cash exchange activity), fraud and tax offences featuring prominently. Q4 also saw sustained engagement with domestic law enforcement, supervisors and international FIUs through incoming and outgoing RFIs and a high volume of spontaneous disclosures, alongside the introduction of consent letters to support transaction decision-making by reporting entities. Overall, Q4 2023 underscores a slightly reduced but still elevated level of detection, cooperation and analytical output as FIA Bermuda continues to address complex and evolving AML/CFT and sanctions risks.

2.0 Incoming Reports & Requests

In Q4 2023, FIA Bermuda saw notable changes compared to Q3 2023. IRIs decreased from 17 to 14 (-17% decline), SARs dropped from 107 to 103 (-4% decline), and STRs fell from 105 to 98 (-7% decline). UIRs showed the largest reduction, moving from 41 to 29 (-29% decline). CTR submissions, which were 1 in

Q3, dropped to 0 (100% decline), while AIFs remained absent after 2 in Q3 (100% decline). Overall, Q4 reflects a downward trend across most reporting categories.

Chart 1 - Reports received by FIA for Q4 2023 vs Q3 2023



Source: FIA (2023)

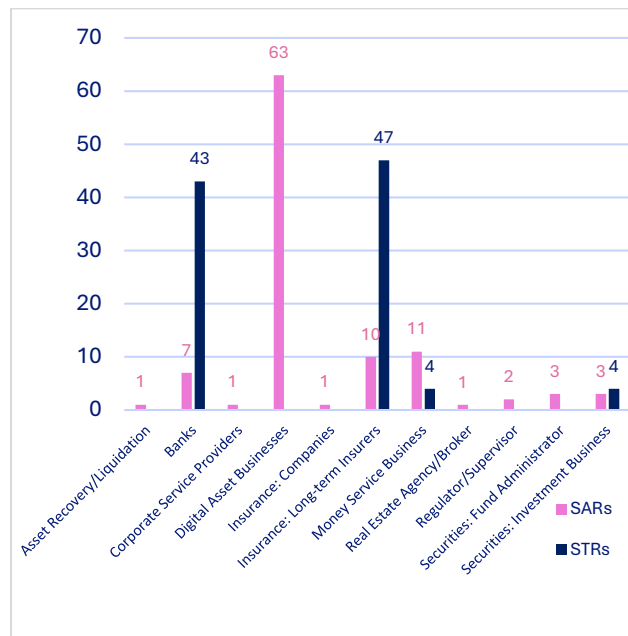
3.0 SARs/STRs Reporting

3.1 SARs / STRs by Reporting Sector

In Q4 2023, FIA received a total of 103 SARs and 98 STRs across all reporting sectors. DABs were the largest contributor to SARs with 63 reports, while LTIs led STR submissions with 47 reports. Banks also played a significant role, accounting for 7 SARs and 43 STRs. Other notable contributors

included MSBs and Securities sectors, though their volumes were comparatively lower.

Chart 2 - SARs / STRs submitted to FIA by Agency Type Q4 2023



Source: FIA (2023)

3.2 SARs/STRs by Monetary values

In Q4 2023, the total monetary value reported through SARs and STRs across all sectors amounted to \$24,912,081.00. The largest share came from LTIs, contributing \$13,573,152.00, followed by Banks with \$9,255,426.00, and Securities: Investment Business with \$2,083,018.00. Other sectors, including Money Service Businesses, reported negligible amounts (\$485.00), while most sectors recorded zero monetary values, highlighting a concentration of high-value reports within a few key financial sectors.

3.3 SARs/STRs by Suspected Offences

In Q4 2023, FIA Bermuda recorded a total of 103 SARs and 98 STRs linked to suspected crime offences. The leading category for SARs

was Sanctions Related with 37 reports, while Money Laundering topped STR filings with 47 reports. Other significant contributors included Fraud (24 SARs, 23 STRs) and Corruption (1 SAR, 6 STRs). Money Laundering-related offences collectively accounted for the highest combined volume, emphasizing its prominence in reported activities.

Table 1 – SAR/STR filing by suspected crime offences in Q4 2023

#	Crime Classification	SARs	STRs
1.	Abnormal Activity	1	1
2.	Bribery	1	
3.	Corruption	1	6
4.	Fraud	24	23
5.	Human Trafficking	1	2
6.	Insider Trading (Market Abuse)		3
7.	Money Laundering	32	47
8.	Money Laundering – Cash Exchange Related		13
9.	Money Laundering – Crypto Related		
10.	Narcotics		
11.	Sanctions Related	37	
12.	Sexual Exploitation		
13.	Tax Offences	4	2
14.	Terrorist Financing	2	1
	TOTAL	103	98

Source: FIA (2023)

4.0 International and Domestic Cooperation

4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs)

In Q4 2023, FIA Bermuda received a total of 43 incoming requests and reports, comprising 14 IRIs and 29 UIRs. Among IRIs, Egmont (FFIUs) accounted for 4 requests from jurisdictions including Qatar, South Africa, UK, and USA, while Local Law Enforcement (LLEAs)

submitted 9 requests (8 from BPS and 1 from HM Customs), and Supervisor/Regulator (BMA) contributed 1 request. For UIRs, LLEAs – primarily HM Customs for this quarter) was the main source with 26 filings; Egmont partners submitted 3 reports from Cayman, Germany, and Luxembourg. These figures highlight strong engagement from law enforcement and international FIU counterparts during the quarter.

Table 2 Incoming IRIs / UIRs in Q4 2023

Reporting Sector	# of Filings
IRIs	
Egmont (FFIUs)	4 (Qatar, South Africa, UK, USA)
Local Law Enforcement	9 (BPS (8), HM Customs (1))
Supervisor/Regulator	1 (BMA)
UIRs	
Local Law Enforcement	26 (HM Customs)
Egmont (FFIUs)	3 (Cayman, Germany, Luxembourg)
TOTAL	43

Source: FIA (2023)

4.2 Outgoing Requests for Information (Domestic & International)

In Q4 2023, FIA Bermuda disseminated a total of 44 outgoing requests. The majority were Section 16 Requests to domestic reporting entities, totaling 28 filings, followed by 11 outgoing requests to domestic competent authorities. Additionally, 5 international RFIs were issued to counterparts in BVI, Colombia, Taiwan, UK, and USA, reflecting continued engagement with both local and international stakeholders.

Table 3 Outgoing RFIs disseminated in Q4 2023

Report Types		# of Filings
1.	Section 16 Requests (Reporting Entities - Domestic)	28
2.	Outgoing Requests for Domestic (Competent Authorities)	11
3.	Outgoing Requests for Information (International)	5 (BVI, Colombia, Taiwan, UK, USA)

Source: FIA (2023)

5.0 Consent Letters

During Q4 2023, the FIA initiated the practice of issuing Consent Letters to reporting entities that submitted SARs/STRs and sought approval for transactions or activities deemed suspicious. For this period, the FIA issued 3 letters of consent in response to three incoming reports, which originated from both LTIs and Securities: Investment Business companies. This development reflects an important step in enhancing communication and compliance processes between the FIA and reporting entities.

6.0 Intelligence Reports (Response / Spontaneous Disclosures)

6.1 Outgoing Disclosures

In Q4 2023, FIA Bermuda disseminated a total of 44 outgoing reports across various disclosure types. The majority were Spontaneous Disclosures to LLEAs, totaling 26 filings directed at BPS and HM Customs. Additionally, 11 Spontaneous Disclosures to Egmont FIUs were issued to jurisdictions including Bahamas, BVI, Colombia, Hong Kong, Isle of Man, Switzerland, Thailand, UK,

and USA. Response Disclosures accounted for 6 reports, comprising 4 to Egmont FIUs (Barbados, BVI, USA, Qatar) and 2 to Local LEAs, while Spontaneous Disclosures to Local Competent Authorities included 1 filing to BMA. These figures underscore strong engagement with both domestic law enforcement and international FIU counterparts during the quarter.

Table 4 Outgoing Report Types disseminated in Q4 2023

Report Types		# of Filings
1.	Response Disclosures to Local Competent Authorities	0
2.	Response Disclosures to Local LEAs	2
3.	Response Disclosures to Egmont FIUs	4 (Barbados, BVI, USA, Qatar)
4.	Spontaneous Disclosures to Local Competent Authorities	1 (BMA)
5.	Spontaneous Disclosures to Local LEAs	26 (BPS, HMS Customs)
6.	Spontaneous Disclosures to Egmont FIUs	11 (Bahamas, BVI, Colombia, Hong Kong, Isle of Man, Switzerland, Thailand, UK, USA)

Source: FIA (2023)

7.0 Reporting Sector Filing Breakdown

A breakdown of SAR/STR filings according to reporting sector, crime classifications and other characteristics are shown below.

7.1 Reporting Sector: Banks

Classification: Fraud

During Q4 2023, several red flags of suspected fraud were identified within the banking sector. Phishing (Imposter Scam) was reported in one case where a caller impersonated an employee of One

Communications, a Bermuda based internet / mobile provider, claiming to assist with an internet line issue. The victim granted remote access to her device and was persuaded to log into her bank account under the pretext of receiving a refund. The fraudster then attempted to initiate a wire transfer from her account. Business Email Compromise incidents were also reported, involving fraudulent instructions that resulted in funds being sent to unauthorized beneficiaries, with recovery efforts still ongoing. Elder Abuse Fraud cases highlighted compromised bank accounts involving family members and caregivers. Additionally, one case of Ransom Payment/Extortion was noted, where a local charity paid a ransom settlement on behalf of an individual located overseas. Overall, these filings underscore the evolving nature of fraud typologies and the need for heightened vigilance across banking operations.

Classification: Money Laundering

Multiple red flags of suspected money laundering were identified within the banking sector. Cases included customers conducting internal transfers to fund gambling activities on BET365, for individuals linked to adverse media involving drug charges and gang activity. BET365 is a British online gambling company that offers betting and gaming products to customers globally. Other indicators involved accounts receiving excessive amounts of USD for storage in safe deposit boxes, large unexplained cash deposits inconsistent with declared income, and transactions lacking supporting documentation for claimed sources such as rental income. Several clients exhibited patterns of structuring and smurfing,

including frequent small deposits followed by rapid withdrawals or transfers to third parties, often linked to suspected gambling rings. Businesses were also flagged for misusing accounts, such as sending and receiving funds through personal accounts instead of associated entities and using business funds for private purposes like home construction. Additional concerns included joint accounts with substantial cash deposits withdrawn in rounded amounts, reluctance to provide KYC documentation, and evasive explanations regarding employment and source of wealth. In some cases, adverse media linked customers to illegal employment practices and possible immigration violations.

In response to these findings, banks have terminated or initiated termination of relationships with clients exhibiting high-risk behaviors and non-compliance with KYC requirements.

Classification: Money Laundering Involving Cash Exchanges

In Q4 2023, twenty-six filings highlighted suspected money laundering linked to cash exchange activities, with patterns such as transactions inconsistent with client profiles, multiple bank branches visited on the same day, and cash deposits withdrawn immediately after being credited. Clients often refused to provide source of funds documentation, displayed anxious behavior, and structured transactions below the \$5,000.00 reporting threshold. USD remained the dominant currency exchanged, followed by CAD. Other indicators included joint accounts used for exchanges, reliance on third parties to complete transactions, and unusual customer behavior such as avoiding eye contact or demanding leftover change in

cash rather than leaving it in the account. Several cases involved clients with insufficient income to justify the volume of exchanges, and one client receiving government financial assistance while conducting frequent foreign currency exchanges. Surveillance footage at reporting entities confirmed that some customers coordinated exchanges with the same third party across different branches. Individuals involved were primarily employed in low-income or cash-intensive roles such as housekeeper, cleaner, porter, construction worker, tour guide, dental assistant, courier, cashier, and maintenance worker, with some unemployed. Most were previously known to the BPS or had prior reports of suspicious activity filed by local banks. These filings resulted in one client relationship being terminated and two others recommended for exit. USD remains the dominant currency for exchanges, reinforcing the need for enhanced monitoring.

Classification: Tax Offences

One incident involving suspected tax offences was reported during the quarter, where a potential customer refused to provide tax information required under applicable regulations, declined to disclose ownership structures of intermediary companies to identify beneficial owners, and failed to submit certified documents such as an organizational chart necessary for compliance with banking requirements. These actions raised concerns about transparency and regulatory adherence. The filing included key indicators such as declined or refused business due to suspected criminal activity, first-time customer, inadequate or evasive explanations, refusal to comply with

KYC requirements, and tax offences, signaling significant risk for non-compliance and potential illicit activity.

Classification: Investment-related Fraud and Market Abuse

One incident reported during the quarter involved suspected investment-related fraud and market abuse, where a SAR was filed following adverse media linking the entity and its ultimate beneficial owners (UBOs) to a trade manipulation scheme executed through an offshore company using overseas traders. Transaction reviews revealed that funds were received from the UBO's company and either immediately transferred back to the UBOs without any trades, paid to unlicensed investment traders in potential breach of SEC regulations, or routed to high-risk jurisdictions associated with tax evasion without a clear business purpose. These activities raised concerns of investment scams, market manipulation, and possible violations of U.S. tax and securities laws.

7.2 Reporting Sector: Digital Asset Businesses

Classification: Investment-related Fraud and Market Abuse

During the quarter, suspected fraud within the DAB sector included a major incident where a company reported an attack resulting in the theft of fifty million tokens, later deposited at a DAB. Additional red flags included direct exposure to addresses linked to fraud shops such as "Btc2pm.me - PinPays - UAPS", accounts appearing commonly controlled due to shared IP addresses and similar activity, and a user identified as a true match

to an individual previously convicted of tax fraud. Other concerns involved account compromise through unauthorized IP access, attempted deposits using credit cards not belonging to the customer, and blockchain analytics identifying clusters associated with stolen funds.

Classification: Sanctions

Sanction-related filings by DABs revealed both direct and indirect exposure to sanctioned entities and jurisdictions. These included transactions linked to Garantex.io, Tornado.cash, HDPay.ir, and Nobitex.ir, as well as sanctioned jurisdictions such as Iran and Russia. Indirect exposure was also noted to addresses associated with SurBitcoin, an OFAC-sanctioned Venezuelan crypto exchange. These findings highlight significant compliance risks related to international sanctions and the need for enhanced screening measures.

7.3 Reporting Sector: Fund Administrator

During the quarter, one filing from the Fund Administrator sector involved suspected fraudulent activity. Red flags included a forged signature on a resolution authorizing a transfer of shares, executed by an individual holding power of attorney on behalf of an investor. Adverse media findings indicate that the subject appeared to be under investigation in the USA for bank fraud, wire fraud, and money laundering. Further concerns arose from inconsistent account activity, including the investor changing bank accounts four times within four years.

7.4 Reporting Sector: Money Service Businesses

During the quarter, filings from the MSB sector revealed red flags of both suspected money laundering and fraud. Money laundering indicators included erratic sending patterns, customers providing recipient details on scraps of paper, evasive behavior when asked for additional information, and reliance on third parties to complete transactions. Several customers alternated between branches, split transactions to avoid detection, and became defensive when questioned about the purpose of transfers or source of funds. Bundled cash in small denominations and vague explanations such as “rent money” further raised concerns. Fraud-related filings highlighted patterns of customers sending funds to multiple locations for loan payments or to individuals with no verifiable ties, often while communicating with unknown parties during transactions. Additional red flags included unsatisfactory explanations for source of funds, suspicious WhatsApp messages referencing bank details and package deliveries, and attempts to send money to foreign contacts for implausible reasons such as grocery purchases. These behaviors, combined with prior blocks and resurfacing suspect activity, underscore significant risks of scams and illicit financial flows within the MSB sector.

Transactions during the quarter involved destination countries such as Nigeria, Jamaica, Dominican Republic, USA (California and Florida), Colombia, Luxembourg, El Salvador, Ireland, Netherlands, Spain, France, Costa Rica, Thailand, UK, and India, reflecting a broad international footprint. Despite the low

number of filings, this was largely due to transactions being cancelled and local senders blocked for suspicious activity. Notably, some recipients were previously known to the FIA through filings from other reporting sectors, and it is suspected that certain transactions disguised as scams—such as sweetheart scams—were actually intended to facilitate money laundering. Emerging patterns suggest that local senders may be deliberately routing funds through less commonly reported countries to obscure the trail before reaching the intended recipient, highlighting the complexity and global reach of these criminal networks. Six individuals were identified as first-time customers, and approximately one-third of transactions were cancelled, with three senders subsequently blocked.

7.5 Reporting Sector: Real Estate

During the quarter, one filing from the real estate sector highlighted a significant compliance concern classified under “Other.” The red flag involved a purchaser’s failing to provide required KYC documentation despite the final property payment being completed. This refusal to comply with KYC requirements raised concerns about transparency and regulatory adherence, signaling potential vulnerabilities in real estate transactions.

7.6 Reporting Sector: Securities: Investment Businesses

Filings from the Investment sector revealed multiple crime classifications, including fraud, tax offences, and money laundering. Money laundering concerns arose when adverse media linked a client to suspected

dealings in proceeds of crime, suggesting that funds deposited into trading accounts may have originated from illicit sources. Tax-related red flags involved economically irrational behavior, such as a client's son declining to claim assets, raising suspicions under South African tax legislation. Fraud indicators included adverse media reports of a client defrauding a company of millions and surrender requests tied to individuals charged with fraud offences, suggesting that life policies may have been funded with criminal proceeds. These cases underscore the need for enhanced due diligence and monitoring within investment services.

7.7 Reporting Sector: Long Term Insurers

The LTI sector reported a wide range of crime classifications, including fraud, tax offences, bribery, corruption, money laundering, and terrorist financing. Red flags included adverse media linking customers to money laundering, frequent ownership changes without valid reasons, large cash settlements without source of funds, and refusal to comply with FATCA requirements. One case involved a broker seeking to place a policy for a subject connected to the Panama Papers and ongoing fraud investigations. Bribery concerns were raised following correspondence from ICCAC, while corruption indicators involved clients suspected of assisting a former first lady in laundering funds. A notable terrorist financing risk was identified in a policy liquidation potentially linked to Russia-Ukraine war efforts. These findings highlight significant cross-border risks and the importance of robust AML/CFT controls.

7.8 Reporting Sector: Insurance Company

The insurance company sector reported crime classifications including fraud, market abuse, money laundering, bribery, narcotics, sanctions, and tax offences. Fraud and bribery concerns were primarily driven by adverse media and questionable source of funds documentation. Market abuse indicators included clients exited by a global bank due to negative media. Money laundering patterns involved large cash transactions, temporary fund repositories, U-turn transfers, and misuse of personal accounts for premium payments. Sanctions-related risks were evident in the decline of a potential client listed on the US OFAC list for ties to the Russian financial system. These cases underscore the sector's exposure to complex financial crime typologies and the need for enhanced screening and transaction monitoring.

8.0 Key Report Indicators

During Q4 2023, reporting entities across sectors flagged several critical indicators of suspicious activity. These indicators collectively reflect heightened vigilance around financial crime risks, sanctions evasion, and politically exposed or high-risk clients. Report indicators of interest that were chosen by the various reporting sectors during Q4 2023 are as follows:

- Adverse Media
- Fraud
- Money Laundering
- Tax Evasion
- Bribery
- Corruption
- Terrorist Financing

Additional indicators noted were Consent Requests, High-Risk Country Associations, Declined or refused business due to suspected criminal activity, False

Documents, Criminal History, Sanctions List matches, Panama Papers references, Drug Trafficking/Activity, and Arms/Military links.

-END -