Q4 QUARTERLY STATISTICS REPORT

OCTOBER - DECEMBER 2024

Financial Intelligence Agency
Bermuda
QUARTERLY REPORT
October 1st to December 31st, 2024

1.0 Table of Contents

KEY STATISTICS

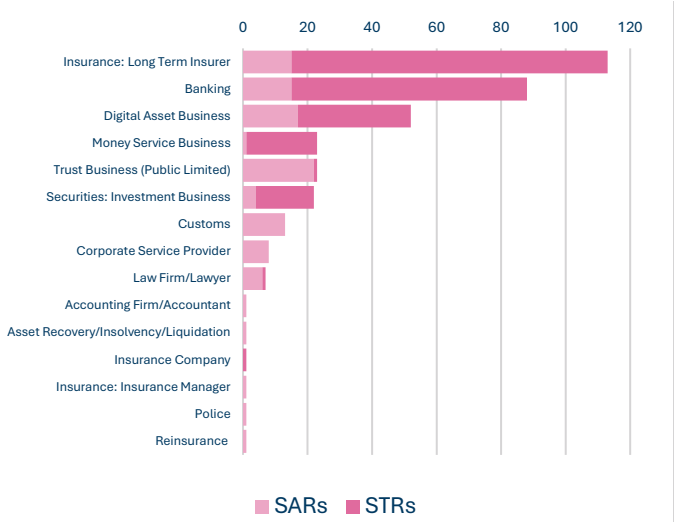
Total Incoming Reports	Highest Reporting Sector	Total Monetary Values (SARs/STRs)
112	Banking	$25,373,180.00

Q3 2024 Reporting (Q2 Comparison)

AIFs			
C-SARs			
C_STRs			
CTRs			
IRIs	12	▼	-8%
SARs	36	▼	-66%
STRs	61	▼	-76%
UIRs	3	▼	-84%

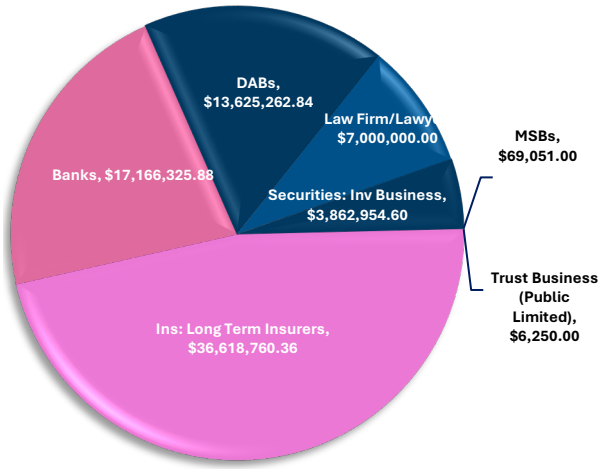
Largest Reporting Sectors

(SARs/STRs)



Highest Monetary Values

(STRs/SARS)



Glossary

ACRONYM	MEANING
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

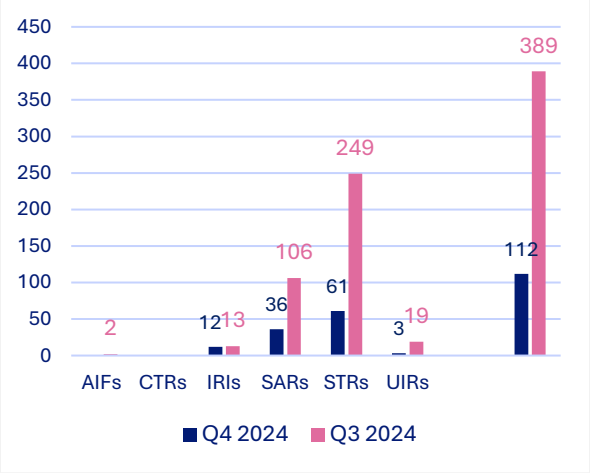
1.0 Introduction

This report presents an overview of the Financial Intelligence Agency (FIA) Bermuda operational statistics and analytical observations for Q4 2024, highlighting trends in suspicious reporting, international cooperation, and key financial crime risks identified across reporting sectors. During the quarter, the FIA continued to receive and analyse SARs, STRs, IRIs, UIRs, and related intelligence to support domestic law enforcement, competent authorities, and international counterparts. While overall reporting volumes declined compared to Q3 2024, the filings received continued to demonstrate exposure to money laundering, fraud, market abuse, sanctions-related activity, and other predicate offences across banking, digital asset businesses (DABs), LTIs, and investment sectors. The data and analysis contained in this report provide insight into emerging typologies, sectoral risk concentrations, and the nature of intelligence exchanges undertaken during the period, supporting the FIA's ongoing role in detecting, analysing, and disseminating financial intelligence to mitigate ML/TF/PF risks within Bermuda's financial system.

2.0 Incoming Reports & Requests

During Q4 2024, the FIA recorded a total of 112 all incoming reports and requests, comprising SARs, STRs, IRIs, and UIRs, representing a substantial decrease compared to 389 filings received in Q3 2024. This decline was primarily driven by a significant reduction in suspicious reporting volumes, with Suspicious Activity Reports (SARs) decreasing from 106 to 36 and Suspicious Transaction Reports (STRs) falling sharply from 249 to 61, indicating a notable contraction in both activity-based and transaction-driven reporting across sectors.

Chart 1 - Reports received by FIA for Q4 2024 vs Q3 2024



Source: FIA (2024)

Incoming Requests for Information (IRIs) declined marginally from 13 in Q3 2024 to 12 in Q4 2024, suggesting relatively stable levels of investigative information requests from domestic and international counterparts. Unsolicited Intelligence Reports (UIRs) also decreased, from 19 to 3, reflecting a lower volume of spontaneous intelligence disclosures received during the quarter. No Additional Information Files (AIFs) or Cash Threshold Reports (CTRs) were recorded during Q4 2024.

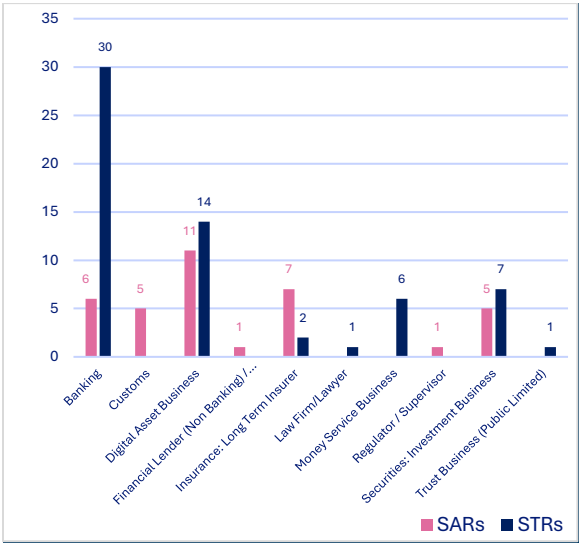
Overall, the reporting landscape for Q4 2024 reflects a marked reduction in suspicious reporting activity compared to the previous quarter, particularly in relation to STR submissions, while requests for investigative assistance remained comparatively steady. This shift may suggest either a moderation in escalated suspicious activity or changes in

reporting behaviour across sectors during the period, alongside continued but more targeted intelligence engagement with the FIA.

3.0 SARs/STRs Reporting

3.1 SARs / STRs by Reporting Sector

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



Source: FIA (2024)

In Q4 2024, a total of 97 SARs and STRs were submitted to the FIA across reporting sectors, comprising 36 SARs and 61 STRs. Filings were concentrated primarily within the banking, digital asset business (DAB), and securities sectors, reflecting continued detection of transaction-driven suspicious activity within both traditional and virtual financial services.

The banking sector recorded the highest reporting volume with 36 filings (6 SARs and 30 STRs), underscoring the sector's continued exposure to high-value transactional monitoring and cross-border financial activity. Digital Asset Businesses accounted for the second largest volume with 25 filings (11 SARs and 14 STRs), highlighting ongoing AML/CFT risks within the virtual asset ecosystem. Securities: Investment Businesses submitted 12 reports (5 SARs and 7 STRs), reflecting the sector's exposure to potential market abuse, fraud, and other investment-related suspicious activity.

Other sectors reported smaller but notable volumes. Long-Term Insurers (LTIs) submitted nine filings (7 SARs and 2 STRs), while Money Service Businesses (MSBs) filed six STRs, consistent with the cash-intensive risk profile of the sector. Customs submitted five SARs, demonstrating continued engagement by law enforcement-related agencies in intelligence-led reporting. Additional filings were submitted by Financial Lenders (Non-Banking/Microfinance) (1 SAR), Regulators/Supervisors (1 SAR), Law Firms/Lawyers (1 STR), and Trust Businesses (Public Limited) (1 STR).

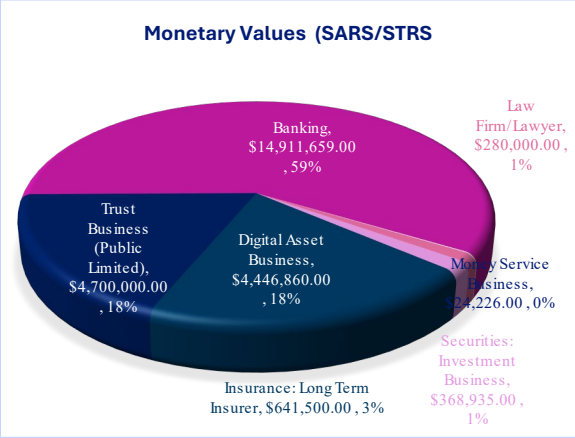
Overall, Q4 2024 reporting reflects a continued concentration of suspicious transaction reporting within banks and DABs, while SAR submissions were more broadly distributed across supervisory authorities, insurers, and professional service providers, illustrating the multi-sectoral nature of financial crime detection and escalation.

3.2 SARs/STRs by Monetary values

In Q4 2024, the aggregate monetary value associated with SARs and STRs totalled approximately USD 25.37 million, reflecting a concentration of higher-value suspicious activity within the banking, trust, and digital asset sectors. The banking sector accounted for the largest share, reporting approximately USD 14.91 million, followed by Trust Businesses (Public Limited) with USD 4.7

million and Digital Asset Businesses (DABs) with USD 4.45 million, highlighting continued exposure to high-value transactions within both traditional financial institutions and the virtual asset ecosystem.

Chart 3 Monetary values of SARs/STRs by Sectors



Source: FIA (2024)

Moderate transaction values were reported by Long-Term Insurers (LTIs) at approximately USD 641,500 and Securities: Investment Businesses at USD 368,935, reflecting suspicious activity linked to insurance and investment products. Lower-value reports were recorded by Law Firms/Lawyers, totalling USD 280,000, and Money Service Businesses (MSBs) with USD 24,226, consistent with the lower-value transaction profile associated with remittance and legal service-related reporting.

The distribution of monetary values indicates that while suspicious reporting was submitted across a range of sectors during Q4 2024, most of the financial exposure remained concentrated within banks, trust structures, and digital asset platforms. *(Refer to Chart – Highest Monetary Values on Key Statistics page)*

The FIA notes that reported monetary values vary in accuracy, as several sectors—particularly DABs—continue to submit filings containing incorrect, inconsistent, or incomplete suspicious transaction values. Consequently, the monetary figures presented should be interpreted with caution and may not fully reflect the true value of suspicious activity reported during Q4 2024.

SARs/STRs by Suspected Offences

Table 1 – SAR/STR filing by suspected crime offences in Q3 2024

#	Crime Classification	SARs	STRs	Total
1.	Bribery		1	1
2.	Corruption	3	1	4
3.	Drug Trafficking/ Narcotics	2	3	5
4.	Fraud	17	17	34
5.	Human Trafficking	1		1
6.	Insider Trading (Market Abuse)	1	4	5
7.	Intelligence	3		3
8.	Money Laundering – Cash Exchange Related		6	6
9.	Money Laundering (General)	8	28	36
10.	Sexual Exploitation		1	1
11.	Terrorist Financing	1		1
	TOTAL	**36**	**61**	**97**

Source: FIA (2024)

Q4 2024, SAR and STR filings reflected a diverse range of suspected criminal activity, with money laundering and fraud continuing to dominate the overall offence profile. Money Laundering (general) accounted for the highest volume of reports, comprising 8 SARs and 28 STRs (36 total), highlighting the continued prevalence of transaction-driven laundering risks across reporting sectors. Fraud represented the second largest category with 17 SARs and 17 STRs (34 total), demonstrating the persistent impact of fraud-related typologies, including scams, misrepresentation, and deception-based financial crimes.

Other notable offences included drug trafficking/narcotics, which generated five

reports (2 SARs and 3 STRs), and insider trading/market abuse, which accounted for five filings (1 SAR and 4 STRs), reflecting ongoing concerns regarding market integrity within the investment sector. Corruption generated four reports (3 SARs and 1 STR), while money laundering involving cash exchange activity produced six STRs, indicating continued monitoring of cash-intensive transactions and currency exchange activity.

Lower frequency but high-risk offences included bribery (1 STR), human trafficking (1 SAR), sexual exploitation (1 STR), and terrorist financing (1 SAR). Additionally, three SARs were classified as intelligence-related, reflecting reports submitted primarily for information-sharing purposes rather than direct transactional suspicion.

Overall, the offence profile for Q4 2024 demonstrates that money laundering and fraud remain the primary drivers of suspicious reporting, with STRs continuing to outnumber SARs, underscoring the significant role of transaction monitoring in identifying potential financial crime activity across reporting sectors.

4.0 International and Domestic Cooperation

4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs)

During Q4 2024, the FIA received a total of 15 incoming requests and unsolicited intelligence disclosures, reflecting continued cooperation with both domestic and international partners, albeit at lower volumes compared to the previous quarter. Incoming Requests for Information (IRIs) accounted for 12 filings, comprising seven (7) requests from Local Law Enforcement, specifically the Bermuda Police Service (BPS), and five (5) requests from Egmont Group Foreign FIUs (FFIUs) originating from Canada, Gabon, Luxembourg, Monaco, and Tunisia. No IRIs was received from domestic supervisors or regulators during the reporting period.

In addition, the FIA received three (3) Unsolicited Intelligence Reports (UIRs). Of these, two (2) were submitted by Local Law Enforcement, specifically HM Customs, while one (1) disclosure originated from a Supervisor/Regulator. No unsolicited disclosures were received from Egmont FFIUs during the quarter.

Overall, the composition of incoming IRIs and UIRs in Q4 2024 highlights continued engagement with domestic law enforcement and selected international FIU counterparts, supporting ongoing intelligence development and investigative collaboration.

Table 2 Incoming IRIs / UIRs in Q3 2024

Reporting Sector	# of Filings
IRIs	
Egmont (FFIUs)	5 (Canada, Gabon, Luxembourg, Monaco, Tunisia)
Local Law Enforcement	7 (BPS 9)
Supervisor/Regulator	0
UIRs	
Local Law Enforcement	2 (HM Customs)
Egmont (FFIUs)	0
Supervisor/Regulator	1

Source: FIA (2024)

4.2 Outgoing Requests for Information (Domestic & International)

During Q4 2024, the FIA disseminated a total of 42 outgoing Requests for Information (RFIs) in support of ongoing intelligence analysis and investigative cooperation with both domestic and international counterparts. Section 16 Requests to domestic reporting entities accounted for most of these enquiries, totalling 35 requests, and were directed primarily to banks, credit unions, and money service businesses (MSBs) to obtain transaction records, beneficial ownership information, and other supporting documentation relevant to ongoing cases.

In addition, three (3) outgoing requests were issued to domestic competent authorities, specifically the Registrar of Companies, reflecting targeted enquiries relating to corporate structures and beneficial ownership information.

International cooperation also continued during the quarter, with four (4) outgoing RFIs disseminated to Foreign FIUs (FFIUs), including counterparts in Brazil and the United States, highlighting the cross-border nature of several investigations involving potential money laundering and related financial crimes.

Overall, the volume and distribution of outgoing RFIs in Q4 2024 demonstrate the FIA's continued reliance on both domestic reporting entities and international FIU networks to obtain critical intelligence and financial information necessary to support complex financial crime investigations.

Table 3 Outgoing RFIs disseminated in Q3 2024

	Report Types	# of Filings
1.	Section 16 Requests (Reporting Entities - Domestic)	35 Banks, Credit Unions, MSB
2.	Outgoing Requests for Domestic (Competent Authorities)	3
3.	Outgoing Requests for Information (International)	4 (Brazil, USA)

Source: FIA (2024)

5.0 Consent Letters

During Q4 2024, the FIA continued to operate its consent regime for higher-risk matters, issuing Consent Letters in response to SARs and STRs where reporting entities sought approval to proceed with transactions or activities identified as suspicious. Of the seven (7) consent-seeking filings received during the quarter, four (4) formal Consent Letters were issued. These arose from reports submitted by Digital Asset Businesses (DABs), Securities: Investment Businesses, a commercial bank, and a Long-Term Insurer (LTI). Consent was implied in respect of the remaining requests.

This process reflects the FIA's continued commitment to proportionate regulatory oversight, timely decision-making, and clear communication with reporting entities, while ensuring that transactions presenting elevated ML/TF risk are subject to appropriate review before being permitted to proceed.

6.0 Intelligence Reports (Response / Spontaneous Disclosures)

Table 4 Outgoing Report Types disseminated in Q3 2024

	Report Types	# of Filings
1.	Response Disclosures to Local Competent Authorities	0
2.	Response Disclosures to Local LEAs	5
3.	Response Disclosures to Egmont FIUs	3
4.	Spontaneous Disclosures to Local Competent Authorities	3 (AML/ATF Board (1), Reg General (1), FSIU (1))
5.	Spontaneous Disclosures to Local LEAs	24 (BPS (15), HMS Customs/JIU (9)
6.	Spontaneous Disclosures to Egmont FIUs	14 (BVI, Cyprus, Guatemala, Ireland, Israel, Kyrgyz Republic, Malta, Palestine, Panama, Slovenia, Switzerland, Turkey, UK, USA)

Source: FIA (2024)

During Q4 2024, the FIA disseminated a total of 49 outgoing intelligence disclosures, supporting both domestic and international cooperation in the detection and investigation of financial crime. No response disclosures were issued to local competent authorities during the quarter; however, five (5) response disclosures were provided to Local Law Enforcement Agencies (LLEAs), alongside three (3) response disclosures to Egmont Group Foreign FIUs (FFIUs) in response to formal intelligence requests.

Proactive intelligence sharing remained a key feature of the FIA's operational activity. The FIA issued three (3) spontaneous disclosures to local competent authorities, specifically the AML/ATF Board (1), the Registrar General (1), and the Financial Sanctions Implementation Unit (FSIU) (1), reflecting targeted information-sharing with supervisory and sanctions-related authorities.

Domestic law enforcement agencies received the largest volume of spontaneous intelligence. A total of 24 spontaneous disclosures were disseminated to Local LLEAs, including 15 to the Bermuda Police Service (BPS) and nine (9) to HM Customs/JIU, demonstrating strong operational collaboration in support of active investigations.

International cooperation also remained robust, with 14 spontaneous disclosures shared with Egmont FIUs across multiple jurisdictions, including the British Virgin Islands, Cyprus, Guatemala, Ireland, Israel, Kyrgyz Republic, Malta, Palestine, Panama, Slovenia, Switzerland, Turkey, the United Kingdom, and the United States.

Overall, the volume and distribution of outgoing disclosures in Q4 2024 underscore the FIA's continued role in facilitating intelligence exchange with domestic and international partners, contributing to the detection, disruption, and investigation of money laundering, fraud, and related financial crime risks.

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: Banking

Classification: Suspected Fraud

During Q4 2024, banks reported several instances of suspected fraud involving cyber-enabled scams, impersonation, and exploitation of vulnerable individuals. One notable typology involved phishing, where a fraudster allegedly gained unauthorised access to a customer's online banking credentials and transferred funds to accounts in another jurisdiction. Banks also identified

vishing-related activity, whereby individuals impersonated representatives of a local bank to obtain sensitive banking information and gain access to customer accounts.

Additional concerns arose in cases involving elder abuse fraud, including attempts by caregivers to open bank accounts jointly with senior citizens, raising suspicions of potential financial exploitation. Banks also reported theft-related activity, including cases where individuals accessed and utilised the bank accounts of deceased family members following their death. In some instances, adverse media screening further heightened suspicion, identifying allegations linking customers to international fraud schemes, which prompted enhanced scrutiny and escalation through SAR filings.

Classification: Suspected Money Laundering & Cash Exchanges

During Q4 2024, banks also reported suspected money laundering linked to cash exchange activity, where transaction patterns were inconsistent with customer profiles and lacked a credible economic rationale. A key indicator involved unknown or unexplained sources of funds, where customers deposited cash to conduct foreign currency exchanges that were not commensurate with their expected income or historical account activity.

In several cases, no associated travel activity could be identified before or after the currency exchanges, despite the transactions suggesting preparation for overseas travel. This raised concerns that the exchanges were conducted for purposes unrelated to legitimate travel or personal use. Banks also observed sudden reactivation of previously inactive accounts, which began conducting multiple cash exchange transactions within short periods, often funded through deposits with unclear origins. Collectively, these indicators suggested potential attempts to utilise cash exchange services as a means of layering or disguising the origin of illicit funds.

Classification: Suspected Money Laundering

During Q4 2024, banks reported several instances of suspected money laundering (ML) characterised by unusual transaction behaviour, inadequate explanations regarding the source of funds (SoF), and misuse of personal and business banking relationships. One notable case involved exposure to the Azerbaijani Laundromat scheme, where trusts and corporate service providers associated with former corporate clients of a local bank were linked to the broader laundering network.

Other filings highlighted the commingling of funds and misuse of accounts, including cases where sole trader business accounts were used to facilitate personal transactions, obscuring the true nature of financial activity. Banks also identified deposits involving counterfeit USD currency mixed with legitimate bills, raising concerns regarding the possible introduction of illicit cash into the financial system. Additional red flags included sanctions-related enquiries, where customers sought guidance on transacting with Russian individuals despite widely publicised sanctions restrictions.

In several cases, adverse media screening identified customers linked to domestic drug trafficking and firearms offences, further elevating ML risk. Customers frequently failed or refused to provide credible SoF

documentation, with some becoming uncooperative or requesting account closure when questioned about the origin of cash deposits. Banks also observed funds being rapidly transferred to unknown or unrelated recipients, inconsistent with the stated purpose of the account. Additional indicators included inconsistent account activity, such as individuals on financial assistance depositing large amounts of cash, unusual patterns of cash inflows followed by international transfers, and accounts receiving funds from individuals previously reported in SAR filings. Instances of misuse of personal and business accounts were also identified, including the operation of personal transactions through business accounts or accounts opened for use by other family members. Collectively, these indicators suggested potential attempts to obscure the origin and movement of illicit funds through the banking system.

Action Taken by Banks

During Q4 2024, banks implemented a range of mitigation and reporting measures in response to suspicious activity, including filing SARs and STRs with the FIA, reporting matters to the Bermuda Police Service, and submitting attempted fraud and suspicious interaction reports for intelligence purposes. In several cases, internet banking access was suspended, new authentication credentials were issued, and efforts were made to recall fraudulent transfers. Banks also declined new business relationships, closed accounts where appropriate, and reported potential elder abuse or exploitation to relevant authorities such as Ageing and Disability Services. Investigations frequently involved phishing and vishing scams, with funds transferred to jurisdictions including the USA, Hong Kong, the UK, Peru, Thailand, and Jamaica.

Additional Points of Interest

Additional points of interest included the continued use of USD as the preferred currency for suspicious cash exchanges, as well as three STRs linked to the cannabis industry and six filings involving suspect cash exchange activity across three local banks. The report indicators selected by banks reflected a wide spectrum of financial crime risks, including fraud, money laundering, cash-intensive transactions, cyber-enabled scams, adverse media exposure, misuse of accounts, structuring, high-risk jurisdictions, and refusal to comply with KYC requirements, highlighting persistent vulnerabilities across both traditional banking transactions and digital banking channels.

7.2 Reporting Sector: Digital Asset Business (DAB)

Classification: Suspected Fraud

Fraud-related filings were largely driven by attempts to circumvent platform security controls and identity verification processes. Investigations identified cases where individuals repeatedly modified identification numbers to create multiple accounts, enabling them to bypass onboarding safeguards. In one instance, a customer admitted to submitting false identification documents and using multiple identities in an effort to verify and operate a funded DAB account. Adverse media screening further revealed that a client had promoted alleged

cryptocurrency Ponzi schemes under an alternative surname, raising concerns regarding fraudulent investment activity. Additional red flags included transactions linked to a "fraud shop", an online marketplace involved in the purchase and sale of stolen account credentials and counterfeit identification documents, indicating possible involvement in organised cyber-enabled fraud networks.

Classification: Suspected Drug Offences

DABs also reported cases linked to suspected drug-related activity, including instances where local law enforcement submitted requests for information concerning customers believed to be utilising their digital asset accounts in connection with suspected narcotics offences. These enquiries prompted enhanced monitoring and escalation through formal reporting channels.

Classification: Suspected Sexual Exploitation

During Q4 2024, DABs also reported cases involving suspected sexual exploitation, specifically relating to potential Child Sexual Abuse Material (CSAM) activity. One investigation was initiated following the receipt of a subpoena from an overseas law enforcement agency linked to an ongoing child exploitation enquiry. Subsequent analysis indicated that the user was suspected of receiving funds associated with child exploitation and CSAM-related activities, raising serious concerns of illicit conduct involving child endangerment. Further transactional review identified that the customer had sent funds to a vendor associated with CSAM, prompting escalation through formal reporting channels and cooperation with relevant law enforcement authorities.

7.3 Reporting Sector: Securities: Investment Business

Classification: Suspected Market Abuse

Market abuse-related filings were driven primarily by suspected insider trading and market manipulation. Red flags included CFD trading executed ahead of public announcements regarding a company sale, combined with no prior trading history in the stock and unusually large exposures that generated significant profits. These trading patterns, together with adverse media linked to market manipulation, raised concerns regarding the legitimacy of trading activity and the potential use of investment platforms to exploit non-public information.

Classification: Suspected Terrorist Financing

Terrorist financing concerns were triggered by adverse media screening, which identified a former client suspected of involvement in terrorism financing. The findings resulted in the company and its owner being added to OFAC's Specially Designated Nationals (SDN) list, prompting escalation and reporting due to the elevated sanctions and TF risk.

Classification: Suspected Drug Offences and Fraud

Filings under this classification were primarily driven by screening alerts and adverse media. In one case, a prospective client was flagged as a PEP linked to a drug cartel, leading to the decline of the business relationship. Additional cases involved true name matches to embezzlement, adverse media identified during death liquidation and full liquidation requests, and historical imprisonment linked to fundraising fraud, all of which raised concerns regarding the legitimacy of funds and potential financial crime exposure.

Classification: Suspected Human Trafficking

Human trafficking risk was identified through a full name match to adverse media, where the customer's name, gender, and jurisdiction corresponded to reports involving human trafficking and conspiracy. This raised concerns that the source of wealth may have derived from illicit trafficking-related activity.

Classification: Suspected Bribery and Corruption

Bribery and corruption-related suspicion arose following adverse media identified during a full liquidation process, which was determined to be a true match to the customer's name and country of birth, indicating potential involvement in corruption-related offences.

Points of Interest and Actions Taken

During the quarter, three (3) consent requests were submitted by Investment Businesses, totalling approximately USD 330,000, primarily linked to liquidation requests following adverse media findings. Actions taken included declining onboarding, denying client applications, blacklisting customers, and seeking FIA consent for both full liquidation and death liquidation requests.

7.4 Reporting Sector: Insurance: Long-Term Insurers (LTIs)

Classification: Suspected Money Laundering

LTI filings highlighted multiple indicators of suspected money laundering, particularly involving unusual policy ownership changes, early surrender activity, third-party payments, and questionable source of wealth (SoW). Several cases involved policies transferred between unrelated parties, often described as gifts or business arrangements, followed by early surrender of policies shortly after ownership changes. Additional red flags included large withdrawals following premium payments, frequent non-scheduled premium prepayments, and third-party funding of policies. Concerns were further elevated by cash-based source of funds, payments from numerous unrelated counterparties, and patterns suggesting temporary repository of funds and U-turn transactions. Other high-risk indicators included links to Russian PEPs, sanctions exposure, Iranian interests, shared business addresses with high-risk entities, and involvement in cash-intensive industries such as casinos. In several instances, counterparties associated with the policyholder were designated by OFAC, further heightening ML and sanctions evasion risk.

Classification: Suspected Fraud

Fraud-related activity included imposter fraud, where a fraudulent surrender request was submitted seeking refund to a foreign bank account. Verification with the legitimate policyholder confirmed that no such request had been made and that the customer had no connection to the destination jurisdiction, prompting escalation and reporting.

Classification: Suspected Tax Evasion

Tax evasion concerns arose from transfers of policy ownership from corporate entities to UBOs, particularly where the company had filed dormant accounts with UK Companies House, suggesting attempts to obscure income from tax authorities. Additional risk was identified through FATCA non-compliance, where customers refused to provide required tax documentation despite repeated requests.

Classification: Suspected Market Abuse

Market abuse-related suspicion was triggered by adverse media and law enforcement correspondence, which identified clients under investigation for insider trading, raising concerns regarding the origin of funds used to fund policies.

Classification: Suspected Bribery

Bribery risk was identified following receipt of a law enforcement enquiry letter indicating that the customer was involved in a bribery case, prompting enhanced scrutiny and reporting.

Classification: Suspected Corruption

Corruption-related suspicion arose where adverse media indicated that the policyholder was wanted for corruption around the time the policy was issued, raising concerns that the source of wealth may represent proceeds of crime.

Points of Interest and Actions Taken

Of the 75 filings, 66 were dual filings submitted by LTIs reporting to Bermuda and other jurisdictions, primarily involving Chinese, Taiwanese, Japanese, and European customers as both victims and subjects. Two filings referenced potential North Korea (DPRK) exposure, while additional cases identified direct and indirect links to Iran and Russia, including activity involving dual-use goods, technology sectors, and potential sanctions exposure. Prospective business relationships were declined due to adverse media linked to sanctions, illicit gambling, bribery, fraud, and suspected terrorist financing, and internal freezes were placed on high-risk policies where appropriate.

Actions taken by LTIs included filing SARs with the FIA, declining new business, placing policies on internal freeze, blocking policies, seeking FIA consent for surrender or termination, and ongoing monitoring of high-risk relationships.

8.0 Key Report Indicators

Across all reporting sectors in Q4 2024, several recurring indicators consistently signalled elevated money laundering (ML),

fraud, and broader financial crime risks. The most frequently selected indicators included adverse media, no or inadequate source of funds/wealth, misrepresentation and false documentation, third-party transactions, unusual ownership changes, and inconsistent account activity. Banking and MSB-related filings were characterised by cash-intensive behaviour, including large or unexplained cash deposits, BMD/USD cash exchanges, structuring, and rapid cross-border wire transfers, often coupled with phishing, vishing, imposter scams, and elder abuse. DAB filings highlighted identity fraud, use of multiple accounts, exposure to illicit actors, darknet and fraud-shop interactions, and rapid crypto movement, alongside links to drug offences and sexual exploitation (CSAM). LTI and securities sector filings reflected complex layering typologies, including early policy surrenders, third-party premium payments, sanctions exposure, PEP involvement, insider trading, and suspicious liquidation requests. Professional service providers such as CSPs, law firms, and investment businesses reported governance and integrity risks, including bribery, corruption, market abuse, and adverse media linked to organised crime or regulatory action. Collectively, these indicators highlight continued vulnerabilities across cash, corporate, and digital asset channels, with common themes of beneficial ownership opacity, misuse of legitimate financial products, sanctions exposure, and attempts to circumvent AML/CFT controls.

-END -