Q1 QUARTERLY STATISTICS REPORT

JANUARY - MARCH 2024

Financial Intelligence Agency
Bermuda
QUARTERLY REPORT
January 1st to March 31st 2024

1.0 Table of Contents

1.0 Introduction 4
2.0 Incoming Reports & Requests 4
3.0 SARs/STRs Reporting 5
3.1 SARs / STRs by Reporting Sector 5
3.2 SARs/STRs by Monetary values 5
3.3 SARs/STRs by Suspected Offences 5
4.0 International and Domestic Cooperation 6
4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs) 6
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 7
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: Money Service Businesses 11
7.4 Reporting Sector: Long Term Insurers 11
8.0 Key Report Indicators 13

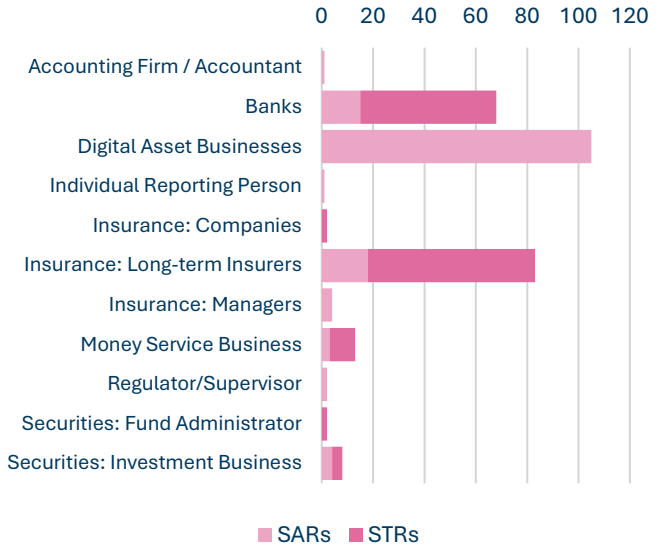
KEY STATISTICS

Total Incoming Reports	Highest Reporting Sector	Total Monetary Values
341	DABs	$233,087,904.0

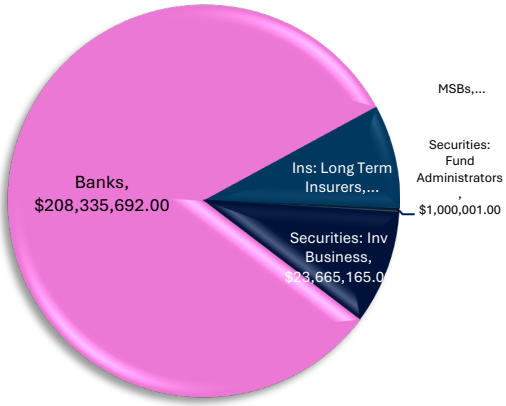
Q4 2023 Reporting (Q3 Comparison)

AIFs	7	▲	n/a
C-SARs			
C_STRs			
CTRs	0	▼	-100%[1]
IRIs	7	▼	-50%
SARs	153	▲	49%
STRs	136	▲	39%
UIRs	38	▲	31%

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] Percentage change reflects reduction from 1 CTR in Q4 2023 to zero in Q1 2024.

1.0 Introduction

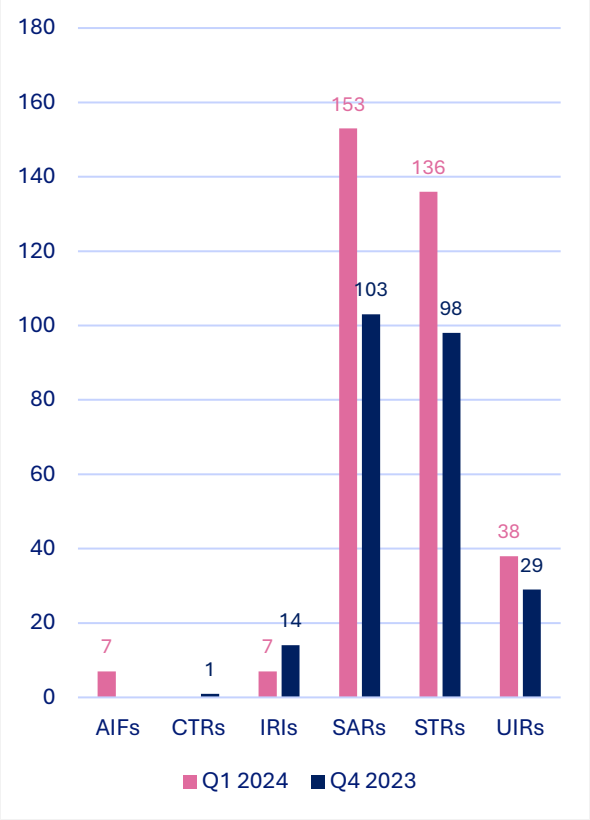
In Q1 2024, the Financial Intelligence Agency (FIA) Bermuda recorded heightened reporting, investigative support activity, and intelligence dissemination across the national AML/CFT framework. Total incoming filings increased to 341 alongside AIF reporting and increased UIRs, despite lower IRIs and the absence of CTRs. Reporting remained concentrated in key sectors, with DABs leading SAR submissions, and Long-Term Insurers (LTIs) and Banks driving STR volumes and high-value STR transaction amounts, resulting in an aggregate $233.1M in STR-linked value largely concentrated in the banking and securities sectors.

Across suspected offences, money laundering and fraud continued to dominate suspicious reporting, while cash exchange-related laundering, insider trading/market abuse, bribery, tax offences, and terrorist financing featured at lower but notable levels. Operationally, the FIA maintained strong domestic and international engagement through incoming and outgoing requests for information, issued consent letters to support reporting entities, and disseminated 119 intelligence reports, mainly as spontaneous disclosures to law enforcement and international Egmont counterparts. Sector narratives further reflected evolving typologies across traditional finance, insurance products, and digital assets, reinforcing the importance of adverse media screening, robust KYC/CDD, and proactive transactional monitoring in identifying and escalating financial crime risk.

2.0 Incoming Reports & Requests

In Q1 2024, FIA Bermuda recorded a total of 341 filings, representing a 39.2% increase compared to 245 filings in Q4 2023. Key increases were observed in SARs, which rose from 103 to 153 (48.5% increase), and STRs, which grew from 98 to 136 (38.8% increase). AIFs also saw new activity, rising from 0 to 7, while IRIs decreased from 14 to 7 (-50.0% decline). UIRs increased from 29 to 38 (31.0% increase), and CTRs dropped from 1 to 0 (100% decline). Overall, Q1 2024 reflects significant growth in SAR and STR filings, driving the overall upward trend.

Chart 1 - Reports received by FIA for Q1 2024 vs Q4 2023



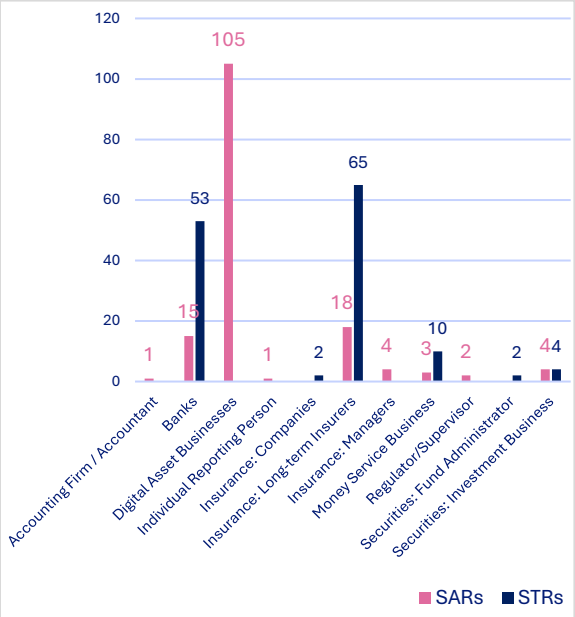
Source: FIA (2024)

3.0 SARs/STRs Reporting

3.1 SARs / STRs by Reporting Sector

In Q1 2024, FIA Bermuda received 153 SARs and 136 STRs across multiple reporting sectors. The largest contributor to SAR filings was DABs, accounting for 105 reports, followed by LTIs with 18 SARs and Banks with 15 SARs. For STRs, LTIs led with 65 filings, while Banks submitted 53 STRs, making these two sectors the primary sources of transaction-related reports. Other notable contributors included MSBs (3 SARs, 10 STRs) and Securities: Investment Business (4 SARs, 4 STRs). Several sectors, such as CSPs, Law Firms, and Real Estate agencies, recorded no filings during the quarter, highlighting concentrated reporting activity within financial and insurance sectors.

Chart 2 - SARs / STRs submitted to FIA by Agency Type Q1 2024



Source: FIA (2024)

3.2 SARs/STRs by Monetary values

In Q1 2024, the total monetary value associated with STRs across reporting sectors amounted to $233,087,904.00. The largest contributor was Banks, accounting for $208,335,692.00, followed by Securities: Investment Business with $23,665,165.00, and LTIs with $21,669,697.00. Other sectors reported minimal amounts, such as Securities: Fund Administrators ($1,000,001.00) and MSBs ($17,337.00), while most sectors recorded zero values. These figures highlight a significant concentration of high-value transactions within banking and securities sectors.

3.3 SARs/STRs by Suspected Offences

In Q1 2024, the majority of SARs were associated with Money Laundering, accounting for 91 reports, followed by Fraud with 49 SARs. For STRs, Money Laundering also dominated with 43 filings, while Cash Exchange-related Money Laundering contributed 31 STRs. Other notable categories included Insider Trading (Market Abuse) with 2 SARs and 20 STRs, and Bribery with 1 SAR and 7 STRs. Tax offences and terrorist financing were reported at lower levels, while several categories such as Human Trafficking and Crypto-related laundering recorded no filings. These figures underscore the continued prevalence of money laundering and fraud as primary concerns in suspicious reporting.

Table 1 – SAR/STR filing by suspected crime offences in Q1 2024

#	Crime Classification	SARs	STRs
1.	Bribery	1	7
2.	Corruption	1	1
3.	Drug Trafficking/ Narcotics	2	
4.	Fraud	49	24

#	Crime Classification	SARs	STRs
5.	Human Trafficking		
6.	Insider Trading (Market Abuse)	2	20
7.	Money Laundering	91	43
8.	Money Laundering – Cash Exchange Related	2	31
9.	Sexual Exploitation	1	
10.	Tax Offences	2	10
11.	Terrorist Financing	2	
	TOTAL	**153**	**136**

Source: FIA (2024)

4.0 International and Domestic Cooperation

4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs)

In Q1 2024, FIA Bermuda received a total of 38 incoming requests and reports, comprising 7 IRIs and 38 UIRs. Among IRIs, Egmont (FFIUs) accounted for 4 requests from the BVI, Ukraine and the UK. Local Law Enforcement (LLEAs) submitted 4 requests (3 from BPS and 1 from HM Customs). For UIRs, LLEAs – primarily HM Customs for this quarter) was the main source with 34 filings; Egmont partners submitted 4 reports from Australia, Guernsey, Syria and USA. These figures highlight strong engagement from law enforcement and international FIU counterparts during the quarter.

Table 2 Incoming IRIs / UIRs in Q1 2024

Reporting Sector	# of Filings
IRIs	***7***
Egmont (FFIUs)	3 (BVI, Ukraine, UK)
Local Law Enforcement	4 (BPS (3), HM Customs (1))
Supervisor/Regulator	0
UIRs	***38***
Local Law Enforcement	34 (HM Customs)
Egmont (FFIUs)	4 (Australia, Guernsey, Syria, USA)
TOTAL	**45**

Source: FIA (2024)

4.2 Outgoing Requests for Information (Domestic & International)

In Q1 2024, FIA Bermuda disseminated a total of 33 outgoing requests. The majority were Section 16 Requests to domestic reporting entities, totalling 25 filings, with 5 outgoing requests to domestic competent authorities. 3 international RFIs were issued to the UK and USA for this reporting period.

Table 3 Outgoing RFIs disseminated in Q1 2024

	Report Types	# of Filings
1.	Section 16 Requests (Reporting Entities - Domestic)	25
2.	Outgoing Requests for Domestic (Competent Authorities)	5
3.	Outgoing Requests for Information (International)	3 (UK, USA)

Source: FIA (2024)

5.0 Consent Letters

In Q1 2024, the FIA maintained its practice of issuing Consent Letters to reporting entities that submitted SARs or STRs and requested approval for transactions or activities identified as suspicious. During this quarter, three letters of consent were issued in response to reports originating from LTIs and entities within the Securities sector, including Fund Administrators and Investment Business firms. This continued initiative underscores the FIA's commitment to strengthening compliance oversight and fostering transparent communication with reporting entities.

6.0 Intelligence Reports (Response / Spontaneous Disclosures)

6.1 Outgoing Disclosures (Intelligence Reports)

In Q1 2024, FIA Bermuda disseminated a total of 119 outgoing reports across various disclosure types. The majority were Spontaneous Disclosures to LEAs, totalling 89 filings directed to BPS and HM Customs. Additionally, 15 Spontaneous Disclosures to Egmont FIUs were issued to jurisdictions including BVI, Bahamas, Canada, Cayman Islands, Ecuador, Honduras, Saudi Arabia, Uganda, UK, and USA. Response Disclosures to Egmont FIUs accounted for 10 reports, while Spontaneous Disclosures to Local Competent Authorities included 5 filings (BMA and FSIU). No response disclosures were made to local competent authorities or LEAs during this period. These figures highlight strong engagement with both domestic law enforcement and international FIU counterparts.

Table 4 Outgoing Report Types disseminated in Q1 2024

	Report Types	# of Filings
1.	Response Disclosures to Local Competent Authorities	0
2.	Response Disclosures to Local LEAs	0
3.	Response Disclosures to Egmont FIUs	10 (Bangladesh, Belize, Montenegro, Nepal, Paraguay, Syria, UAE)
4.	Spontaneous Disclosures to Local Competent Authorities	5 (BMA (3), FSIU (2))
5.	Spontaneous Disclosures to Local LEAs	89 (BPS, HMS Customs)
6.	Spontaneous Disclosures to Egmont FIUs	15 (BVI, Bahamas, Canada, Cayman Islands, Ecuador, Honduras, Saudi Arabia, Uganda, UK, USA)

Source: FIA (2024)

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

In Q1 2024, banks reported seventeen (17) suspected fraud cases involving a range of complex and escalating typologies, including imposter scams, business email compromise, investment scams, securities fraud, and elder financial exploitation. Red flags frequently centred on vulnerable customers—particularly elderly clients—being manipulated by relatives, caregivers, or fraudsters who gained unauthorized access to personal banking information, online banking tokens, or remote access to devices. Several cases involved clients being deceived into initiating global wire transfers to the USA, Thailand, Cayman Islands, South Africa, and Jamaica, often after being contacted through phishing emails, fake refund schemes, or fraudulent job opportunities. Other schemes included unauthorized use of digital signatures following email compromise traced to Nigeria, online investment fraud linked to deceptive social media promotions, and a corporate client receiving funds tied to an SEC-sanctioned individual. Fraudsters exploited customers through intimidation, misinformation, and misuse of authority (including questionable Power of Attorney claims), while some victims unknowingly acted as money mules by forwarding funds for criminal networks. These cases collectively demonstrate continued exposure to cyber-enabled fraud, elder abuse, romance and employment scams, and misuse of digital channels, reinforcing the need for strong customer authentication, proactive

monitoring, and enhanced fraud-awareness outreach.

Classification: Money Laundering

During Q1 2024, the banking sector submitted eleven (11) suspected money laundering filings, primarily involving deficiencies in KYC/CDD, unexplained financial activity, and suspicious cross-border fund movements. Several cases revealed attempts to misuse local trust and scholarship plan structures to circumvent foreign regulatory restrictions, including solicitation of private placements online without issuing periodic statements to subscribers. Other filings involved customers unable to articulate the nature or purpose of their business activity, resulting in declined relationships, as well as an overseas client with a criminal history in arms and drug trafficking whose Bermuda account received small cash deposits later withdrawn via ATMs in Jamaica. Key indicators referenced included adverse media, unexplained cash deposits, ATM withdrawals abroad, refusal to provide KYC documentation, use of corporate vehicles and trusts, inconsistent account activity, high-risk jurisdictions, and patterns suggestive of layering through electronic transfers and cross-border cash flows.

Classification: Money Laundering Involving Cash Exchanges

In Q1 2024, banks submitted thirty-three (33) filings related to suspected money laundering through cash exchange activity, with cases characterised by rapid deposits and same-day foreign currency withdrawals, inconsistent customer explanations, and transactional patterns lacking any legitimate economic rationale. Customers frequently deposited BMD cash into one bank and withdrew USD from another despite holding USD accounts, behaviour indicative of structuring. Additional red flags included overdrawn accounts at the time of exchanges, adverse media linking individuals to drug trafficking, wire transfers to abandoned properties, and observable customer discomfort, evasiveness, or skittish behaviour when questioned. Several customers provided implausible or unverifiable sources of funds—including bingo winnings, online gambling, food sales, or wages inconsistent with deposited amounts—while others relied on government financial assistance despite engaging in high-volume cash exchanges totalling approximately $950,000.00 over the review period. Some exchanges were linked to a known third-party facilitator operating across multiple branches. Activity remained concentrated in USD exchanges, often supplemented by wire transfers to overseas jurisdictions, cryptocurrency platforms, and PayPal. Indicators referenced across filings included smurfing, structuring, unusual cash activity, lack of travel history, refusal to provide KYC information, and inconsistent transactional behaviour. One customer relationship was recommended for exit as banks continued to face increasing customer resistance to source-of-funds inquiries.

Classification: Tax Offences

In Q1 2024, five (5) filings involved suspected tax offences, with cases reflecting patterns of foreign currency purchase tax (FCPT) evasion, unverified sources of funds, and informal currency exchange networks. Customers were found structuring transactions to avoid FCPT and bank exchange fees by circulating USD and BMD between multiple parties and institutions, often without legitimate business

justification. Several accounts displayed large third-party transfers, unexplained global movements of funds, and activity inconsistent with declared income, while overseas affiliate banks raised concerns about unclear fund origins and suspicious betting-related payments. Filings revealed customers facilitating currency exchanges for friends and family, routing funds through personal accounts, and conducting betting transactions on behalf of others, creating pass-through activity with no genuine economic purpose. These behaviours, combined with evasive explanations, inconsistent account activity, and indicators such as structuring, use of gatekeepers, internet gambling, and third-party transfers, resulted in the classification of these matters as suspected tax offences.

Classification: Terrorist financing

During Q1 2024, one (1) filing involved suspected terrorist financing, triggered by adverse media identifying the ultimate beneficial owners (UBOs) of a Bermuda-incorporated company as being involved in a coup d'état and an escalating political dispute in South America. Two wire transfers were sent to the UBO shortly after the coup and given the proximity of these transactions to the political unrest, the potential for terrorism-related funding could not be ruled out. Indicators selected for this filing included terrorism-related activity and suspected terrorist financing.

Classification: Corruption

In Q1 2024, there was one (1) filing related to suspected domestic corruption, prompting enhanced scrutiny and risk mitigation measures by the reporting bank. Actions taken included recommendations to exit the client relationship, active monitoring of the account, and the implementation of additional controls to manage identified risks. The customer was also declined further business, and the filing was submitted for information purposes, although no consent request was required.

7.2 Reporting Sector: Digital Asset Businesses

Classification: Fraud

During Q1 2024, DABs reported twenty-eight (28) filings involving suspected fraudulent activity, with cases reflecting a range of account compromises, identity misuse, and links to known fraud ecosystems. Customers attempted verification using multiple inconsistent IDs, while others used their accounts to sell stolen payment cards, store points, or subscription credentials. Several cases involved questionable documentation, unclear sources of funds, and direct exposure to high-risk platforms such as Russian Market and VClub, as well as crypto addresses tied to Medusa Locker ransomware. Additional red flags included shared IP addresses and email credentials suggesting commonly controlled accounts or collusion, repeated suspicious activity involving previously reported customers, and instances of elder financial exploitation. Collectively, these indicators highlight significant fraud-related vulnerabilities within the DAB sector.

Classification: Money Laundering

In Q1 2024, seventy-four (74) filings involving suspected money laundering, characterised by extensive exposure to high-risk crypto typologies and behaviour indicative of layering

were reported by DABs. Several customers transacted with wallets linked to mixing services, darknet markets such as Hydra and Solaris, decentralized exchanges, privacy coins, and unlabelled or unknown wallets, while repeatedly avoiding source-of-funds and source-of-wealth requests. Filings highlighted rapid in-and-out movement of funds—including USDT deposits and withdrawals without intermediary trades—patterns consistent with unregistered money service business activity, and repeated transactions of similar amounts with no apparent economic or lawful purpose. Additional concerns included shared IP addresses, use of personal accounts for employer-related trading, and immediate flow-through of large crypto amounts shortly after account opening. In multiple cases, customers were unresponsive to enhanced due diligence, unemployed despite large transaction volumes, and engaged in activities illegal in their jurisdictions, underscoring significant AML risks and the use of digital asset platforms for potential layering and obfuscation.

Classification: Suspected Market Abuse

In Q1 2024, two (2) filings involved suspected market abuse, specifically wash trading[2], with red flags centred on questionable sources of funds and adverse media linking the client's ultimate beneficial owner to prior illegal market manipulation activity. One SAR detailed a sophisticated pattern in which multiple DAB accounts— believed to be commonly controlled— executed extraordinarily high-volume reciprocal trades in the USDT market. Between October 2021 and February 2022, 98% of all trades were conducted between two related accounts, followed by a second cluster of accounts that dominated over 99% of trades between September and November 2023. Shared IP addresses across South Korea and Indonesia, shared withdrawal addresses, and interconnected email activity further supported common control. The absence of any legitimate business or economic purpose, combined with trading patterns engineered to inflate market activity, strongly indicated wash trading and deliberate manipulation of market liquidity. AGM appeared timed to increase control and voting power while insiders held privileged information. Collectively, these cases underline the convergence of adverse media, suspicious trading patterns and concentrated control of accounts as core indicators of market abuse.

Classification: Suspected Sexual Exploitation

In Q1 2024, one (1) filing involved suspected sexual exploitation, triggered by adverse media linking the customer to a 2018 arrest for operating a website hosting child pornographic material. Although the transactional behaviour within the DAB account did not independently raise concerns, suspicion arose regarding the source of funds, as open-source intelligence indicated that the website and its hosting provider accepted cryptocurrency payments. This increased the likelihood that the crypto deposited into the account was derived from the platform's illicit operations, particularly

[2] NB. Wash trading is a form of market manipulation wherein a trader buys and sells an asset for the express purpose of fabricating misleading information regarding trading volume or liquidity. Wash trading is conducted by the execution of trades by a single party operating as both sides of the transaction, thus cancelling out any potential gain or loss for the trades.

given that all activity occurred shortly before the client's arrest. In response, the DAB disabled the accounts, offboarded the user, and submitted a filing, with a consent request required due to the customer's remaining balance.

7.3 Reporting Sector: Money Service Businesses

Classification: Money Laundering

During Q1 2024, Money Service Businesses (MSBs) submitted 10 filings involving suspected money laundering, with cases marked by unusual sending behaviours and attempts to obscure transaction purposes. Customers with historically low sending profiles abruptly began initiating larger transfers, often multiple times per month, to various recipients and destinations. Several sends were accompanied by handwritten notes on bits of paper, and in one case, cash presented for transfer had a strong odour of cannabis. Customers frequently insisted on sending "the exact amount minus fees," attempted to redirect funds to alternative recipients when transactions were cancelled, or resumed sending activity after periods of inactivity. Patterns included repeated transfers to the same individuals or countries, inconsistent explanations for transaction purposes, and behaviours suggestive of smurfing, structuring, or third-party sending. These indicators, combined with limited or no verifiable source-of-funds information, raised significant money laundering concerns.

Classification: Fraud

MSBs also reported three (3) reports involving suspected fraud, primarily related to scam activity targeting vulnerable customers, including elderly individuals. Red flags included customers sending funds to multiple recipients simultaneously, becoming defensive or evasive when questioned about transaction purpose, and repeatedly citing "business purposes" without supporting documentation—such as invoices for purported furniture purchases. Some customers used multiple MSB locations to facilitate sends, in one instance seeking guidance on how to remit funds to an online ministry. The behaviours reflected common scam typologies, including business email compromise, investment-related scams, and imposter fraud, with victims often pressured into sending money to unknown individuals abroad. Actions taken included blocking senders, cancelling transactions, requesting proof of legitimate business activity, and elevating customer risk profiles, as MSBs continued strengthening monitoring to mitigate ongoing fraud risks.

7.4 Reporting Sector: Long Term Insurers

In Q1 2024, long-term insurers submitted a total of eighty-three (83) filings, reflecting a broad spectrum of financial crime risks within the sector. Reported crime classifications included bribery, corruption, drug trafficking/narcotics, fraud, insider trading and other forms of market abuse, money laundering, tax offences, and terrorist financing. The diversity and volume of filings underscore the sector's exposure to complex, high-risk, and often cross-border activity, as well as the continued vigilance of long-term insurers in identifying and reporting suspected illicit conduct during the review period.

Classification: Bribery

Eight (8) filings were submitted in relation to suspected bribery. These cases were primarily driven by adverse media identifying clients or associated parties as being linked to bribery-related conduct, prompting enhanced scrutiny and reporting by long-term insurers.

Classification: Fraud

Twenty-one (21) filings involved suspected fraud, with red flags largely stemming from adverse media referencing false representations, fake companies, forged documentation, and fictitious contractual arrangements. In several cases, clients were subject to Global Freeze Orders, while other prospective customers were declined onboarding due to links to fraud and money laundering identified through due diligence and media screening.

Classification: Money Laundering

Twenty-nine (29) filings were associated with suspected money laundering, reflecting complex layering and misuse of insurance products. Key red flags included questionable or absent source-of-funds and source-of-wealth documentation, adverse media linking customers to criminal activity, and large cash transactions inconsistent with declared business activities. Additional concerns involved shell companies facilitating third-party fund flows, frequent and unexplained loan withdrawals and repayments, repeated ownership changes with unclear relationships, and links to entities designated by OFAC for involvement in transnational crimes such as drug trafficking, human trafficking, bribery, and wildlife trafficking.

Classification: Tax Offences

Seven (7) filings involved suspected tax offences, characterised by refusals to comply with FATCA requirements, adverse media relating to tax evasion, and transaction patterns inconsistent with customers' declared income. Indicators included frequent changes in policy ownership, rapid policy restructuring, in-and-out transactions of identical amounts, large cash payments by individuals without cash-intensive occupations, and repeated policy loan withdrawals, often via cheque. Cross-border payments and high-value premiums within short timeframes further raised concerns of tax avoidance and potential layering.

Classification: Terrorist Financing

One (1) filing involved suspected terrorist financing, arising from a refusal to update KYC information coupled with adverse media linking the client to terrorist financing and money laundering activities. These factors elevated the risk profile and warranted reporting and further regulatory consideration.

Classification: Insider Trading / Market Abuse

Fourteen (14) filings related to suspected insider trading and market abuse. These cases were primarily driven by adverse media identifying regulatory fines and illicit gains associated with insider trading, as well as suspicious transactional activity observed in policyholders linked bank accounts, suggesting potential misuse of insurance products in connection with market manipulation.

Actions Taken by Long-Term Insurers

In response to the identified risks, long-term insurers submitted filings for informational

purposes and sought the FIA's consent to implement risk-mitigating measures, including freezing affected policies, considering policy termination, or maintaining business relationships under enhanced monitoring and controls.

8.0 Key Report Indicators

Across the Banking, DAB, MSB, Securities, Insurance, and stakeholder filings in Q1 2024, several recurring indicators consistently signalled elevated financial crime risk.

- Adverse media screening remained a primary trigger, repeatedly identifying customers, corporate clients, and UBOs linked to fraud (including imposter and investment scams), market abuse/insider trading, money laundering, tax evasion, bribery/corruption, drug trafficking, sanctions exposure, and potential terrorist financing.
- KYC/CDD deficiencies were persistent, including refusal or delays in providing documentation, inconsistent or evasive explanations, unclear source of funds or wealth, questionable identity documentation (including multiple IDs with varying birth dates), and reluctance to cooperate with enhanced due diligence.
- Transactional red flags included large or frequent cash deposits and withdrawals; structuring and smurfing behaviours; cash exchanges lacking economic rationale (often involving same-day BMD deposits and USD withdrawals); pass-through and third-party transactions; rapid in-and-out flows; wires to multiple jurisdictions; and account activity inconsistent with customer profile, including suspected elder abuse and misuse of accounts.
- In the digital asset environment, key triggers included exposure to darknet markets, mixing services, privacy coins, unlabelled wallets, fraud shops, ransomware-linked addresses, sanctions-related exposure (direct and indirect), shared IP/common control indicators, and flow-through layering patterns.
- Customer and contextual indicators included vulnerable or elderly victims, use of POAs or gatekeepers in potentially coercive arrangements, foreign and high-risk country exposure, and links to sanctioned entities. Finally, the use of control measures such as transaction cancellations, consent requests, account disabling/offboarding, account freezes, relationship exits, sender blocking, and elevated risk scoring demonstrates that reporting entities are actively escalating and mitigating higher-risk activity in parallel with reporting to the FIA.

-END -