Q3 QUARTERLY STATISTICS REPORT

JULY - SEPTEMBER 2024

Financial Intelligence Agency

BERMUDA

Financial Intelligence Agency
Bermuda
QUARTERLY REPORT
July 1st to September 30th, 2024

1.0 Table of Contents

KEY STATISTICS

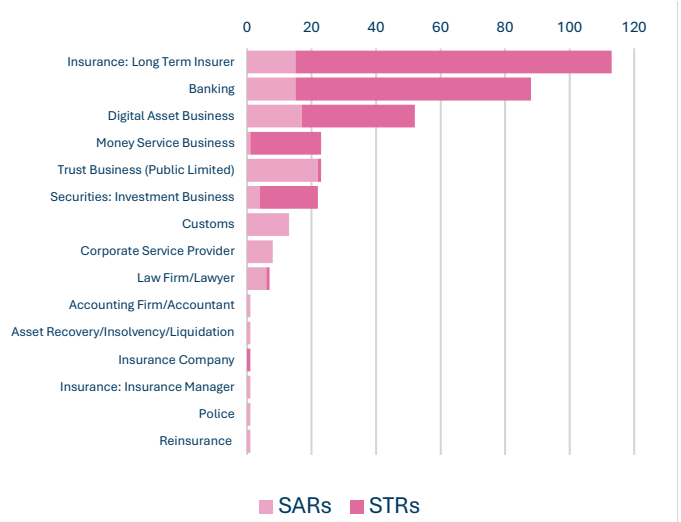
Total Incoming Reports	Highest Reporting Sector	Total Monetary Values (SARs/STRs)
389	LTIs	$78,348,610.97

Q3 2024 Reporting (Q2 Comparison)

AIFs	2	=	0%
C-SARs			
C_STRs			
CTRs			
IRIs	13	▼	-52%
SARs	106	▲	82%
STRs	249	▲	144%
UIRs	19	▼	-30%

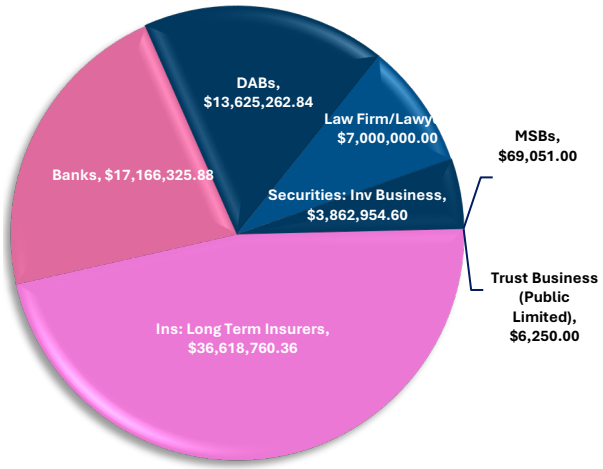
Largest Reporting Sectors

(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
UTR	Unsolicited Intelligence Reports
C-SAR	Consent SAR Requests
C-STR	Consent STRs

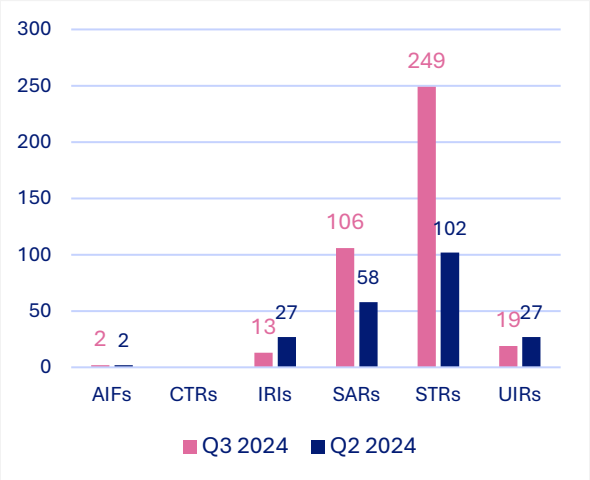
1.0 Introduction

This Q3 2024 report provides an overview of suspicious reporting, intelligence exchange, and financial crime trends identified by the Financial Intelligence Agency (FIA) during Q3 2024. The reporting period was characterised by a significant resurgence in suspicious activity, driven primarily by a sharp increase in Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) across multiple sectors, notably banking, long-term insurance, digital asset businesses (DABs), trust structures (TSPs), and professional service providers. The data reflects heightened detection of money laundering (ML), fraud, corruption, tax evasion, sanctions evasion, and emerging risks linked to terrorist and proliferation financing, alongside increasing transaction-led reporting in high-value and cross-border contexts. While intelligence-led requests and unsolicited disclosures (UIRs) moderated compared to the previous quarter, the overall reporting landscape in Q3 2024 demonstrates strengthened vigilance by reporting entities, improved escalation of complex typologies, and continued reliance on domestic and international cooperation mechanisms. Collectively, the findings underscore evolving financial crime risks within both traditional and non-traditional financial channels and reinforce the FIA's central role in safeguarding Bermuda's AML/CFT/CPF framework through analysis, intelligence dissemination, and regulatory coordination.

2.0 Incoming Reports & Requests

During Q3 2024, the FIA recorded a total of 389 incoming reports and requests, representing a significant increase compared to 216 filings received in Q2 2024. This rise was driven by substantial growth in suspicious reporting, with SARs increasing from 58 to 106 and STRs rising sharply from 102 to 249, indicating a marked escalation in both activity-based and transaction-based reporting across sectors. AIF volumes remained stable at two filings across both quarters, while CTRs continued to record no submissions during the period. In contrast, IRIs declined from 27 in Q2 2024 to 19 in Q3 2024, suggesting a reduction in formal investigative information requests from domestic and international counterparts. UIRs also decreased from 27 to 19 quarter-on-quarter, reflecting lower volumes of spontaneous intelligence referrals. Overall, Q3 2024 demonstrates a pronounced rebound in suspicious reporting activity, particularly STR-driven, reinforcing increased detection and escalation of potential ML/TF and related financial crime risks, notwithstanding a moderation in intelligence-led requests and unsolicited disclosures.

Chart 1 - Reports received by FIA for Q3 2024 vs Q2 2024



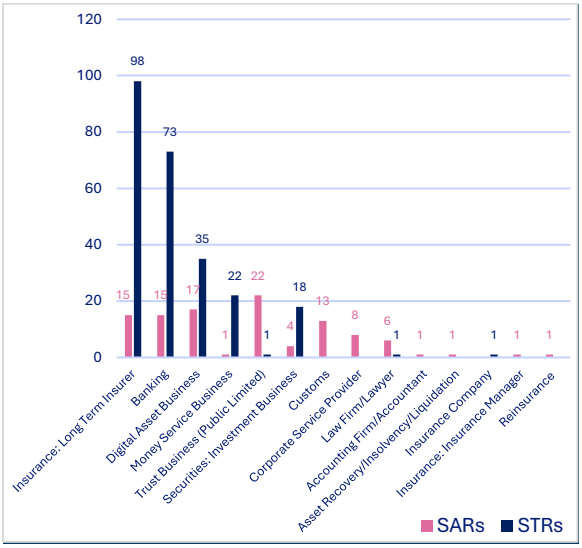
Source: FIA (2024)

3.0 SARs/STRs Reporting

3.1 SARs / STRs by Reporting Sector

In Q3, SAR/STR submissions were concentrated primarily within the banking, LTI, DAB and Trust sectors, reflecting heightened detection of transaction-driven and high-value suspicious activity. Banks and LTIs accounted for the largest volumes of STRs, submitting 73 and 98 STRs respectively, alongside 15 SARs each, underscoring continued exposure to complex ML and fraud typologies within traditional financial and insurance products. DABs filed a combined 52 reports (17 SARs and 35 STRs), highlighting ongoing risk within the virtual asset sector, while MSBs submitted 22 STRs and one SAR, consistent with cash-intensive risk profiles.

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

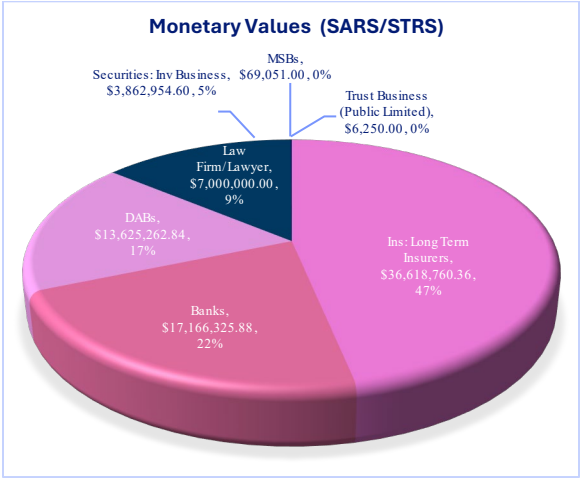


Source: FIA (2024)

Trust Businesses (Public Limited) recorded a higher proportion of SARs (22), and Securities: Investment Businesses reported 18 STRs and four SARs, reflecting transaction-led risk within capital markets. Smaller but relevant contributions were made by CSPs, Law Firms, Customs, and other professional sectors. Overall, Q3 2024 reporting reflects a strong concentration of STR activity among banks, LTIs, DABs, and MSBs, with SARs more broadly distributed across fiduciary and professional reporting entities.

3.2 SARs/STRs by Monetary values

Chart 3 Monetary values of SARs/STRs by Sectors



In Q3 2024, the aggregate monetary value associated with SARs/STRs totalled approximately USD 78.35 million, reflecting a concentration of higher-value suspicious activity within the insurance, banking, and digital asset sectors. LTIs accounted for the largest share, reporting USD 36.62 million, followed by banks at USD 17.17 million and DABs at USD 13.63 million, underscoring continued exposure to complex, high-value transactions across these sectors. Law Firms/Lawyers reported USD 7.0 million, primarily linked to isolated but material cases, while Securities: Investment Businesses accounted for USD 3.86 million, reflecting transaction-driven risk within capital markets. Lower values were reported by MSBs (USD 69,051.00), Trust Businesses (Public Limited) (USD 6,250.00), and Insurance Companies (USD 6.30). Overall, the distribution highlights that while reporting volumes may be broad-

based, the majority of financial exposure during Q3 2024 remained concentrated within LTIs, banks, and DABs. *(Refer to Chart – Highest Monetary Values on Key Statistics page)*

FIA notes that reported monetary values vary in accuracy, as several sectors, particularly DABs, continue to submit filings with incorrect, inconsistent, or incomplete suspicious transaction values. As such, the monetary figures presented should be interpreted with caution and may not fully reflect the true value of suspicious activity reported during Q3 2024.

SARs/STRs by Suspected Offences

In Q3 2024, SAR and STR filings reflected a broad spectrum of suspected criminal activity, with ML and fraud remaining the predominant offence categories across reporting sectors. Money laundering accounted for the highest volume, comprising 36 SARs and 100 STRs, followed closely by fraud with 33 SARs and 74 STRs, underscoring the continued dominance of transaction-driven and deception-based financial crime risks. Corruption also featured prominently, generating 17 SARs and 8 STRs, while tax offences were more transaction-focused, with a comparatively low number of SARs (3) but a higher volume of STRs (18). Market integrity risks were evident through 20 STRs relating to insider trading and market abuse, alongside 18 STRs linked to money laundering involving cash exchange activity. Drug trafficking-related concerns resulted in 11 SARs and 2 STRs, indicating entity-level suspicion with limited transactional escalation. Lower-frequency but high-risk offences included bribery (4 SARs and 4 STRs), sanctions-related activity (1 SAR and 3 STRs), terrorist financing (1 SAR and 1 STR), and a single STR linked to WMD proliferation. Overall, the offence profile for Q3 2024 demonstrates a strong concentration on money laundering and fraud, with STRs significantly outnumbering SARs across most categories, reflecting a continued emphasis on transaction-led detection and reporting.

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

#	Crime Classification	SARs	STRs	Total
1.	Money Laundering	36	100	**136**
2.	Fraud	33	74	**107**
3.	Corruption	17	8	**25**
4.	Tax Offences	3	18	**21**
5.	Insider Trading (Market Abuse)		20	**20**
6.	Money Laundering – Cash Exchange Related		18	**18**
7.	Drug Trafficking/ Narcotics	11	2	**13**
8.	Bribery	4	4	**8**
9.	Sanctions Related	1	3	**4**
10.	Terrorist Financing	1	1	**2**
11.	WMD Proliferation		1	**1**
	TOTAL	**106**	**249**	**355**

Source: FIA (2024)

4.0 International and Domestic Cooperation

4.1 Incoming Requests for Information / Spontaneous Disclosures (UIRs)

During Q3 2024, the FIA received a total of 32 incoming requests and unsolicited intelligence disclosures, reflecting continued domestic and international cooperation. Incoming Requests for Information (IRIs) accounted for 13 filings, the majority of which originated from Local Law Enforcement, with the Bermuda Police Service (BPS) submitting nine (9) requests, underscoring ongoing reliance on FIA intelligence to support active investigations. The remaining IRIs were received from Egmont Group Foreign FIUs (FFIUs), totalling four (4), and originating from Bangladesh, the British Virgin Islands (BVI), Jersey, and the United States, demonstrating

sustained cross-border engagement. Unsolicited Intelligence Reports (UIRs) comprised 19 filings, predominantly submitted by Local Law Enforcement, with HM Customs accounting for seventeen (17) disclosures, indicating a strong flow of spontaneous domestic intelligence. An additional two (2) UIRs were received from Egmont FFIUs, specifically Argentina and Malta. Overall, the composition of IRIs and UIRs in Q3 2024 highlights robust cooperation with domestic law enforcement and continued, albeit more targeted, engagement with international FIU counterparts.

Table 2 Incoming IRIs / UIRs in Q3 2024

Reporting Sector	# of Filings
IRIs	
Egmont (FFIUs)	4 (Bangladesh, BVI, Jersey, USA)
Local Law Enforcement	9 (BPS 9)
Supervisor/Regulator	0
UIRs	
Local Law Enforcement	17 (HM Customs)
Egmont (FFIUs)	2 (Argentina, Malta)

Source: FIA (2024)

4.2 Outgoing Requests for Information (Domestic & International)

During Q3 2024, the FIA disseminated a total of 60 outgoing Requests for Information (RFIs), reflecting active intelligence development and sustained engagement with both domestic and international counterparts. Section 16 Requests to domestic reporting entities accounted for the largest proportion, totalling 33 filings, and were primarily utilised to obtain beneficial ownership information, transaction records, and supporting intelligence in aid of ongoing analytical and law enforcement enquiries. A further one (1) outgoing request was directed to a domestic competent authority, indicating limited but targeted domestic inter-agency escalation during the quarter. International cooperation remained robust, with 26 outgoing RFIs issued to Foreign FIUs (FFIUs) across a broad range of jurisdictions, including Andorra, Azerbaijan, Barbados, the BVI, Indonesia, the Isle of Man, Malaysia, Mexico, Peru, Portugal, Singapore, Switzerland, and the USA. Overall, the volume and geographic spread of outgoing RFIs underscore the increasingly cross-border nature of ML, fraud, and related financial crime risks identified during Q3 2024, and the FIA's continued reliance on international cooperation mechanisms to support complex investigations.

Table 3 Outgoing RFIs disseminated in Q3 2024

	Report Types	# of Filings
1.	Section 16 Requests (Reporting Entities - Domestic)	33
2.	Outgoing Requests for Domestic (Competent Authorities)	1
3.	Outgoing Requests for Information (International)	26 (Andorra, Azerbaijan, Barbados, BVI, Indonesia, Isle of Man, Malaysia, Mexico, Peru, Portugal, Singapore, Switzerland, USA)

Source: FIA (2024)

5.0 Consent Letters

During Q3 2024, the FIA maintained its consent framework for higher-risk matters, issuing Consent Letters in response to SARs and STRs where reporting entities sought approval to proceed with transactions or activities assessed as suspicious. Of the 68

consent-seeking filings received during the quarter, ten (10) formal Consent Letters were issued, arising from reports submitted by Long-Term Insurers, commercial banks, and the BPS, with consent implied in respect of the remaining requests. This approach reflects the FIA's continued focus on proportionate regulatory oversight, timely decision-making, and clear communication with reporting entities, while ensuring that higher-risk transactions are subject to appropriate scrutiny prior to execution.

6.0 Intelligence Reports (Response / Spontaneous Disclosures)

6.1 Outgoing Disclosures

During Q3 2024, the FIA disseminated a total of 49 outgoing intelligence reports across response and spontaneous disclosure channels, reflecting sustained domestic and international engagement. No response disclosures were issued to local competent authorities during the quarter; however, five (5) response disclosures were provided to Local LLEAs, alongside three (3) response disclosures to Egmont FIUs, supporting active international intelligence requests. Proactive intelligence sharing remained a key feature of the FIA's operational output, with three (3) spontaneous disclosures issued to local competent authorities, specifically the AML/ATF Board, Registrar General (1) and the Financial Sanctions Implementation Unit (FSIU) (1). A further twenty-four (24) spontaneous disclosures were disseminated to LLEAs, predominantly to the BPS (15) and HM Customs/JIU (9), underscoring strong domestic law enforcement cooperation. International engagement was also robust, with fourteen (14) spontaneous disclosures shared with Egmont FIUs across a broad range of jurisdictions, including the BVI, Cyprus, Guatemala, Ireland, Israel, Kyrgyz Republic, Malta, Palestine, Panama, Slovenia, Switzerland, Turkey, the UK, and the USA, highlighting the FIA's continued role in facilitating cross-border intelligence exchange in support of ML/TF/PF risk mitigation.

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)

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: Insurance: Long-Term Insurers

Classification: Money Laundering

During Q3 2024, LTIs identified suspected ML activity characterised by policy circumvention, sanctions exposure, and questionable source of funds (SoF) / source of wealth (SoW). Key patterns included repeated transfers of policy ownership between the same parties over extended periods, pass-through account behaviour involving rapid inflows and outflows across Chinese and UK

bank accounts, and significant credit activity (exceeding USD 1 million within six months) that was inconsistent with customer profiles. Sanctions screening further identified exposure to OFAC-designated SDNs operating within the Russian technology sector, as well as residential addresses subject to US export control restrictions linked to counter-Russian aggression measures, elevating ML and sanctions-evasion risk.

Classification: Bribery

Bribery-related filings were driven primarily by adverse media and screening results, where policyholders were positively matched to individuals previously convicted of bribery offences. These cases were assessed as high risk due to the nature of the predicate offence and the potential use of insurance products to conceal or legitimise the proceeds of corruption.

Classification: Proliferation Financing (Suspected)

LTIs reported PF concerns arising from links to the export of potential dual-use goods to high-risk jurisdictions, including North Korea (DPRK), coupled with a lack of transparency and refusal to provide supporting documentation. Additional risk was identified where policyholders held beneficial ownership in companies transacting with networks connected to a Chinese entity indicted by US authorities for PF activity, indicating indirect exposure to proliferation-linked financial networks.

Classification: Drug Trafficking

Drug-trafficking-related risk was identified through adverse media and World-Check screening, where applicants were matched to confirmed convictions for drug trafficking offences. Despite this background, affected individuals sought to establish new insurance policies, prompting reporting due to the elevated risk that policies could be funded with or used to launder criminal proceeds.

Classification: Fraud

Fraud-related SARs and STRs reflected a wide range of typologies, including embezzlement, forged documentation, telecom fraud, crypto-related theft, and asset concealment. Red flags included policyholders sentenced to lengthy prison terms for financial crimes, the use of multiple passports, dubious bills of lading, misrepresentation of long-standing commercial relationships, and ownership transfer requests linked to known fraud networks. Several cases involved crypto as a declared SoF, where blockchain analysis identified exposure to addresses linked to major fraud schemes, leading to declined business and escalation to the FIA.

Classification: Tax Evasion

Tax evasion concerns were identified through adverse media, FATCA non-compliance, and opaque ownership and residency structures. Indicators included the use of overseas ATMs to extract cash following corporate or familial transfers, transfer-of-ownership requests inconsistent with stated residency and banking arrangements, refusal to provide FATCA documentation, and reliance on citizenship or residence-by-investment passports that conflicted with actual residence and business activity. These patterns suggested deliberate attempts to obscure tax obligations across multiple jurisdictions.

Classification: Market Abuse

Market abuse risk was identified in limited cases where policyholders were the subject of active police investigations into false trading, price rigging, or stock market manipulation. Intelligence received from financial crime authorities prompted reporting due to the potential linkage between capital market abuse and the laundering of illicit gains through insurance products

7.2 Reporting Sector: Banking

Classification: Money Laundering

Bank filings highlighted high-value credits and cash deposits followed by international wire transfers, primarily to the UK and USA, where the origin of funds could not be adequately explained. Several cases involved previously dormant or low-activity accounts that became active abruptly, receiving large inbound wires from unknown third parties. Transaction flows were often inconsistent with stated account purposes, including trust accounts remitting funds to multiple unrelated parties and personal accounts being used to facilitate business-related wires. In several instances, banks observed aggregation of large cash deposits over short periods, materially inconsistent with the customer's profile or historical activity.

Classification: Sanctions Evasion and Jurisdictional Risk

Sanctions-related concerns featured prominently, particularly in cases involving Russian-linked customers or shareholders. Banks identified attempts to circumvent restrictions by opening accounts in alternative jurisdictions to facilitate outbound transfers, following an inability to move funds locally due to sanctions constraints. Changes in residency status and cross-border account structuring raised concerns of sanctions evasion and concealment of beneficial ownership, warranting enhanced scrutiny and reporting.

Classification: Source of Funds/Cash-Intensive Behaviour

Multiple filings involved large BMD cash deposits where customers—often retired or with limited declared income—were unable to substantiate SoF. In some cases, deposited cash exceeded the customer's annual income, while others involved currency mismatches (USD withdrawals followed by equivalent BMD deposits) without credible explanations. Claims of gambling winnings were not supported by verifiable documentation, and in several instances, no SoF was provided despite account restrictions or blocking, escalating ML concerns.

Classification: Behavioural Risk and Non-Cooperation

Banks also reported elevated behavioural risk, including abusive or threatening communications from customers or their relatives, deliberate attempts to avoid enhanced due diligence, and refusal to provide identification documents—particularly in cases involving elderly customers. Some customers opted to terminate relationships rather than comply with SoF or Know Your Customer (KYC) requests, while others were already known persons of interest to local LEAs, further heightening risk.

Classification: Adverse Media and Business Profile Concerns

Adverse media linked to drug trafficking and other criminal activity featured in several cases, reinforcing suspicions regarding the legitimacy of funds. Corporate filings also revealed unclear or misrepresented business models, including entities operating in a manner inconsistent with their stated purpose (e.g. gaming-style activity presented as a members' club), alongside contradictory or unreliable supporting documentation. Collectively, these indicators supported ML concerns and, in some cases, prompted account restrictions, exits, or escalation to LEAs.

Classification: Suspected Money Laundering Involving Cash Exchanges

During Q3 2024, banks reported SARs/STRs identifying suspected ML linked to cash exchange activity that was inconsistent with customer profiles and indicative of potential criminal proceeds. Key red flags included cash deposits emitting a strong odour of marijuana masked with perfume, suggesting concealment, alongside repeated cash exchanges conducted without credible justification. In several cases, customers were unable to demonstrate any legitimate travel purpose despite conducting currency exchanges, stating vague or non-existent travel plans. Transactional behaviour was also inconsistent with stated account usage, including customers who claimed accounts were used solely for bill payments but conducted multiple deposits across various currencies. Assertions that funds were derived from casino winnings were unsupported by documentary evidence, and no verifiable SoF was provided despite follow-up requests. Collectively, these indicators raised concerns regarding laundering through cash exchanges, particularly involving vulnerable individuals and USD-denominated transactions.

Classification: Suspected Fraud

Banks also submitted filings identifying a broad range of fraud typologies, frequently underpinned by social engineering, impersonation, and payment diversion schemes. Adverse domestic media featured in several cases, indicating that credited funds may have originated from illegal activity. One complex matter involved exposure to the Azerbaijani Laundromat, where nominee directors, officers, and beneficial owners linked through nested corporate structures were identified as existing local bank customers, raising concerns of organised financial crime and corruption.

Imposter scams were a recurring theme, particularly affecting senior citizens. Victims were contacted by fraudsters impersonating local bank staff or telecommunications officials and were persuaded that their accounts had been compromised. In several instances, customers were convinced to install remote-access software, transfer funds to purported "safe accounts," or cooperate with one imposter to identify another, resulting in full account compromise. Additional fraud typologies included real estate fraud, where corporate customers acted without proper authority in estate-related transactions or attempted property purchases using dubious SoF, as well as phishing attacks involving unauthorised transfers between local banks. Business Email Compromise (BEC) and payment diversion fraud were also identified,

where intercepted communications or altered invoice instructions led to funds being sent to fraudulent overseas accounts, with limited recovery prospects.

7.3 Reporting Sector: Digital Asset Businesses (DABs)

Classification: Fraud

During Q3 2024, DABs identified multiple fraud-related typologies primarily associated with onboarding risk, misuse of identities, exposure to illicit actors, and scam-related activity. Several prospective clients were rejected at onboarding following true positive AML screening results, demonstrating the effectiveness of upfront controls. Red flags included the use of generic email domains hosted in jurisdictions inconsistent with declared residency, raising concerns regarding identity masking and account fabrication.

Direct and indirect exposure to illicit actor-linked blockchain addresses was identified, including addresses attributed to webhp and Simbolika, both associated with Breached.co, a known hacking forum. In addition, several accounts were linked to investment scam activity, including receipt of funds from high-risk exchanges such as eXch.cm and interaction with wallets known to facilitate scam transactions. In some cases, it remained unclear whether customers were victims or beneficiaries of the underlying scam activity.

Further concerns arose from false identification and misrepresentation, where a single individual operated multiple accounts using fabricated identities and generic email naming conventions consistent with scam-related behaviour. One customer admitted to creating multiple accounts under false names due to perceived regulatory or political constraints in their home jurisdiction. Exposure to unlabelled wallets was also identified, including indirect Litecoin transfers linked to potential scam activity. In one corporate case, the beneficial owner was alleged to have misappropriated customer funds, withdrawing monies held at the DAB via multiple bank wires, giving rise to both fraud and ML concerns.

Classification: Money Laundering

DAB filings during the quarter also highlighted suspected ML activity characterised by rapid transaction velocity, lack of economic rationale, sanctions exposure, and non-cooperation with due diligence requests. A recurring typology involved rapid “crypto-in, crypto-out” behaviour, where customers repeatedly purchased and sold cryptocurrency within very short timeframes, incurring transaction fees without any clear commercial purpose. Transaction volumes significantly exceeded peer benchmarks, with activity levels more than three times the median for comparable customers over a 90-day period.

In several cases, accounts intended for the safeguarding of digital dollars were instead used for high-frequency flow-through activity, including the receipt of substantial crypto assets followed by immediate off-platform transfers. One customer conducted over 30 transactions within two months, transferring approximately USD 500,000 to other exchanges and unlabelled wallets. These patterns were compounded by failure or

refusal to provide SoF documentation, despite repeated requests.

Sanctions-related ML risks were also identified, particularly within corporate accounts where board members were listed on the OFAC SDN List for providing asset management services to sanctioned Russian nationals, calling into question the legitimacy of deposited funds. Additional high-risk indicators included direct exposure to darknet market addresses and both direct and indirect interaction with addresses associated with Nobitex.ir, categorised as a sanctioned jurisdiction. In response, DABs escalated concerns through SAR/STR submissions, enhanced monitoring, and, where appropriate, account restrictions or rejection.

7.4 Reporting Sector: Trust Service Providers (TSPs)

The crime classifications identified within the TSP reporting sector during Q3 2024 included Fraud, Terrorism, Terrorist Financing (TF), Corruption, Bribery, Tax Evasion, and Money Laundering (ML). In total, 23 filings were submitted by TSPs, all relating to heightened integrity and compliance concerns within a limited number of trust relationships.

Filings from this sector were primarily driven by adverse media exposure and persistent refusal by clients to comply with KYC/CDD requirements, despite repeated requests. The adverse media identified referenced serious predicate offences, including corruption, bribery, tax evasion, and terrorism-related activity, in some cases involving foreign PEP exposure and associations disclosed through large-scale data leaks such as the Paradise Papers. The lack of cooperation from clients in addressing these risks significantly impeded the TSP's ability to satisfactorily assess and mitigate ML/TF exposure.

In response, the TSP submitted the filings for FIA information purposes, highlighting elevated risk indicators and ongoing concerns regarding transparency, governance, and regulatory compliance within the affected trust structures.

7.5 Reporting Sector: Money Service Businesses (MSBs)

Classification: Fraud

Fraud-related filings were dominated by elder abuse and romance scam typologies, primarily affecting senior citizens. Customers were observed sending funds to individuals they claimed to know personally, often describing romantic relationships with overseas recipients—frequently located in Africa—whom they had never met in person. In several cases, family members intervened to advise the MSB that the customer had been scammed, while victims continued to receive persistent calls and harassment from unknown numbers.

Additional red flags included frequent changes to recipient details, implausible explanations for the inability of recipients to provide identification (e.g. claims of undercover military work), and repeated attempts to circumvent controls by visiting multiple MSB branches after transactions were challenged or blocked. Newly onboarded senior citizens were noted to send large sums shortly after registration approval, sometimes successfully and sometimes unsuccessfully, further indicating grooming and manipulation by scam networks.

Classification: Money Laundering

ML-related filings highlighted patterns of previously inactive customers re-engaging after prolonged periods and sending funds to the same destinations and receivers as other customers, suggesting possible coordination. Structuring behaviour was also observed, with customers sending funds below reporting thresholds using a single form of identification. In some cases, multiple individuals were identified sending funds to identical recipients and jurisdictions, raising concerns regarding third-party control and organised activity.

Reporting Sector: Securities – Investment Business

During Q3 2024, Investment Businesses identified suspected Fraud, Money Laundering (ML), Corruption, Bribery, Tax Evasion, and Market Abuse, with red flags spanning documentation integrity, adverse media exposure, and trading behaviour. Fraud-related concerns included the submission of potentially altered or fabricated bank statements, identified through metadata analysis and inconsistencies in PDF properties, as well as misrepresentation and accounting irregularities where estimated earnings ratios did not align with sector comparators. Corruption and tax evasion risks were primarily driven by adverse media linking subjects to PEPs convicted or accused of serious financial crimes, and by suspicions that proceeds from family businesses associated with bribery and fraud were being intermingled with client funds. ML concerns were further elevated where entities were in regions with known organised crime influence, raising questions regarding the origin of funds. Market abuse filings reflected classic rumour-driven trading typologies, including accounts with no prior trading history entering positions following unconfirmed takeover speculation, and coordinated trading by multiple individuals with no historical exposure to the stock. Collectively, the filings underscore the sector's exposure to integrity risks across onboarding, transaction monitoring, and market conduct.

7.6 Reporting Sector: Corporate Service Providers (CSPs)

CSP filings during Q3 2024 reflected suspected Money Laundering, Fraud, Bribery, and Corruption, driven by transparency failures, adverse media, and governance concerns within trust and foundation structures. ML-related indicators included refusal or reluctance to provide SoW/SoF, combative behaviour during customer due diligence (CDD) enquiries, and undue urgency to complete onboarding, suggesting attempts to circumvent controls. Additional risk arose from PEP involvement, adverse media linked to the jurisdiction of grantor trusts, and reputational concerns surrounding the underlying structures. Fraud indicators included misrepresentation, where purported SoF documentation was supported by non-official email domains. More serious concerns were raised through whistleblower information alleging misappropriation of funds from domestic trusts holding Bermuda real estate, as well as adverse media indicating that Bermuda trust structures may have been established to shield assets from foreign law enforcement action. In response,

CSPs escalated concerns through SAR filings and enhanced scrutiny of affected relationships.

7.7 Reporting Sector: Law Firms / Lawyers

In Q3 2024, Law Firms submitted filings relating to suspected Fraud and Bribery, driven by atypical client approaches, falsified documentation, and whistleblower intelligence. Red flags included cold calls requesting urgent CSP services, prospective clients openly shopping for alternative Bermuda CSPs, and refusal to comply with CDD requirements, including attempts to minimise or bypass regulatory obligations. Fraud risks were heightened by the identification of forged documents, including promissory notes bearing identical signatures across unrelated transactions, and correspondence falsely signed by a deceased Bermuda partner. Additional indicators included misrepresentation of prior professional relationships, abnormal communication methods inconsistent with standard legal instructions, lack of any credible online presence despite claims of substantial commercial backing, and the use of informal Gmail accounts with poor drafting and no professional sign-off. Law firms declined the engagements, ceased communications, closed all related matters, and filed SARs where reasonable suspicion of criminal conduct arose.

7.8 Reporting Sector: Accounting Firms

One filing was submitted by an Accounting Firm during Q3 2024, identifying suspected Money Laundering and Fraud. ML concerns arose following allegations by a creditor that the UBO's acquisition of a company may be linked to laundering activity, raising doubts about the legitimacy of the transaction. Fraud risks were compounded by adverse media indicating prior fraud charges against the client. Given the presence of reasonable grounds for suspicion, the accounting firm reported the matter pursuant to section 46(A1) of POCA, highlighting the role of professional service providers in identifying early-stage financial crime risk.

7.9 Reporting Sector: Reinsurance

The Reinsurance sector recorded one filing in Q3 2024 relating to suspected Money Laundering and Fraud. Enhanced due diligence identified adverse media concerning a potential investor, including criminal management bans imposed in Europe for allegedly raising funds and selling investment products without appropriate authorisation. Given the severity of the findings and associated reputational risk, the reinsurer terminated negotiations with the counterparty and escalated the matter through formal reporting.

7.10 Reporting Sector: Insurance – Insurance Manager

During Q3 2024, one filing was submitted by an Insurance Manager relating to suspected Money Laundering. The filing was triggered through ongoing screening, where Dow Jones monitoring identified adverse media linked to the UBOs of a South American parent

company and an associated Bermuda-regulated entity. The case highlights the importance of continuous monitoring in identifying evolving ML risk post-onboarding, particularly within cross-border insurance structures.

8.0 Key Report Indicators

Across all reporting sectors in Q3 2024, the report indicators collectively selected by reporting entities demonstrate a broad and persistent pattern of elevated financial crime risk spanning money laundering, fraud, corruption, bribery, tax evasion, sanctions exposure, terrorist financing, and market abuse. Core indicators most frequently cited across filings included adverse media, refusal or inability to provide CDD/SoF/SoW, misrepresentation and false or altered documentation, suspect comportment, and inconsistent or unexplained account activity, often coupled with attempts to expedite onboarding or circumvent established controls. Cash and transaction-based indicators—such as large or structured cash deposits, high-value or rapid cross-border transfers, use of personal accounts for business purposes, and pass-through or flow-through activity—featured prominently within banking and MSB reports, while crypto-specific indicators including exposure to illicit actors, darknet markets, unlabelled wallets, rapid crypto in/crypto out activity, and sanctions-linked jurisdictions were prevalent among DAB filings. Professional service providers, including CSPs, law firms, accountants, insurers, and investment businesses, consistently reported governance and integrity risks, notably PEP exposure, shell or trust structures, forged or unreliable documents, whistleblower intelligence, and efforts to conceal beneficial ownership or shield assets from authorities. Market integrity indicators—such as insider trading, market abuse, rumour-driven trading, and coordinated activity with no prior trading history—were also observed, alongside emerging risks linked to organised crime, drug trafficking, proliferation financing, and terrorism-related concerns. Taken together, the indicators selected in Q3 2024 reflect convergence across cash, crypto, corporate, and professional services channels, underscoring systemic vulnerabilities associated with opacity, misuse of legitimate structures, and deliberate evasion of regulatory and AML/CFT controls.

-END -