Q2 QUARTERLY STATISTICS REPORT

APRIL - JUNE 2024

Financial Intelligence Agency
Bermuda
QUARTERLY REPORT
April 1st to June 30th, 2024

1.0 Table of Contents

KEY STATISTICS

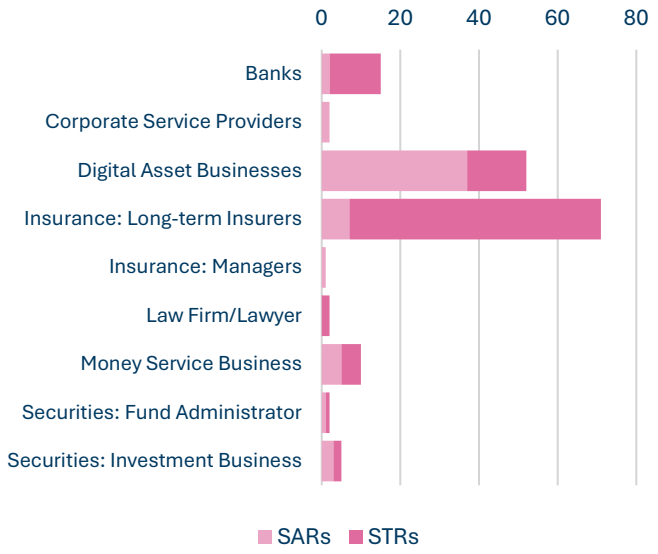
Total Incoming Reports	Highest Reporting Sector	Total Monetary Values
216	LTIs	$430,607,410.0

Q4 2023 Reporting (Q3 Comparison)

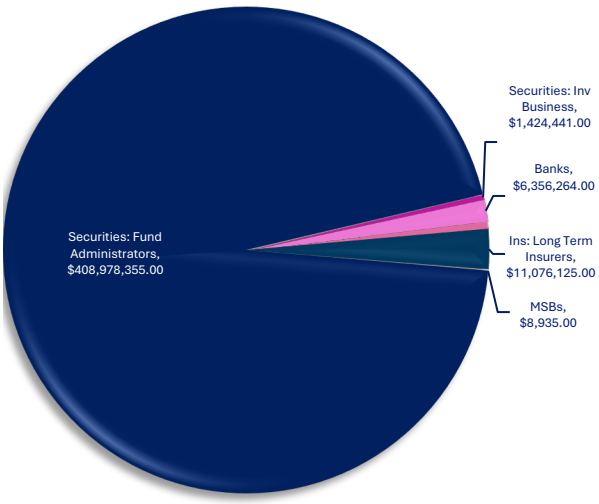
•	AIFs	2	▼ -71%
•	C-SARs		
•	C_STRs		
•	CTRs		
•	IRIs	27	▲ 286%
•	SARs	58	▼ -62%
•	STRs	102	▼ -25%
•	UIRs	27	▼ -29%

Total 216

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

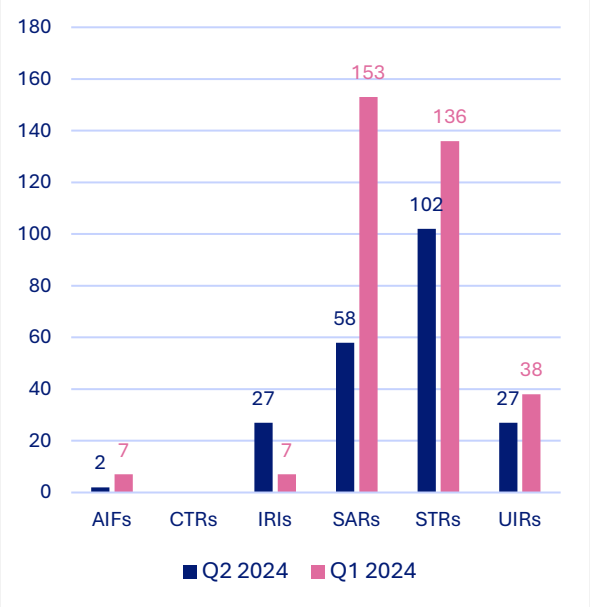
1.0 Introduction

This report presents an overview of FIA Bermuda's operational, analytical, and intelligence activity during Q2 2024, reflecting a period of reduced overall suspicious reporting volumes alongside sustained and, in some areas, intensified intelligence engagement. A total of 216 filings were received during the quarter, representing a marked decline from Q1 2024, driven primarily by reductions in SARs and STRs, while Requests for Information—particularly IRIs from domestic law enforcement and foreign FIUs—increased significantly, underscoring heightened investigative demand and cooperation. Suspicious reporting remained concentrated within a limited number of sectors, notably Long-Term Insurers, Digital Asset Businesses, banks, and securities entities, with reported monetary values heavily skewed toward high-value activity within fund administration and insurance structures. Across all sectors, filings continued to be dominated by money laundering and fraud typologies, complemented by market abuse, tax offences, corruption, and emerging crypto-enabled risks, including sanctions exposure. The quarter was further characterised by robust domestic and international cooperation, active use of Section 16 and outgoing RFIs, the issuance of consent letters for higher-risk transactions, and sustained dissemination of intelligence through response and spontaneous disclosures. Collectively, the findings illustrate a contraction in reporting volume but a continued concentration of complex, high-risk financial crime activity, reinforcing the FIA's central role in intelligence coordination, regulatory engagement, and the mitigation of cross-border ML/TF risks.

2.0 Incoming Reports & Requests

In Q2 2024, FIA Bermuda recorded a total of 216 filings, reflecting a notable decline compared to Q1 2024, which recorded 341 filings. This reduction was primarily driven by significant decreases in SARs, which fell from 153 in Q1 to 58 in Q2 (−62.1%), and STRs, which declined from 136 to 102 (−25.0%). AIFs also decreased from 7 to 2 (−71.4%). In contrast, IRIs rose sharply from 7 to 27 (+285.7%), indicating increased demand for intelligence support, while UIRs declined from 38 to 27 (−28.9%). CTRs remained at zero during the period. Overall, Q2 2024 reflects a contraction in suspicious reporting volumes, partially offset by a substantial increase in investigative and intelligence-related requests.

Chart 1 - Reports received by FIA for Q2 2024 vs Q1 2024



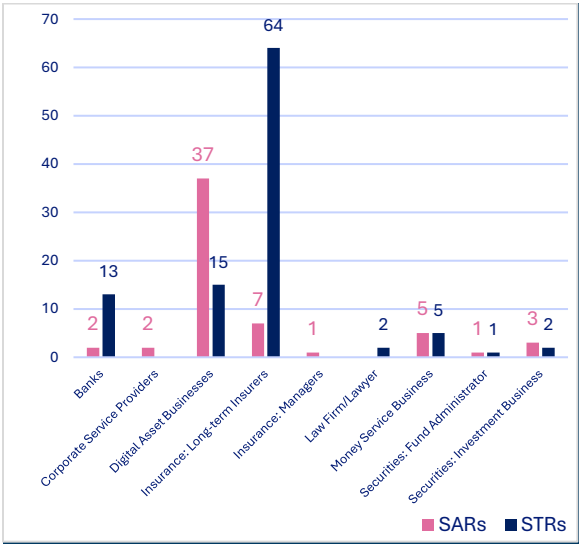
Source: FIA (2024)

3.0 SARs/STRs Reporting

3.1 SARs / STRs by Reporting Sector

In Q2 2024, SAR and STR filings were concentrated within a small number of reporting sectors, with Insurance: Long-Term Insurers (LTIs) emerging as the dominant source of STRs, submitting 64 reports, reflecting continued detection of transaction-based risk within the insurance sector. DABs were the largest contributors of SARs, filing 37 reports, alongside 15 STRs, underscoring the ongoing prevalence of suspicious activity within the digital asset ecosystem.

Chart 2 - SARs / STRs submitted to FIA by Agency Type Q2 2024



Source: FIA (2024)

Banks submitted a limited number of SARs (2) but reported 13 STRs, indicating a greater focus on transaction-driven suspicion during the quarter. MSBs filed an equal number of SARs and STRs (5 each), suggesting balanced reporting across activity- and transaction-based concerns. The securities sector recorded lower volumes, with Investment Businesses submitting 3 SARs and 2 STRs, and Fund Administrators filing 1 SAR and 1 STR. Other sectors recorded minimal activity, including CSPs (2 SARs), Insurance Managers (1 SAR), and Law Firms, which submitted 2 STRs only. Overall, Q2 2024 reporting reflects continued sectoral concentration, with insurance, digital asset, and banking institutions accounting for the majority of suspicious reporting.

3.2 SARs/STRs by Monetary values

The monetary values associated with SARs and STRs in Q2 2024 were heavily concentrated within the securities and insurance sectors, reflecting the presence of fewer but significantly higher-value suspicious transactions. Securities: Fund Administrators accounted for the overwhelming majority of reported value at $408.98 million, underscoring the high-risk, high-value nature of fund-related activity. This was followed by LTIs, which reported $11.08 million, and Banks, with $6.36 million, indicating continued exposure to material transaction risks within traditional financial institutions. DABs reported $2.16 million, while Securities: Investment Business accounted for $1.42 million, reflecting moderate but notable transaction values within capital markets and digital finance. Lower-value activity was reported by Law Firms/Lawyers ($605,900) and MSBs ($8,935). No monetary values were recorded for CSPs, Insurance Brokers, Insurance Companies, Life Insurance entities, or Regulators/Supervisors. Overall, the data highlights a clear concentration of high-value suspicious activity within fund administration and long-term insurance structures, with

comparatively limited financial exposure reported across other sectors.

3.3 SARs/STRs by Suspected Offences

In Q2 2024, suspicious reporting continued to be dominated by money laundering and fraud-related activity, reflecting persistent systemic risk across reporting sectors. Money laundering accounted for the highest volume of filings, with 39 SARs and 59 STRs, reinforcing its position as the primary driver of suspicious transaction reporting. Fraud followed as the second most prevalent offence, generating 14 SARs and 15 STRs, indicating both account-level suspicion and transaction-driven risk. Insider trading and market abuse featured exclusively in STRs, with 10 filings, highlighting transaction-specific detection within capital market activity. Bribery and tax offences also emerged as notable concerns, with 6 STRs each, while corruption resulted in 3 SARs, reflecting entity-level risk identification. Lower-volume but high-risk categories included human trafficking (1 STR), terrorist financing (2 STRs), and niche typologies such as crypto-related money laundering (1 STR) and cash exchange–related money laundering (2 STRs). No filings were recorded for sanctions-related activity, sexual exploitation, drug trafficking, or abnormal activity during the quarter. Overall, the distribution underscores a continued shift toward transaction-based reporting, with STRs outpacing SARs across most offence categories, particularly for money laundering, fraud, and market abuse.

Table 1 – SAR/STR filing by suspected crime offences in Q2 2024

#	Crime Classification	SARs	STRs
1.	Abnormal Activity		
2.	Bribery		6
3.	Corruption	3	
4.	Drug Trafficking/ Narcotics		
5.	Fraud	14	15
6.	Human Trafficking		1
7.	Insider Trading (Market Abuse)		10
8.	Money Laundering	39	59
9.	Money Laundering – Cash Exchange Related		2
10.	Money Laundering – Crypto Related		1
11.	Sanctions Related		
12.	Sexual Exploitation		
13.	Tax Offences	2	6
14.	Terrorist Financing		2
	TOTAL	**58**	**102**

Source: FIA (2024)

4.0 International and Domestic Cooperation

4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs)

In Q2 2024, FIA Bermuda received a total of 54 incoming requests and unsolicited disclosures, reflecting sustained domestic and international cooperation. IRIs accounted for 27 filings, led by Local Law Enforcement (LLEAs) with 19 requests, all submitted by the Bermuda Police Service (BPS), underscoring continued reliance on FIA intelligence to support active investigations. Egmont FIUs submitted 8 IRIs from a diverse range of jurisdictions, including Belarus, BVI, Cayman Islands, France, India, Monaco, and the United States, highlighting ongoing cross-border intelligence exchange.

UIRs also totalled 27 filings, with LLEAs, primarily HM Customs, contributing 21 reports, while Egmont FIUs submitted 6 UIRs

from jurisdictions including Cayman Islands, Jersey, Syria, and the United States. Overall, the volume and composition of IRIs and UIRs in Q2 2024 demonstrate strong operational engagement by domestic law enforcement and continued collaboration with international FIU counterparts.

Table 2 Incoming IRIs / UIRs in Q2 2024

Reporting Sector	# of Filings
IRIs	
Egmont (FFIUs)	8 (Belarus, BVI, Cayman, France, India, Monaco, USA)
Local Law Enforcement	19 (BPS 19)
Supervisor/Regulator	0
UIRs	
Local Law Enforcement	21 (HM Customs)
Egmont (FFIUs)	6 (Cayman, Jersey, Syria, USA)
TOTAL	**54**

Source: FIA (2024)

4.2 Outgoing Requests for Information (Domestic & International)

In Q2 2024, FIA Bermuda disseminated a total of 59 outgoing requests. The majority were Section 16 Requests to domestic reporting entities, totalling 38 filings, followed by 10 outgoing requests to domestic competent authorities. Additionally, 13 international ORIs were issued to counterparts in BVI, Cayman, Hong Kong and other listed in Table 3, reflecting continued engagement with both local and international stakeholders.

Table 3 Outgoing RFIs disseminated in Q2 2024

	Report Types	# of Filings
1.	Section 16 Requests (Reporting Entities - Domestic)	38
2.	Outgoing Requests for Domestic (Competent Authorities)	8
3.	Outgoing Requests for Information (International)	13 (All FIUs, BVI, Cayman, Hong Kong, India, Kenya, Kyrgyz Republic, Mauritius, Portugal, Switzerland, USA, UK)

Source: FIA (2024)

5.0 Consent Letters

In Q2 2024, the FIA continued its practice of issuing Consent Letters to reporting entities that submitted SARs or STRs and sought approval to proceed with transactions or activities identified as suspicious. During the quarter, five (5) consent letters were issued in response to reports submitted by Long-Term Insurers and a Fund Administrator within the Securities sector. This ongoing practice underscores the FIA's commitment to robust compliance oversight, timely regulatory engagement, and transparent communication with reporting entities in managing higher-risk transactions.

6.0 Intelligence Reports (Response / Spontaneous Disclosures)

6.1 Outgoing Disclosures

In Q2 2024, FIA Bermuda disseminated a total of 58 outgoing reports across various disclosure types. Spontaneous Disclosures to LEAs, totalled 22 filings directed to BPS and HM Customs. Additionally, 22 Spontaneous Disclosures to Egmont FIUs were issued to jurisdictions including Argentina, Australia, Bolivia, Cayman Islands, Ghana, India, Kenya, Mauritius, South Africa, UK, Uruguay and USA.

Response Disclosures to LLEAs accounted for 12 reports but no response disclosures were made to Egmont FFIUs during this period. Spontaneous Disclosures to Local Competent Authorities included 2 filings (BMA and FSIU), as such overall these figures highlight strong engagement with both domestic law enforcement and international FIU counterparts.

Table 4 Outgoing Report Types disseminated in Q2 2024

	Report Types	# of Filings
1.	Response Disclosures to Local Competent Authorities	0
2.	Response Disclosures to Local LEAs	12
3.	Response Disclosures to Egmont FIUs	0
4.	Spontaneous Disclosures to Local Competent Authorities	2 (BMA (1), FSIU (1))
5.	Spontaneous Disclosures to Local LEAs	22 (BPS, HMS Customs)
6.	Spontaneous Disclosures to Egmont FIUs	22 (Argentina, Australia, Bolivia, Cayman Islands, Ghana, India, Kenya, Mauritius, South Africa, UK, Uruguay and 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

During Q2 2024, banks reported a range of fraud-related SARs/STRs characterised by complex typologies, adverse media exposure, and indicators of both victimisation and potential complicity. Key red flags included adverse media linked to customers and UBOs, disqualification of a UBO as a UK director following conviction for an indictable offence, unverifiable corporate registrations on UK Companies House, and transactional patterns consistent with laundering and misappropriation, such as payroll and third-party credits followed by immediate cash withdrawals. Reports also highlighted account takeover activity, business email compromise leading to fraudulent wire transfers, misuse of loan proceeds for betting contrary to stated purposes, suspected ATM skimming incidents, identity misuse following the death of account holders, inflated invoicing to extract funds from deceased relatives' accounts, and links to individuals previously sanctioned by foreign securities regulators. Fraud typologies identified included business email compromise, elder abuse fraud, identity and account takeover, imposter and phishing scams, investment and lending fraud, ATM skimming, and tax fraud involving abuse of company assets. In response, banks implemented a range of mitigating actions, including card inhibition, dispute processing and customer reimbursement, filing with the FIA, beneficiary notifications to authorities, account exit recommendations, and escalation for external reporting where appropriate. Reported losses from fraudulent activity totalled approximately USD 130,000.00, with beneficiaries located in Nigeria, the UK, and the USA, and a notable trend emerging of Bermudian residents acting as unwitting—and in some cases witting—participants in account takeovers, including involvement in smurfing activity.

Classification: Tax Evasion

During Q2 2024, banks submitted SARs/STRs highlighting suspected tax evasion involving complex corporate and personal structures designed to obscure true income, ownership, and tax liabilities. Key red flags included layered loan arrangements between related

entities with the same UBO, transaction activity inconsistent with documented loan agreements, and a lack of transparency regarding the activities of central transfer recipients. Reports also identified inadequate source-of-funds evidence, circular currency movements involving the conversion of USD receipts to BMD and subsequent offshore transfers, and income tax withholdings that appeared materially inconsistent with applicable US tax brackets. Additional concerns arose from salary documentation that failed to substantiate claimed employment with entities bearing the names of well-known US companies, suggesting misrepresentation and concealment of income sources. One illustrative case involved a customer who became uncooperative when requested to provide source-of-wealth documentation during the attempted opening of a USD account and was further linked to an undisclosed association with a global precious metals dealer, giving rise to suspected tax evasion and associated ML concerns. In response, banks declined account opening, filed SARs for FIA awareness, initiated enhanced review of existing relationships, and recommended account closure where activity persisted. The activity demonstrated cross-border exposure, with jurisdictions connected to these cases including the UK, Switzerland, Cyprus, the USA, and China, reinforcing the international dimension of suspected tax evasion risks identified during the period.

Classification: Money Laundering Involving Cash Exchanges

During Q2 2024, banks submitted SARs / STRS identifying suspected ML involving cash exchange activity that was inconsistent with customer profiles and indicative of possible criminal proceeds. Key red flags included sudden and unexplained cash deposits into previously dormant or low-balance accounts, repeated BMD/USD cash exchanges without a credible source of funds, and behavioural indicators suggestive of third-party control or direction. In several cases, cash deposits exhibited unusual characteristics, including a strong odour of marijuana masked with perfume, and were followed by attempted international wire transfers to the USA. Customers frequently failed to provide substantiating employment or income information despite repeated requests, and transaction behaviour was inconsistent with stated occupations, such as informal cash-based “side hustles.” Additional concerns arose where individuals appeared unfamiliar with transaction fees, relied on external instructions during exchanges, or demonstrated urgency and distress indicative of acting on behalf of others. Notably, one customer had previously been exited by a bank but subsequently succeeded in opening new accounts, which were again identified for closure following renewed suspicious activity. Points of interest included both male and female exchangers of Dominican Republican, American, Peruvian, and Bermudian nationalities, exclusively involving BMD/USD exchanges, with questionable sources of funds in all cases. As a result of these concerns, banks-initiated SAR/STR filings, enhanced monitoring, and relationship exit procedures, with banking relationships in the process of being terminated due to sustained ML risk linked to cash exchange activity.

Classification: Money Laundering

During Q2 2024, banks submitted SARs/STRs identifying suspected money laundering activity linked to KYC/CDD deficiencies, unexplained cash-intensive behaviour, adverse media exposure, and high-risk domestic and cross-border wire activity. Red flags included significant overpayment of loans inconsistent with stated purposes, transaction activity misaligned with documented loan agreements, and a lack of transparency regarding transfer recipients central to the flow of funds. Several cases involved customers receiving funds from individuals previously associated with adverse media, prior SARs, or S16 requests, as well as the operation of accounts for the benefit of third parties. Additional concerns arose from customers refusing or failing to provide source-of-funds evidence, engaging in repeated large cash deposits—often structured below reporting thresholds—or utilising business banking bag drops without a clear economic rationale. Banks also identified prolonged retention of large cash holdings prior to deposit, continued account usage despite cessation of underlying business operations, and profits reported by entities with no apparent physical presence or operational activity. Behavioural indicators included uncooperative responses to due diligence requests, avoidance of bank contact, and threats to close accounts when challenged. Cross-border exposure featured prominently, with suspect wires linked to Burundi, the UK, Pakistan, Morocco, and the USA, alongside adverse media involving drug trafficking, firearms, environmental crime, and the laundering of conflict minerals. In response, banks escalated concerns through SAR filings, enhanced monitoring, account restrictions, and exit procedures, with at least one banking relationship in the process of being terminated due to sustained and unresolved ML risk.

7.2 Reporting Sector: Digital Asset Businesses (DABs)

Classification: Fraud

During Q2 2024, DABs submitted a total of 52 filings across three reporting entities, with fraud emerging as a dominant classification alongside related ML concerns involving sanctions exposure. Fraud-related SARs/STRs highlighted a range of sophisticated crypto-enabled typologies, including direct exposure to illicit actors, false identification, platform exploitation, phishing, hacking, and large-scale drainage attacks. Key red flags included direct interaction with wallet addresses linked to known fraud services, the use of falsified identity documents to onboard crypto accounts, and the coordinated exploitation of a VASP donation feature, whereby multiple accounts were created using identical photographs, similar email formats, and linked donation accounts to facilitate the laundering of illicit proceeds. Additional activity involved suspected NFT-related hacking[1], merchant activity offering illegal streaming services in breach of copyright laws, and the acceptance of crypto payments to monetise unlawful services.

A notable **case study** involved a high-value drainage attack in which a customer suffered an alleged seed compromise resulting in the loss of approximately 3 million USDC. The

[1] What is an NFT?
According to Coindesk, "Non-fungible tokens (NFTs) are tradable digital assets that contain information that essentially says, "the person in control of this crypto wallet address is the owner of a computer file, stored in this location." (Refer to this website for more information: https://www.coindesk.com/learn/what-are-nfts-and-how-do-they-work)

DAB's investigation identified rapid movement of funds between DAB branches, conversion of USDC into ETH, and subsequent dispersal across newly created wallets. Analysis further revealed that the perpetrator may have inadvertently linked the draining wallet to a previously used DAB account, exposing an identifiable transaction history dating back to 2019. In response, the DAB implemented immediate risk mitigation measures, including account closure requests, zeroing of crypto balances held with the Bermuda branch, and confirmation that no fiat balances remained. Overall, the filings demonstrate the increasing complexity of fraud typologies within the DAB sector and underscore the importance of robust KYC, transaction monitoring, and cross-branch intelligence sharing to detect and disrupt crypto-enabled fraud and associated ML risks.

Classification: Money Laundering

During Q2 2024, DABs submitted SARs and STRs identifying suspected ML activity characterised by rapid fund movement, limited transparency, and non-cooperation with due diligence requirements. Prominent red flags included the use of unlabelled wallets, whereby customers received Ethereum and, within short timeframes, transferred comparable values in other crypto assets—such as SEAM—to different unlabelled wallets, indicating potential layering and flow-through behaviour. Several accounts were newly established yet exhibited high transaction volumes over very short periods, with crypto assets received and immediately transferred off-platform in consecutive transactions lacking any apparent economic or lawful purpose. In multiple cases, customers failed or refused to provide source-of-funds information, despite profiles indicating unemployment or reliance on family and third-party funding. Additional concerns arose where law enforcement subpoenas were received in relation to suspected ML, confirming transactional links to addresses associated with laundering activity, and where the predominant use of stablecoins such as USDC raised questions regarding the underlying purpose of the accounts and the origin of funds. In response, DABs implemented risk mitigation measures including account closures or disabling, offboarding, balance holds pending law enforcement action, and the submission of SARs, with consent sought in higher-risk cases. Points of interest during the quarter included two consent-related filings totalling USD 47,261.26, a wide range of customer nationalities, and repeated exposure involving Russian clients transacting with addresses linked to the Military Correspondent Blog Donation. Overall, these filings underscore persistent ML risks within the DAB sector, particularly those associated with rapid on-chain activity, anonymised wallet usage, and cross-border exposure.

Classification: ML Involving Sanctions

During Q2 2024, DABs also submitted filings identifying suspected money laundering activity and identified linkages to sanctions' nexus, reflecting elevated exposure to sanctioned entities, jurisdictions, and illicit actors within the digital asset ecosystem. Red flags included both direct and indirect exposure to wallet addresses associated with Garantex.io, Nobitex.io, and Hydra Marketplace, all of which are linked to sanctioned entities or jurisdictions

designated under the OFAC SDN regime. Additional concern arose from direct transactional exposure to addresses attributed to the Military Correspondent Blog Donation, identified as a pro-Russian propaganda and fundraising initiative. These cases demonstrated the use of crypto assets to facilitate sanctions evasion, obscure beneficiary identity, and move value across borders outside of traditional financial controls. In response, DABs applied enhanced monitoring, restricted account activity, and submitted SARs/STRs to ensure timely escalation to the FIA. Overall, the filings underscore the heightened sanctions risk inherent in cross-border digital asset activity and reinforce the critical role of DABs in identifying, reporting, and mitigating exposure to sanctioned actors and jurisdictions within the crypto sector. Sanctioned countries that were featured in DAB filings during this quarter included Russia and Iran.

7.3 Reporting Sector: Money Service Businesses

Classification: Money Laundering

During Q2 2024, MSBs submitted a total of 10 SARs/STRs, all relating to suspected ML activity and originating from a single reporting entity. The filings highlighted a range of red flags centred on abnormal transaction frequency, structuring behaviour, unexplained cash usage, and heightened behavioural risk. Customers were observed sending funds more frequently and in larger amounts than usual, including back-to-back transactions characterised as "gifts," alongside requests for cash in small denominations and repeated transfers to new or unfamiliar recipients, indicative of potential structuring or smurfing. Several customers were reluctant or unable to provide source-of-funds information, including unemployed individuals attempting to send funds, while others sought to transact on behalf of blocked or restricted customers. Additional concerns arose from the nature of cash presented, including large rolls bound with rubber bands, strong odours of marijuana or potpourri, customer attempts to identify camera locations, and preferences for large BMD denominations. Geographic risk was also evident, with funds sent domestically and internationally to jurisdictions including the Dominican Republic, Jamaica, the USA, St. Lucia, the UK, Australia, New Zealand, Laos, and France, often supported by vague, illogical, or invalid send reasons. Behavioural indicators included recipient agitation following transaction cancellations and attempts to circumvent MSB controls. In response, MSBs implemented transaction cancellations, customer blocking, enhanced monitoring, and placement of customers on internal watchlists. No romance or investment scams were reported during the quarter; however, the breadth of indicators selected—ranging from cash exchange activity and no source of funds to suspect comportment and third-party sending—underscores the continued ML risk within the MSB sector and the importance of vigilant frontline controls.

7.4 Reporting Sector: Securities: Investment Businesses

Classification: Money Laundering

Investment Businesses identified suspected ML activity primarily through frequent withdrawals in amounts below USD 100,000 followed by reinvestment in significantly larger sums, behaviour that was inconsistent

with the client's stated rationale of portfolio rebalancing and profit-taking. Additional concerns arose from formal legal cooperation requests, including notifications from Central American authorities and a foreign District Attorney's office relating to investigations into ML and drug trafficking rings, in which account holders linked to corporate clients of the reporting entities were identified. These cases demonstrate heightened exposure to organised cross-border criminal activity and the use of investment platforms to layer and recycle illicit proceeds.

Classification: Tax Offences

Suspected tax evasion filings were driven by third-party fund movements and non-cooperation with regulatory and tax reporting requirements. Notably, a client admitted to routing funds for a new account application through a banker's personal account to "get around red tape," raising concerns regarding deliberate circumvention of controls. Further red flags included persistent failure of US-citizen UBOs to execute required W-9 forms, despite repeated outreach, and rejected outbound transfers where the receiving bank declined the transaction and reasons for rejection remained outstanding. Customers involved in these cases were of Korean, American, and Bahamian nationality, highlighting international tax exposure risks.

Classification: Corruption, Bribery, and Theft

Filings under this classification were triggered by adverse media and unverifiable sources of wealth, including inheritance claims that could not be substantiated through documentation. Jurisdictional exposure in these cases included Panama, Ireland, and Mexico, and notably involved a filing linked to the Odebrecht case, widely recognised as one of the most significant corruption scandals in recent South American history. No consent requests were filed in relation to these matters; however, the cases underscore the reputational and governance risks faced by Investment Businesses with international client exposure.

Classification: Insider Trading / Market Abuse

Market abuse filings centred on suspected front-running and insider trading, involving coordinated trading behaviour by individuals located in close proximity, particularly clients from Hong Kong, and transactions executed immediately prior to market-sensitive announcements. Red flags included short trading histories in specific stocks, conveniently timed positions, abnormal price movements appearing manufactured, and subsequent trading in the opposite direction yielding favourable outcomes. Violations of share acquisition agreements and the use of nominee accounts to acquire additional shares further heightened suspicion. Across these cases, 18 suspect transactions were identified with a total value of approximately USD 1.93 million, involving customers of Israeli, Chinese (Hong Kong), Taiwanese, and Bermudian nationality, including one Israeli client who was reported four times during the quarter. In response, affected trading accounts were disabled where refunds could not be completed, matters were escalated for investigation, and ongoing monitoring remains in place.

Collectively, the filings from the Investment Business sub-sector illustrate the sector's exposure to complex, high-risk activity spanning financial crime, tax misconduct, and market integrity concerns, reinforcing the

importance of robust KYC, transaction monitoring, and cross-border cooperation.

7.5 Reporting Sector: Insurance: Long-Term Insurers

Long-Term Insurers submitted 71 filings during the quarter across a broad range of crime classifications, including ML, fraud, tax evasion, corruption, bribery, insider trading, drug trafficking, and sanctions-related activity. Key risks centred on questionable SoF/SoW, unusual and repeated transfers of policy ownership, large cash premium payments, adverse media, outstanding CDD, and frequent loan and surrender activity indicative of layering and temporary parking of funds. Several cases involved PEP exposure, sanctioned entities, and cross-border risks, with a total recognised suspicious value of approximately USD 11.1 million. While a number of STRs were rejected due to technical or jurisdictional issues, insurers took robust actions including declining new business, exiting relationships, flagging clients as high risk, and seeking FIA consent where applicable, reflecting the sector's heightened exposure to complex, high-value financial crime risks.

7.6 Reporting Sector: Law Firms/Lawyers

Law Firms and Lawyers made two filings during the quarter relating to suspected fraud and ML, driven by atypical payment arrangements, suspected falsification of KYC, inconsistent documentation, and adverse media linking UBOs to serious criminal charges. Matters often involved unusual settlement methods, premature receipt of funds, and unverifiable client information, with a total value of approximately USD 605,900. Actions taken included refraining from banking suspect instruments and formally seeking FIA consent where court-ordered policy surrenders and onward transfers were requested, reflecting a cautious approach to mitigating legal and reputational risk.

7.7 Reporting Sector: Corporate Service Providers (CSPs)

CSPs submitted two filings during the quarter relating to fraud, ML, and corruption, all connected to the same underlying matter. Red flags included exposure to Canadian sanctions, use of corporate structures for unclear purposes, prolonged non-responsiveness by UBOs, and evidence of fraudulent signatures on corporate documents. In response, CSPs undertook enhanced monitoring, escalated concerns internally, resigned from corporate roles, terminated client relationships, and notified the BMA as appropriate. The filings highlight governance and integrity risks within complex corporate arrangements where transparency and cooperation are lacking.

8.0 Key Report Indicators

Across the Banking, DAB, MSB, Securities, Insurance, and stakeholder filings in Q2 2024, several recurring indicators consistently signalled elevated financial crime risk. Core cross-sector indicators included adverse media, fraud, ML, inconsistent account activity, refusal or inability to provide SoF/SoW, and suspect comportment, often compounded by high-risk countries, third-party involvement, and repeated or prior filings on subjects or entities. Banking and MSB reports were particularly characterised

by cash-intensive typologies—such as large or structured cash deposits, BMD/USD cash exchanges, smurfing, split transactions, unexplained wires, and lack of evidence of travel—alongside elder abuse, BEC, identity theft, and misuse of accounts. DAB filings frequently highlighted crypto-specific risks, including hacking, theft, sanctions exposure, imposter and investment scams, and rapid flow-through activity with no apparent economic purpose. Investment Businesses reported higher-end risks such as market abuse, insider trading, corruption, bribery, tax evasion, nominee and shell company usage, and PEP exposure, while Long-Term Insurers reflected complex ML and fraud risks linked to adverse media, sanctions, embezzlement, misrepresentation, structuring, and the use of insurance products to facilitate illicit value movement. CSP and legal sector filings reinforced governance and integrity concerns, including false documents, dormant entities reactivated, charities or corporate vehicles misused, collusion, and legal arrangements involving real estate and trusts. Collectively, these indicators underscore persistent vulnerabilities across cash, crypto, corporate, and professional services channels, with convergence around concealment of beneficial ownership, misuse of legitimate structures, and attempts to evade regulatory and KYC controls.

-END -