FINANCIAL REPORTING AUTHORITY

2024 ANNUAL REPORT

CAYMAN ISLANDS GOVERNMENT

PORTFOLIO OF LEGAL AFFAIRS

TABLE OF CONTENTS

Message from the Director 3

2024 HIGHLIGHTS 5

I. Legal Framework 6

II. The Financial Reporting Authority 9

1. Background 9

2. Role and Function 9

3. Organisational Structure and Management 12

4. Protecting Confidentiality of Information 14

5. Relationships 14

III. PERFORMANCE REPORTING 19

1. Receiving Information - Suspicious Activity Reports (SARs) 19

2. Analysing Information 27

3. Disseminating Intelligence 34

IV. Scenarios that Would Trigger Filing of a Suspicious Activity Report (Typologies) .. 41

V. Strategic Priorities: performance for 2024 and Building on Strengths in 2025 50

MESSAGE FROM THE DIRECTOR

I am pleased to report on the operations of the Financial Reporting Authority ("FRA") in this annual report for the 2024 financial year ("the Reporting Period"), which marks the twenty second reporting period for the FRA.

As an administrative financial intelligence unit, the FRA is responsible for receiving, requesting, analysing and disseminating financial information disclosures concerning proceeds of criminal conduct or suspected proceeds of criminal conduct. Domestically, the investigation of financial crime and associated offences falls under the ambit of local law enforcement agencies.

The FRA received 1,395 cases during the Reporting Period, comprising 1,194 Suspicious Activity Reports ("SARs") from 291 Reporting Entities; 101 Requests for Information and 43 Voluntary Disclosures from 48 overseas Financial Intelligence Units ("OFIUs"); and 57 Requests for Information from Local Law Enforcement Agencies ("LEAs"). The number of cases received decreased by 7% compared to the number of cases received during 2023 (1,395 vs 1,501).

During 2024 the FRA continued to register users from reporting entities and familiarise them with using the AMLive Reporting Portal in order to electronically submit their reports. At the end of the Reporting Period there were 414 registered users from 212 Reporting Entities; 867 SARs (73%) were filed using AMLive during 2024 and 327 SARs (27%) were filed using secure email.

During the Reporting Period the FRA performed initial analysis on 1,326 cases. It also issued 183 directives pursuant to section 4(2)(c) of the Proceeds of Crime Act ("the POCA") to amplify or clarify information received, or to respond to a request from an OFIU. The FRA also made 46 requests for information to OFIUs, 28 of which were made to assist LEASs with investigations.

The FRA closed 1,107 cases during the Reporting Period, resulting in 449 disclosures to LEAs or competent authorities, and 519 disclosures to OFIUs.

A detailed breakdown of the cases that were analysed and closed, along with details of the disclosures made by the FRA are detailed in Section III of this Annual Report.

During the Reporting Period, the vast majority of the work undertaken by the Sanctions Coordinator was in connection with the ongoing implementation of the unprecedented sanctions imposed against Russia in response to its invasion of Ukraine on 24 February 2022. It was another challenging year for the FRA with workflows similar to 2023, including but not limited to: engagement with industry stakeholders, other competent authorities and partner agencies in the United Kingdom; reviewing and processing licence applications; reviewing and processing Compliance Reporting Forms ("CRFs"); issuing financial sanction notices; issuing ship specification notices; reviewing and commenting on changes to regulations and Orders in Council; and work in connection with the Russia Sanctions Taskforce. Apart from Russia Sanctions, the FRA also continued the actions taken to address recommended actions in the Caribbean Financial Action Task Force ("CFATF") 4th Round Mutual Evaluation Report ("MER") directly related to Targeted Financial Sanctions ("TFS") for terrorist financing ("TF") and proliferation financing ("PF").

During the Reporting Period the FRA also made significant contributions to the work of the Egmont Group, as detailed in the relevant section of this Annual Report.

I would like to take this opportunity to recognise and express my constant appreciation to my staff for their continued commitment to the work of the FRA.

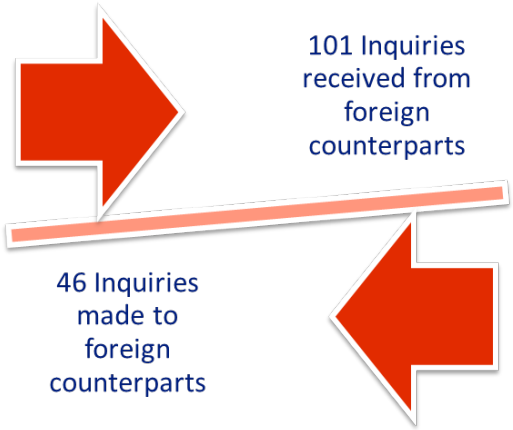
RJ Berry
Director

2024 HIGHLIGHTS

Cases Received and Analysed

Actions Taken & Financial Intelligence Disclosures

Global Contribution



Domestic Action

519 Disclosure to Overseas FIUs

Top 3 Recipients of Overseas Disclosures

FinCEN (US)	NCA (UK)	FIU (Germany)
71	45	31

449 Domestic Disclosures Made

Top 3 Recipients of Domestic Disclosures

RCIP-FCU/CIBFI	CIMA	CBC
244	150	35

Targeted Financial Sanctions

104 Financial Sanctions Notices Issued

I. LEGAL FRAMEWORK

In 2020, the Cayman Islands changed from having a Legislative Assembly to a Parliament. Shortly after, Parliament passed the Citation of Acts of Parliament Law, 2020; under this statute, pieces of legislation formerly referred to as 'Laws' became 'Acts'.

The Cayman Islands fully understands and accepts that operating a financial services centre involves serious obligations. The Cayman Islands Government enforces a strong anti-money laundering (AML), countering the financing of terrorism (CFT) and countering the financing of proliferation (CFP) regime through the following pieces of legislation:

1. The Proceeds of Crime Act (2024 Revision) (" the POCA")

The POCA was introduced in 2008 and consolidated in one place the major anti-money laundering provisions, which were previously in three separate pieces of legislation. The POCA re-defined, clarified and simplified offences relating to money laundering and the obligation to make reports of suspicious activity to the FRA. It also introduced the concept of negligence to the duty of disclosure, and imposed a duty to report if the person receiving information knows, suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct, and such information came to him in the course of business in the regulated sector, or other trade, profession, business or employment.

The POCA also governs the operations of the FRA.

In late 2023, parliament passed the Proceeds of Crime (Amendment) Act, 2023. When Sections 11, 12 and 13 come into force, they will introduce a 'consent regime' to the Cayman Islands and remove the automatic defence contained in sections 133-135 POCA. Work and discussion to draft regulations and develop the infrastructure for receiving, processing and responding to consent requests are at an advanced stage. The relevant amendments will take effect on 2 January 2025.

2. Misuse of Drugs Act (2017 Revision) ("MDA")

The MDA has over the years been amended to give effect to the Cayman Islands' international obligations, and particularly to the United Nations ("UN") Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. The MDA contains measures to deal with drug trafficking and the laundering of the proceeds from such activity. The Act empowers the authorities to seize and confiscate drug trafficking money, and laundered property and assets. The Criminal Justice (International Cooperation) Act (2015 Revision) – originally enacted as the Misuse of Drugs (International Cooperation) Law - provides for cooperation with other countries in relation to collecting evidence, serving documents and immobilising criminally obtained assets in

relation to all qualifying criminal proceedings and investigations.

3. Terrorism Act (2018 Revision) ("TA")

The Terrorism Act is a comprehensive piece of anti-terrorism legislation that, inter alia, implements the UN Convention on the Suppression of Financing of Terrorism.

The 2018 Revision includes the relevant Financial Action Task Force ("FATF") requirements, particularly with regard to "freezing without delay" and reporting obligations of persons in relation to any United Nation Security Council Resolutions related to terrorist financing. The FRA has also assumed responsibilities for coordinating the implementation of targeted financial sanctions in relation to terrorist financing.

4. Anti-Corruption Act (2024 Revision) ("ACA")

Brought into effect on 1 January 2010, the ACA initiated the establishment of the Anti-Corruption Commission ("ACC") and also criminalised acts of corruption, bribery and embezzlement of funds.

The ACA gives effect to the UN Convention against Corruption and the Organisation for Economic Cooperation and Development ("OECD") Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. International cooperation and asset recovery are important components of this legislation including measures to prevent and detect transfers of illegally acquired assets, the recovery of property and return of assets.

5. Proliferation Financing (Prohibition) Act (2017 Revision) ("PFPA")

The Proliferation Financing (Prohibition) Act 2010 conferred powers on the Cayman Islands Monetary Authority ("CIMA") to take action against persons and activities that may be related to terrorist financing, money laundering or the development of weapons of mass destruction. The legislation required CIMA to issue directions, where it reasonably believed that certain activities in these areas were being carried on that posed a significant risk to the interests of the Islands or the United Kingdom (U.K.).

The 2017 Revision brought the PFPA in line with the relevant FATF requirements, particularly with regard to "freezing without delay" and reporting obligations of persons in relation to any United Nation Security Council Resolutions related to proliferation financing. The FRA has also assumed responsibilities for coordinating the implementation of targeted financial sanctions in relation to proliferation financing.

6. The Anti-Money Laundering Regulations (2023 Revision) ("AMLRs")

The AMLRs came into force in January 2023 and repealed and replaced the Money Laundering Regulations (2020 Revision). They align the anti-money laundering framework in the Cayman Islands with the FATF Recommendations.

The AMLRs were amended in 2024

The 2023 Revision incorporates the amendments made in 2017, 2019 and 2020 in one document. These amendments have addressed, inter alia, switching to a risk-based threat, enhanced customer due diligence and eligible introducers, disclosure requirements (including production of information) for persons carrying out relevant financial business and a number of regulations about designated non-financial businesses and professions (DNFBPs). Administrative fines are provided for and are frequently refined.

The AMLRs were amended in 2024, mainly tidying up the language and expanding all regulations to cover AML, CFT and CFP where before only one or two might have been included. The section about assessment of risk has been amended; there is also an increase in the number of regulations relating to Designated Non-Financial Businesses and Professions (DNFBPs) and the scope of supervision and regulation.

There will be a Revision in 2025 incorporating all of the 2024 amendments.

The latest version of the Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (the GNs) were published in February 2024 by The Cayman Islands Monetary Authority (CIMA) under s.34 of The Monetary Authority Law (2020 Revision). These updated GNs incorporate the amendments from 2020 and 2021 which provided additional guidance to Virtual Asset Service Providers and securitisation.

7. Anti-Money Laundering (Money Services Business Threshold Reporting) Regulations, 2020

Regulations passed pursuant to section 145 of the Proceeds of Crime Act (2020 Revision) by the Cabinet - and gazetted in November 2020 - impose a duty on money services businesses (as defined) to make quarterly reports to the FRA regarding single or aggregate transactions in any month in the quarter that equal or exceed US$ 3,500.

8. Anti-Money Laundering (Class A and Class B Bank Threshold Reporting) Regulations, 2022

Regulations passed pursuant to section 145 of the Proceeds of Crime Act (2020 Revision) by the Cabinet - and gazetted in January 2022 - impose a duty on Class A and Class B banks (as defined) to make monthly reports to the FRA regarding threshold transfers in the month that equal or exceed US$ 100,000.

II. THE FINANCIAL REPORTING AUTHORITY

1. BACKGROUND

The FRA, known to counterparts worldwide by its Egmont handle "CAYFIN", is the financial intelligence unit of the Cayman Islands. As such it is the national agency responsible for receiving, requesting, analysing and disseminating financial information disclosures concerning proceeds of criminal conduct, in order to counter money laundering, terrorism, the financing of terrorism or suspicions of any of those crimes.

The FRA has evolved over the years. It began as the Financial Investigation Unit in the early 1980s, operating within police headquarters. In 2000 it underwent a name change to become the Financial Reporting Unit, with the head of the unit becoming a civilian post and the appointment of a legal advisor. Line management for operational work was undertaken by the office of the Attorney General. Throughout this period, the role of the unit was to receive, analyse and investigate SARs, in addition to gathering evidence to support prosecutions.

In 2004, the Cayman Islands moved toward an administrative-type unit. The Proceeds of Criminal Conduct (Amendment) Law 2003 (PCCL) created the Financial Reporting Authority, the name by which the unit is presently known. The law, which came into force on 12th January 2004, mandated that the FRA become a full-fledged civilian body, and that its function change from being an investigative to an analytical type FIU. Accordingly its mandate was restricted to the receipt and analysis of financial information, coupled with the ability to disseminate this intelligence to agencies where authorised to do so by the PCCL. Its existence and independence were further enshrined in the POCA, which repealed and replaced the PCCL and came into force on 30th September 2008. The investigative mandate is undertaken by domestic law enforcement agencies, including the Royal Cayman Islands Police Service ("RCIPS"), the Cayman Islands Customs and Border Control ("CBC") and the Anti-Corruption Commission ("ACC").

2. Role and Function

SARs

The FRA's main objective is to serve the Cayman Islands by participating in the international effort to deter and counter money laundering and the financing of terrorism.

As noted above, a primary role of the FRA is to receive, analyse, request and disseminate disclosures of financial information, concerning the proceeds of criminal conduct, suspected proceeds of criminal conduct, money laundering (ML), or suspected money laundering, all of which are derived from any criminal offence committed in these islands or overseas if the criminal act satisfies the dual criminality test set out in the POCA; or the financing of terrorism (FT) which can be legitimately obtained money or the proceeds of criminal conduct as defined in the POCA.

The FRA also serves as the contact point for international exchanges of financial intelligence within the provisions of the POCA.

Financial intelligence is the end product of analysing one or several related reports that the FRA is mandated to receive from financial services providers ('FSPs') and other reporting entities. Our ability to link seemingly unrelated transactions allows us to make unique intelligence contributions to the investigation of money laundering and terrorist financing activities.

A key priority for the FRA is to provide timely and high quality financial intelligence to local and overseas law enforcement agencies through their local FIU, in keeping with the statutory requirements of the POCA.

Targeted Financial Sanctions (TFS)

The Governor of the Cayman Islands is the competent authority for implementation of financial sanctions measures. Under the Overseas Orders in Council ("OOIC") the Governor's responsibilities and duties include, inter alia, the power to grant, vary and revoke licences (which permit the conduct of specified activities otherwise not permitted under the OOIC), the duty to publish certain lists; and power to delegate any of the Governor's functions. However, the FRA is officially responsible for helping to ensure the implementation of Targeted Financial Sanctions (TFS) with respect to terrorism, terrorism financing, proliferation, proliferation financing, and other restrictive measures related to Anti-Money laundering ("AML"), combatting the financing of terrorism ("CFT") and proliferation ("CFP") within the Cayman Islands; i.e. functions relating to counter-terrorism and proliferation finance, both of which are monitored by FATF/CFATF. The Governor has delegated the function of receiving CT and CP-related reports to the FRA. The Governor has also delegated specified functions and powers to the Director of the FRA ("the Director") with regard to the Russia Sanctions Regime.

The Sanctions Coordinator ("SC") plays a critical role in the implementation and enforcement of these targeted financial sanctions and other restrictive measures, and in developing and enhancing the jurisdiction's AML/CFT regime, while ensuring ongoing compliance with international standards and best practices.

During the Reporting Period the FRA published 102 Financial Sanctions Notices on its website, a decrease from 128 in 2023. The FRA subscribes to the Email Alert provided by the Office of Financial Sanctions Implementation ("OFSI") within UK HM Treasury, advising of any changes to United Nations, European Union and UK financial sanctions in effect. The FRA forwards these notices automatically to local law enforcement agencies and competent

authorities, converts it to a Cayman Notice and publishes the Cayman Financial Sanctions Notice on its website. The average turn-around time for converting these notices, distributing them via e-mail and posting them to the FRA's website is between 1-3 hours.

The FRA published for the first time in September 2024, Specified Ship Sanctions notices under the Russia Regime. During the Reporting Period the FRA published 7 Specified Ship Sanctions Notices (a total of 109 ships specified) on its website. A specified ship is prohibited from entering a port in the Cayman Islands, may be given a movement or a port entry direction, can be detained, and will be refused permission to register on the Cayman Islands Shipping Registry or may have its existing registration terminated. The FRA subscribes to the Email Alert provided by the Foreign, Commonwealth & Development Office ("FCDO"), advising of shipping sanctions. The FRA forwards these notices automatically to subscribers, local law enforcement agencies and competent authorities generally within 1-2 hours of receipt of these notices.

Russia Sanctions

The FRA continued to see a number of sanctions being imposed by the United Kingdom (and other countries) in 2024 in response to the Russian invasion of Ukraine on 24 February 2022, in terms of size, scale and complexity. As a result, it was another challenging year for sanctions implementation due to continued demands on the FRA.

OFSI published an unprecedented number of new designations under the Russia sanctions regime, with over 1,600 new listings since the invasion of Ukraine. The FRA published all of these without delay, and sent emails to over 1,200 subscribers, detailing the changes to the Consolidated List. In addition, the nature and volume of the FRA's engagement with industry stakeholders, other competent authorities, external UK Partners (primarily the Foreign, Commonwealth & Development Office, OFSI, Department for Transport), increased to meet the new challenges posed by the Russia Sanctions regime. The Sanctions Coordinator participated in / presented at four (4) domestic outreach sessions.

As part of their reporting obligations, relevant firms have an obligation to report information concerning funds or economic resources belonging to, owned, held or controlled by a designated person in a Compliance Reporting Form (CRF). This report must be made as soon as practicable to the FRA, which has been delegated by the Governor as the appropriate recipient of these reports.

During 2024, a total of 122 Compliance Reporting Forms (CRFs) and 5 Reports by Designated Persons were received by the FRA related to the Russia Sanctions regime. As of 31 December 2024, a total of approximately USD$ 8.89 billion, EUR€230 million, CHF4 million and GBP234,000 held by or on behalf of persons designated under the Russia Sanctions regime was reported as

being frozen.

The FRA continues to process licence applications and respond to queries received under the Russia Sanction regime. During the year ending December 2024, 13 (compared to 13 in 2023) formal applications have been received.

The Cayman Islands has adopted a robust and comprehensive response to the imposition of the new Russia sanctions measures. Of note, in March 2022 a joint Task Force on Russia, comprising representatives from eleven Ministries/Offices/ Portfolios/Agencies, was formed to coordinate, identify, and implement policy amendments to implement the Russia Sanctions regime. The Director is the Chair of the Task Force and the Sanctions Coordinator is a member. The primary purpose of the Task Force is to provide centralised discussions and decisions around policy and communications arising from the ongoing sanctions. The Task Force continued to meet regularly during 2024.

The following General Licences, which allow multiple parties to undertake specified activities without applicants needing to submit a specific licence request to the FRA, were issued or amended by the Governor with the consent of the UK Secretary of State in 2024.

1. Originally issued on October 4 2022 and amended on April 5 2023, October 6 2023 and on October 16 2024: General Licence GL/2022/0001 allows a Relevant Investment Fund or Fund Manager to redeem, withdraw or otherwise deal with an Investment Interest and make payments for basic needs, routine holding and maintenance and legal fees from frozen accounts. This is due to expire on October 16 2025.

2. General licence GL/2023/0002 originally issued on April 14 2023 replaced on November 15 2023 with GL/2023/0003, on May 24 2024 with GL/2024/001 and on December 19 with GL/2024/0002: General License GL/2024/0002 permits an Attorney or Law Firm, subject to certain conditions, who has provided legal advice to a person designated under the Russia or Belarus regime to received payment from that designated person. This is due to expire on April 28 2025.

These General Licences were posted along with the publication notice on the FRA's website and disseminated to subscribers.

3. Organisational Structure and Management

The FRA is a part of the Cayman Islands Government's Portfolio of Legal Affairs. The head of this portfolio is the Hon. Attorney General, with operation line management to the Solicitor General. In addition, the FRA reports to the AMLSG, a body created by the same statute as the FRA. The AMLSG is chaired by the Hon. Attorney General and the

membership comprises the Chief Officer in the Ministry responsible for Financial Services or the Chief Officer's designate (Deputy Chairman), the Commissioner of Police, the Director of CBC (formerly the Collector of Customs), the Managing Director of CIMA, the Solicitor General, the Director of Public Prosecutions, the Chief Officer or Director, as the case may be, of the department in Government charged with responsibility for monitoring compliance with anti-money laundering and counter terrorism measures for Designated Non-Financial Businesses and Professions ("DNFBPs") and the Chairman of the ACC (added in 2019). The Director is invited to attend meetings, as is the Head of the Anti-Money Laundering Unit, who also serves as secretary.

The AMLSG has responsibility for oversight of the anti-money laundering policy of the Government and determines the general administration of the business of the FRA. It also reviews the annual reports submitted by the Director, promotes effective collaboration between regulators and law enforcement agencies and monitors the FRA's interaction and cooperation with overseas FIUs.

The FRA believes that a healthy and well managed organisation sustains performance. In particular, it maintains strong focus on the effective management of human, financial and technical resources.

At 31 December 2024, the FRA had fifteen (15) staff members: a Director, Legal Advisor, Sanctions Coordinator, Senior Accountant, three Senior Financial Analysts, 7 Financial Analysts and an Administrative Manager, all having suitable qualifications and experience necessary to perform their work.

It is expected that all staff abide by the highest standards of integrity and professionalism. In particular, the FRA places great emphasis on the high level of confidentiality demanded by its role, as well as by the financial industry with whom it interacts. Staff must have the appropriate skills to carry out their duties, and therefore the FRA provides specialised training suited to individual responsibilities, in addition to continuing education to ensure that staff remain up-to-date with industry and regulatory developments crucial to the effective functioning of the FRA.

During the Reporting Period, staff attended / completed numerous training events:

1. ACAMS Anti-Financial Crime/CFT Symposium – Grand Cayman 2024 (3 staff attended)
2. The UNODC - FIU Operational and strategic analysis and risk scoring (1 staff attended)
3. Overseas Territories Countering the Financing of Terrorism Forums (1 staff attended)
4. UK Home Office - Open Source Intelligence Course (1 staff attended)
5. Online training provided by the Egmont Group / Egmont Centre for FIU Excellence and Leadership (ECOFEL) and other training providers on a variety of topics, including:

a. Cooperation and Information Sharing between Financial Intelligence Units, Law Enforcement Authorities and Prosecutors
b. Introduction to Virtual Assets / Virtual Asset Analysis
c. Financial Flows of Online Child Sexual Exploitation
d. FIU / LEA Cooperation
e. Countering Terrorist Financing
f. Introduction to Wildlife Crime
g. FATF Introductory Curriculum
h. FATF Beneficial Ownership Course

During the Reporting Period, the FRA made a number of presentations at outreach events covering one or more of the following topics: (i) functions of the FRA; (ii) SAR statistics; (iii) SAR reporting obligations; and (iv) obligations regarding targeted financial sanctions related to terrorist financing and proliferation financing. Details of those presentations are as follows:

- Two (2) presentations at international and domestic industry association events, or other international events.
- Two (2) 1-on-1 meetings with Money Laundering Reporting Officers (MLROs).
- One (1) meeting with MLROs to demonstrate AMLive Reporting Portal functionalities.

4. Protecting Confidentiality of Information

The POCA provides the framework for the protection of information obtained by the FRA. Furthermore a layered approach to security has been adopted for the FRA's office and systems. Protecting financial information received from reporting entities is a critical function of the FRA. Computer security measures include advanced firewalls to prevent unauthorised access to our database. In addition staff are aware of their responsibilities to protect information, and severe penalties exist, under the POCA, for the unauthorised disclosure of information in our possession and control.

The FRA constantly reviews its security procedures to ensure that those procedures remain current in its continued effort to maintain confidentiality.

5. Relationships

Working with Financial Service Providers and Other Reporting Entities

The FRA recognises that the quality of the financial intelligence it produces is shaped directly by the quality of reports it receives from financial service providers and other reporting entities. If reporting entities are to produce insightful and relevant reports of superior quality, it is of utmost importance that they understand and are able to comply with the requirements of the POCA to which they are subject.

Recognising the vital importance of working with financial service providers and other reporting entities to raise awareness and

understanding of their legal obligations under the POCA, the FRA meets with MLROs to share matters of mutual interest.

The Egmont Group

The Egmont Group (EG) of FIUs is an international, officially recognised body through the adoption of the Egmont Charter in the May 2007 Plenary held in Bermuda and the establishment of its permanent Secretariat in Toronto, Canada. Its membership currently comprises 177 countries; of note two Caribbean OFIUs became members during 2024 – Guyana and Suriname. It sets standards for membership as well as expanding and systematising international cooperation in the reciprocal exchange of financial information within its membership.

The Cayman Islands' commitment to abide by the EG Group Principles for Information Exchange preceded its admission to full Egmont membership in 2000. The FRA continues to actively participate in the Egmont Working Groups, Plenaries and the Heads of FIU meetings.

Since being appointed as a Regional Representative for the Americas Region of the EG in July 2023, the Director has been a member of the Egmont Committee (EC) and has played an even more active role in the work of the EG. During the Reporting period the Director: (1) Served as a judge for the Best Egmont Case Award (BECA), which involved reviewing and scoring numerous cases submitted by several OFIUs that are Egmont members; FIU Peru won the 2024 BECA; (2) Served as a member of an Advisory Panel responsible for interviewing candidates for the Egmont Group Chair and Vice Chair positions and preparing a recommendation to be considered during the Heads of FIU meeting at the June 2024 Egmont Plenary. The Director presented the Advisory Panel's report to the Heads of FIU at their meeting; and (3) Served on a working group responsible for developing the thematic discussions for the June 2024 Egmont Plenary. The Director also served as moderator for the first panel that covered developing the future workforce of a FIU.

A FRA staff member continued to serve as a Regional Support Officer for the Americas Region in relation to the Egmont Secure Web (ESW). This role involved serving as first level support on troubleshooting any IT issues encountered. In addition, the staff member provided assistance to a number of Caribbean OFIUs in completing and submitting their Egmont Biennial Census 2024.

The Director and a member of staff attended the EG Working and Regional Group meetings in St Julian, Malta from 28th January to 2nd February 2024. The meetings were attended by 423 delegates representing Egmont members and 17 observers and international partners who gathered through 16 different meetings to enhance EG member capabilities, improve information sharing among them, and work toward accomplishing the EG's development mission, cooperation, and sharing of expertise.

The Director attended an EC intersessional meeting in Canberra, Australia on 17th and 18th April 2024. The EC is a vital consultation and coordination mechanism for the EG's Heads of FIU, Working and Regional Groups. The EC supports the EG's diverse initiatives, ranging from internal coordination and administration to representation in the global AML/CFT fora. EC members convened to discuss key strategic issues arising from decisions made at the 2024 Working and Regional Group Meetings in Malta and in preparation for the 30th Plenary in Paris.

The Director also attended the 30th annual EG Plenary meetings from 2nd to 7th June 2024, in Paris, France. The Plenary was attended by 400 delegates and 11 observer organisations. The 30th Plenary's Thematic Discussion "Next Generation FIU" examined the adaptations required by FIUs in the coming decade, echoing efforts worldwide to adapt to future challenges, whilst fully embracing digital and environmental transitions. Among the topics explored were: developing the future workforce; how the future FIU uses technology; and the role of FIUs in addressing emerging crime types.

Memoranda of Understanding (MOUs)

The FRA can exchange information with other financial intelligence units around the world with regards to information in support of the investigation or prosecution of money laundering and/or terrorist financing. However some FIUs are required by their domestic legislation to enter into arrangements with other countries to accommodate such exchanges. In this context the FRA is empowered by the POCA to enter into bilateral agreements with its counterpart giving effect to the global sharing of information.

During the Reporting Period the FRA signed three (3) MOUs with the following OFIUs: (1) The Anti-Money Laundering Division (AMLD) of Taiwan (the Republic of China (ROC); (2) The Financial Intelligence Unit of the Commonwealth of The Bahamas; and (3) The Financial Intelligence Unit of the Co-operative Republic of Guyana. The FRA also amended its existing MOU with FIU Guatemala. The FRA is currently in discussions with a number of OFIUS to sign an MOU. The FRA has signed and exchanged MOUs with the following 24 FIUs as of 31 December 2024: Australia, Bahamas, Canada, Chile, Guatemala, Guernsey, Guyana, Honduras, Indonesia, Israel, Jamaica, Japan, Mauritius, Nigeria, Panama, Poland, Republic of Korea (South Korea), the Russian Federation, Saint Vincent and the Grenadines, South Africa, Taiwan (ROC), Thailand, the United States and the Vatican City State.

The Caribbean Financial Action Task Force

The CFATF is an organisation of states of the Caribbean basin that have agreed to implement common countermeasures to address the problem of money laundering. It was established as the result of meetings convened in Aruba in May 1990, and Jamaica in November 1992. CFATF currently has 24 member countries.

The main objective of the CFATF is to achieve implementation of, and compliance with, recommendations to prevent and combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

The Mutual Evaluation Programme (MEP) is a crucial aspect of the work of the CFATF, as it helps the CFATF Secretariat ensure that each member state fulfils the obligations of membership. Through this monitoring mechanism the wider membership is kept informed of what is happening in each member country that has signed the MOU. For the individual member, the MEP represents an opportunity for an expert objective assessment of the measures in place for fighting money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

The 58th CFATF Plenary and Working Group Meetings were held in Port-of-Spain, Trinidad and Tobago from 2nd to 7th June 2024. Two (2) staff attended various working group meetings, including the HoFIUs meeting, which is the focus for the FRA, as well as the Plenary sessions. The Mutual Evaluation Report for Anguilla and Guyana were adopted at the 58th Plenary.

The 59th CFATF Plenary and Working Group Meetings were held in Hanover, Jamaica from 1st to 6th December 2024. Three (3) staff attended various working group meetings, including the HoFIUs meeting, which is the focus for the FRA, as well as the Plenary sessions. The Mutual Evaluation Reports for Belize and Montserrat were adopted at the 59th Plenary. The United States of America became a member of the CFATF on Wednesday 4th December 2024 increasing the CFATF's membership to twenty (25) members.

Staff of the FRA contribute significantly to the work of the CFATF Heads of FIUs Forum and the CFATF Risk, Trends & Methods Group meeting.

The FATF Recommendations and Methodology

Following the conclusion of the third round of mutual evaluations of its members, the FATF reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (which includes the CFATF) and the observer organisations.

The FATF revised its Methodology in 2013, setting out the basis for undertaking assessments of technical compliance with the Recommendations. For its 4th round of mutual evaluations, the FATF has adopted complementary approaches for assessing technical compliance with the Recommendations, and for assessing whether and how the AML/CFT system is effective. The Methodology comprised two components:

a) The technical compliance assessment addresses the specific requirements of the Recommendations, principally as they relate to the relevant legal and

institutional framework of the country, and the powers and procedures of the competent authorities.

b) The effectiveness assessment seeks to evaluate the adequacy of the implementation of the Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional framework is producing the expected results.

The FATF Recommendations and Methodology continue to evolve. A draft 5th Round Methodology was adopted in February 2022 and revised in October 2023, July 2024 (for information purposes), and August 2024 for jurisdictions to learn about the expected changes in the FATF's next round of MEs[1]. The revised Methodology focuses on effectiveness. The CFATF's 5th Round Procedures[2] were updated in August 2024.

[1] https://www.fatf-gafi.org/en/publications/Mutualevaluations/5th-Round-Methodology.html

[2] https://www.cfatf-gafic.org/documents/cfatf-resources/24076-procedures-for-the-fifth-round-of-cfatf-aml-cft-cpf-mutual-evaluation-and-follow-up-pdf?format=html

III. PERFORMANCE REPORTING

1. Receiving Information - Suspicious Activity Reports (SARs)

The FRA receives information from reporting entities relating to suspected money laundering, proceeds of criminal conduct, terrorism and the financing of terrorism through SARs. It also receives requests for information from local law enforcement agencies, local supervisory agencies, such as CIMA, and overseas FIUs. SARs and requests for information are collectively referred to as cases in this report.

Upon receipt, each case is examined to ensure that the report contains all the required data. The case is then assigned a reference number and data from the case is entered into the FRA's SAR database.

During the Reporting Period, the FRA received 1,194 SARs from 291 different reporting entities, down from the 1,290 SARs from 292 different reporting entities in 2023. This number excludes the 48 overseas FIUs that requested information from the FRA, or voluntarily disclosed information to the FRA. SARs received from the 291 reporting entities are classified in the succeeding table according to the licence / registration that they hold with CIMA, if they are a regulated / registered entity. Reporting entities that are not regulated are classified according to the type of service that they provide. Regulated / registered entities are shown as part of the following sectors regulated by CIMA: banking, fiduciary services, insurance services, investment funds and fund administrators, money transmitters and securities investment businesses.

Designated Non-Financial Businesses and Professions (DNFBPs) consist of law practitioners, accounting professionals, real estate brokers, and dealers of high value items.

The number of cases filed under each of those sectors and the DNFBPs are as follows:

Sector	No of Cases
Virtual Asset Service Provider	374
Banking	282
Investment funds and fund Administrators	184
Fiduciary services	125
Money transmitters	31
Securities investment businesses	29
Insurance services	20
DNFBPs	90
LEAs & Competent Authority	29
Others	30
Requests for Information – Domestic	57
Disclosures & Requests for Information – Overseas	144
Total No of Cases	1,395

During the Reporting Period anyone who filed a SAR has a defence against any potential related money laundering or terrorist financing offences; however, this does not apply to the person who committed or was a party to the act that gives rise to the offence. SARs filed under the POCA do not breach the Confidential Information Disclosure Act, 2016, nor do they give rise to any civil liability.

As mentioned in Part 1 (Legal Framework), a 2023 amendment due to take effect on 2nd January 2025 removes that automatic

defence and SAR filers will need to seek the consent of the FRA to continue with the prohibited action at the same time as submitting the SAR. The rule remains that consent cannot be sought, if the person making the report is also the subject of the report.

Chart 3.1 on the succeeding page shows the total number of reports by financial year since 2018. The FRA received 1,395 new cases during the Reporting Period. Since fiscal year 2013/2014, the FRA has used its existing risk ranking for cases to determine which cases are to be expedited while the rest are dealt with in accordance with existing timetables. The existing risk ranking for cases allows the FRA to efficiently focus its resources.

The average number of cases received per month in 2024 was 116, compared to 125 in 2023.

A total of 2,476 subjects were identified in cases (see Chart 3.3 on page 22), comprising 1,746 natural persons and 730 legal entities. 92 natural persons and 40 legal entities were the subject of multiple SARs.

In some cases, particularly where the service provider has limited information about a counterpart to the transaction, the nationality or domicile of the subject is not known. This is also the situation in those cases relating to declined business and scams. There are also instances when a requesting overseas FIU does not have complete details regarding the nationality of all the subjects of their request.

During the year, the number of subjects with unknown nationality or country of incorporation was 397, comprising 277 natural persons (including 35 anonymous subjects) and 120 legal entities.

The number of subjects whose nationality or country of incorporation is not identified declined from 397 to 272 when subjects of request for information from domestic law enforcement agencies, competent authorities and overseas FIUs are excluded. Banks also contributed subjects whose nationality or country of incorporation is not identified, totalling 140.

Charts 3.1 and 3.2 on the next page do not include SARs received during the Reporting Period that were updates to a previously submitted report that is pending. As a consequence, the subjects of those updates are not included in the number of natural persons and legal entities identified as subjects of SARs in Chart 3.3 on page 22.

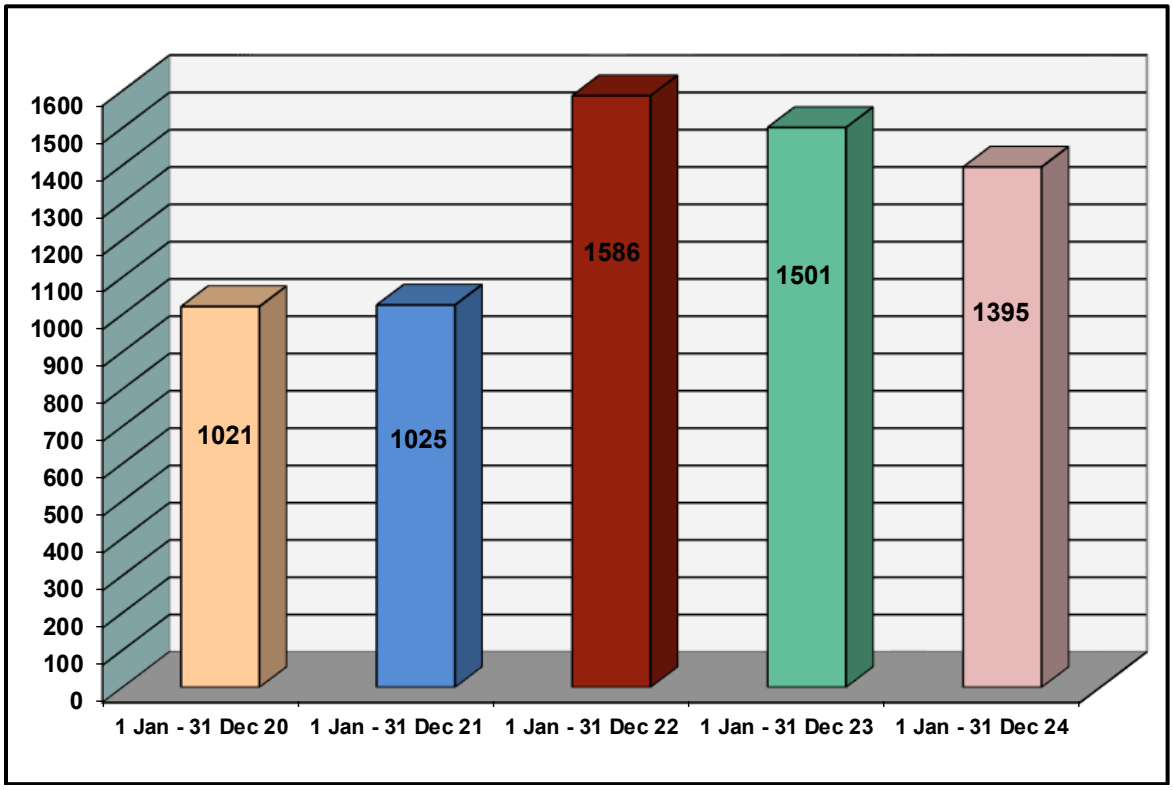


Chart 3.1: Total cases by financial year / Reporting Period

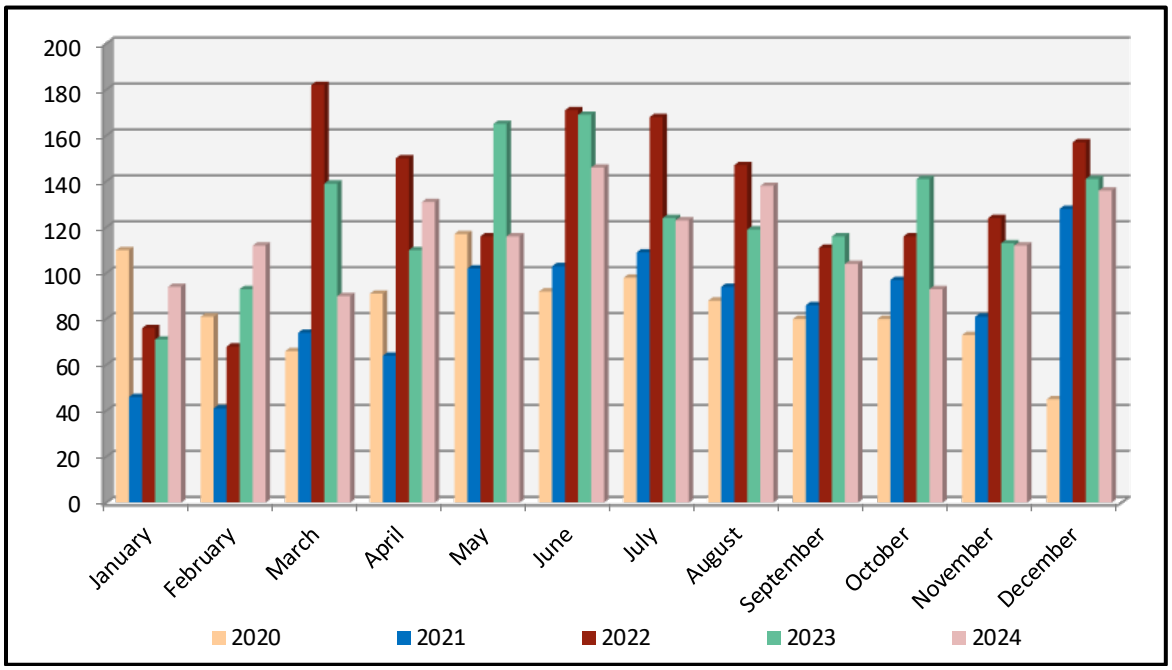


Chart 3.2: Comparison of monthly cases received

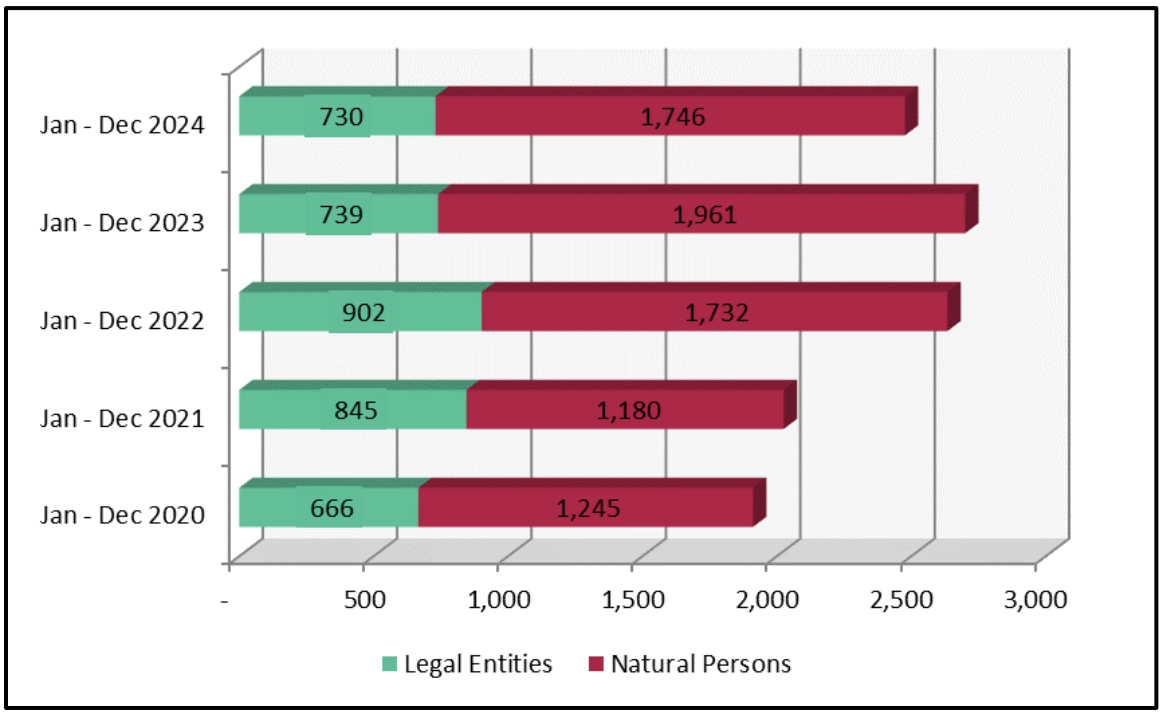


Chart 3.3: Number of subjects by financial year / Reporting Period

Countries of Subjects Reported

The international scope of the Cayman Islands' financial services industry is reflected in the wide range of subjects' countries reported in cases. The "Countries of Subjects" chart on the succeeding page lists 128 different countries for the subjects of the cases. In light of the international character of the subjects reported, our membership of the Egmont Group has proven to be a valuable resource for information exchange and requests, and has enhanced the analysis of information reported in the development of intelligence.

The greatest number of subjects was classed as Caymanian, totalling 374; 79 were Caymanian nationals (natural persons) and 295 were legal entities established in the Cayman Islands. The United States was second largest with 107 natural persons and 51 legal entities. Romania was third with 114 natural persons. The United Kingdom was the fourth largest with 96 natural persons and 17 legal entities followed by: Spain with 86 natural persons; Jamaica with 71 natural persons; Italy comprising 62 natural persons and 4 legal entities; Canada with 56 natural persons and 3 legal entities; Russia with 50 natural persons; Kazakhstan with 44 natural persons and 3 legal entities and the People's Republic of China with 46 natural persons and 1 legal entity. Together these 11 countries account for 1,185 subjects, which represents 48% of the total.

The category "Others" in Chart 3.4 comprises the following countries with 6 or fewer subjects: Afghanistan, Andorra, Antigua and Barbuda, Armenia, Austria, Azerbaijan, Bahrain, Bangladesh, Barbados, Belarus, Belize, Bermuda, Cambodia, Chile, Colombia, Congo (Republic of the), Costa Rica, Croatia, Cuba, Curacao, Czech Republic, Denmark, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Estonia, Georgia, Ghana,

Greece, Guatemala, Guernsey, Guyana, Haiti, Honduras, Hungary, Iceland, Indonesia, Iraq, Isle of Man, Japan, Jersey, Jordan, Kenya, Kuwait, Kyrgyzstan, Libya, Liechtenstein, Lithuania, Luxembourg, Mali, Marshall Islands, Mauritius, Montenegro, Morocco, Mozambique, Nepal, Nicaragua, Nigeria, Norway, Oman, Pakistan, Palestine, Paraguay, Peru, Portugal, Saint Kitts and Nevis, Saint Vincent and the Grenadines. Saudi Arabia, Seychelles, Slovakia, Slovenia, South Africa, South Korea, Sri Lanka, Thailand, Trinidad and Tobago, Turkey, Uruguay, Uzbekistan, Vanuatu, and Vietnam.

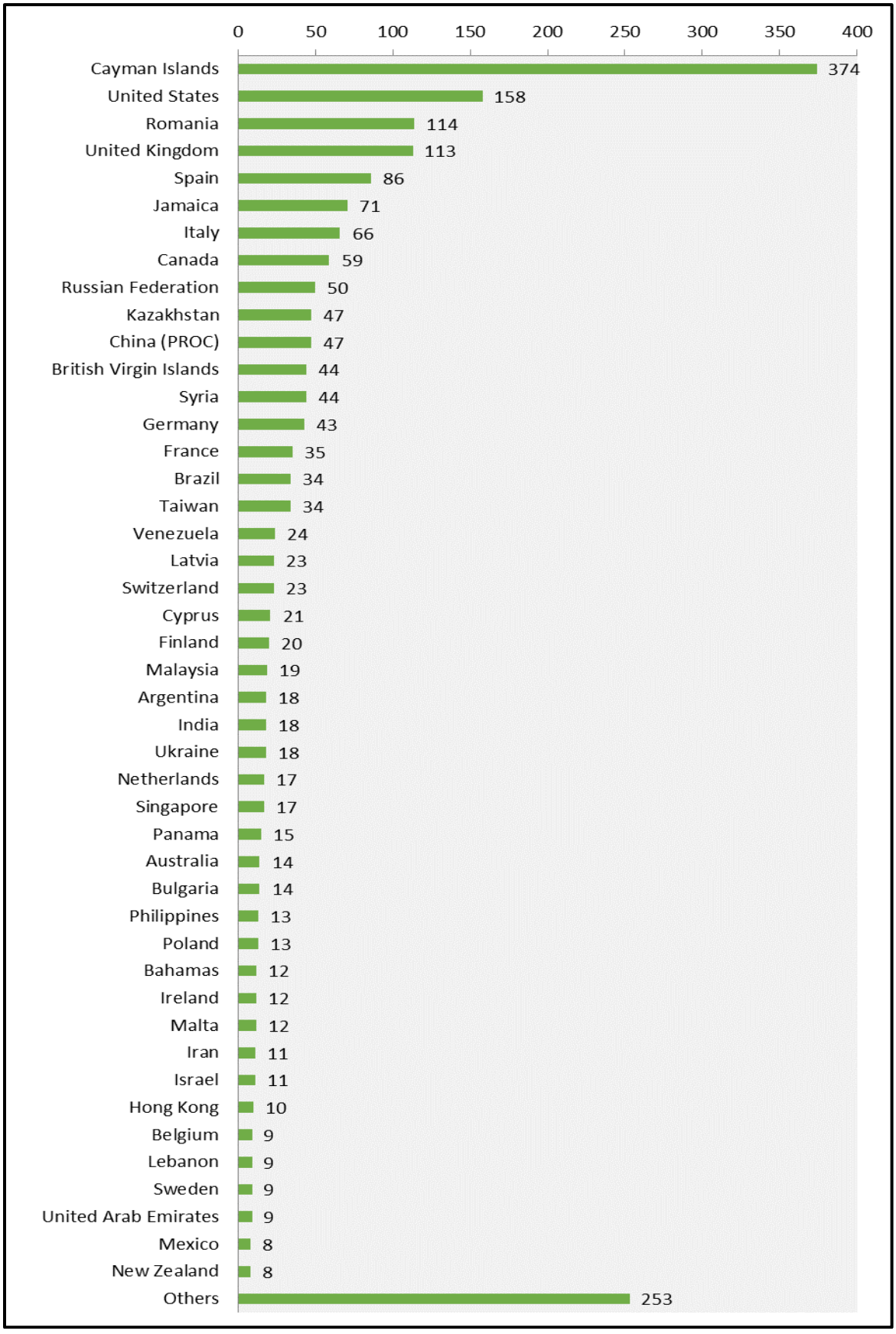


Chart 3.4: Countries of subjects in SARs reported in the Reporting Period

Sources of Cases

Chart 3.5 shows a detailed breakdown of the sources of cases. CIMA regulated financial service providers submitted a substantial portion of the cases that the FRA received. The ten largest contributors were:

- Virtual Asset Service Provider – 374
- Banks – 282
- Overseas Financial Intelligence Units – 144
- Investment Funds – 120
- Company Managers / Corporate Service Providers – 75
- Mutual Fund Administrators - 64
- Lawyers – 55
- Trust Companies – 50
- Money Transmitters – 31
- Securities Licensees – 29

Virtual Asset Service Providers ("VASPs") were the largest source of SARs, with 374 cases filed by ten (10) VASPs. In 2023, six (6) VASPs filed 282 cases.

Banks continue to be a major source of SARs, with 282 cases filed by 19 banks or banking type entities, comprising: 222 cases filed by 5 Class A banks and 60 cases filed by 14 Class B banks. This compares to 392 cases filed by 24 banks or banking type entities during 2023, comprising: 333 cases filed by 8 Class A banks; 52 cases filed by 15 Class B banks; and 7 cases filed by a Credit Union. MSBs filed 31 cases in 2024 which is the same as 31 cases filed in 2023.

Except for VASPs, almost all other sectors registered a decline in SARs filed. Most notable among those is a 28% decline in SARs from banks. Of note, a decline was noted in number of SARs about online schemes that target debit and credit cards.

Investment Funds, comprising Mutual Funds and Private Funds, filed 120 cases, 10 fewer than the 130 cases received in 2023.

Company Managers / Corporate Service Providers and Trust Companies filed 125 SARs during the Reporting Period, compared to 141 in 2023.

Mutual Fund Administrators filed 64 cases during the Reporting Period, compared to 76 in 2023.

Securities Licensees filed 29 SARs during the Reporting Period, compared to 56 in 2023.

Insurance Businesses filed 20 SARs during the Reporting Period, compared to the 40 in 2023

The largest number of SARs received from DNFBPs came from lawyers (55). Other DNFBPs filing SARs included: accounting professionals, real estate brokers, second-hand dealers and dealers of high value goods.

Receipt of Threshold Reports from Money Service Businesses and Banks

For the 12-month period ended 31 December 2024, the combined value of bank threshold transfers was approximately US$915.6 billion for outgoing transfers (97,566 transactions) and US$521.5 billion for incoming transfers (44,556 transactions). For the 12-month period ended 31 December 2023, the combined value of bank threshold transfers

was approximately US$767 billion for outgoing transfers (97,053 transactions) and US$329 billion for incoming transfers (13,463 transactions).

The combined value of MSB threshold transactions for the Reporting Period was approximately US$24.9 million for outgoing remittances (20,237 transactions) and US$612.8 thousand for incoming remittances (260 transactions). The combined value of MSB threshold transactions for 2023 was approximately US$25.7 million for outgoing remittances (21,974 transactions) and US$674.9 thousand for incoming remittances (350 transactions).

These additional data are assessed when analysing cases, and has helped amplify the analysis for a handful of cases. The information received from threshold reporting be also be used in future strategic analysis projects where relevant.

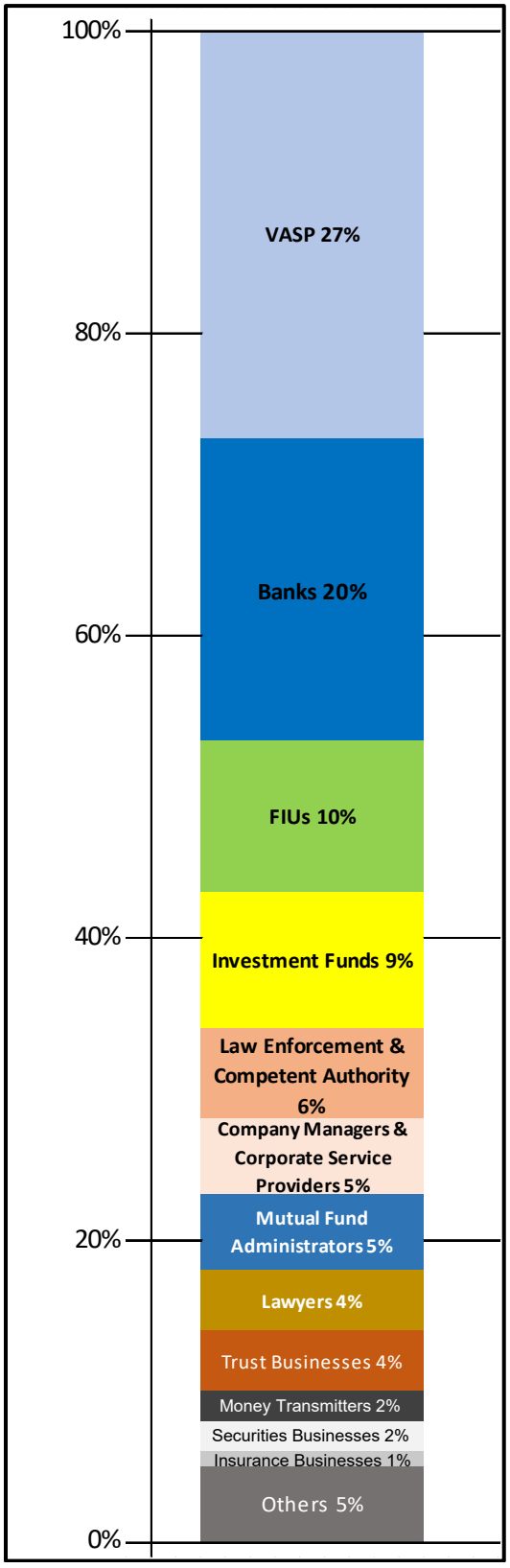


Chart 3.5: Sources of Cases

2. Analysing Information

The FRA conducts in-depth research and analysis by matching data in the SAR to existing records and intelligence information in the SAR database, as well as to information contained in other external databases. An important element of the FRA's analysis is the ability, provided for by the POCA, to request information from any person, in order to clarify or amplify information disclosed in a report, or information from any person, in order to clarify or amplify information disclosed in a report, or at the request of an overseas FIU. Failure to provide this information within 72 hours is an offence under the POCA. A second important element is the FRA's ability to request and exchange information with Egmont Group members.

Consistent with the provisions of the POCA, the FRA made 183 requests locally to clarify or amplify information received in 139 cases; 94 of these requests were to the SAR filer with the other 89 going to third parties. The majority of the information requested consisted of: financial information, such as account statements and details of specific transactions; beneficial ownership (including registers); and constitutional documents.

Forty-six (46) requests for information were made to thirty-one (31) overseas FIUs in connection with twenty-nine (29) unique cases. Forty-two (42) of those requests were to Egmont member FIUs via the Egmont Secure Web. Twenty-eight (28) of those requests were made on behalf of local law enforcement agencies. These requests greatly assisted the FRA in determining whether to make disclosures to local law enforcement, as well as to overseas FIUs, or to assist local law enforcement with their investigations. Chart 3.6 shows the number of requests made locally and overseas by financial year since 2020.

Upon completion of the analysis, an assessment is made to determine if the analysis substantiates the suspicion of money laundering, financing of terrorism or criminal conduct. If, in the opinion of the Director, this statutory threshold is reached, the FRA discloses the information to the appropriate local law enforcement agency, supervisor or overseas FIU.

Additionally, the provisions of section 4(2)(ca) of the POCA allow the FRA, in its discretion or upon request, to disclose information and the results of its analysis to local law enforcement, CIMA and any public body to whom the Cabinet has assigned the responsibility of monitoring AML, in cases where the threshold of suspicion of criminal conduct has not been met.

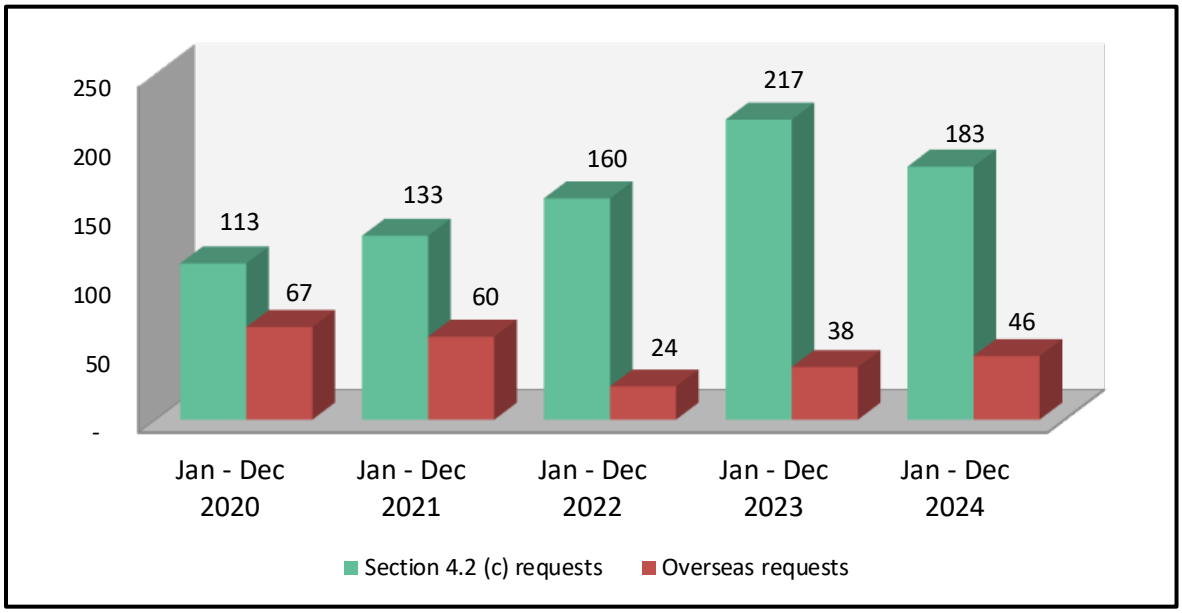


Chart 3.6: Number of requests made locally and overseas

SARs Trend Analysis

Table 3.7 below provides a detailed breakdown of the reasons for suspicion.

Reasons	%
Suspicious Activity	76%
Fraud	55%
Money Laundering	17%
Sanctions	8%
Corruption	7%
Declined Business	5%
Tax Evasion	5%
Theft	4%
Politically Exposed Persons	3%
Drug Trafficking	3%
Regulatory Matters	2%
Terrorism/Terrorist Financing	2%
Unlicensed Regulated Activity	1%
Others	10%

Table 3.7: Reasons for suspicion

Since 2021 multiple reasons for suspicion for each case have been tracked. For the 1,395 cases received, 2,750 reasons for suspicion were recorded

Suspicious Financial Activity

A large number of cases filed with the FRA are due to 'suspicious activity', wherein the reporting entity is noticing more than one unusual activity but could not arrive at a specific suspicion of an offence. The FRA recognises that this is a perfectly valid reason to submit a SAR.

In an effort to provide a more detailed breakdown of what types of activities were deemed suspicious by SAR filers, we have grouped the cases by the most recognisable of the activities as follows:

a) **558 cases that involve unusual conditions or circumstances**: Unusual conditions or circumstances include: VASPs identifying that a digital wallet or virtual assets had an exposure to Darknet entities; an approach made by local or foreign authorities for information about a customer or an account; unusual

inquiries or requests by account holders; and reports about funds being withdrawn from insurance policies within a relatively short period of time of the policy being issued.

b) **173 cases regarding inadequate and / or inconsistent information:** Cases with inadequate and / or inconsistent information provided are those where the reporting entities have received inadequate information or deemed responses to their continuing due diligence inquiries as being evasive, incomplete or inconsistent.

c) **151 cases about activities that appear to lack economic purpose**: Cases about activities that appear to lack economic purpose include reports from VASPs about customer transactions that appear to pass through digital wallets (top-up, conversion followed by withdrawal); reports from banks about customer transactions that appear to pass though accounts (deposit followed by withdrawal shortly thereafter).

d) **112 cases about transactions inconsistent with client profile:** Cases about transactions that are inconsistent with the established client profile include reports where the FSP identified that its client's recent transactions do not match the profile initially provided when the account was established and the client's explanation for the transactions appears to raise further questions.

e) **34 cases of transactions that appear to be structured to avoid reporting thresholds**: These include reports from: banks and MSBs where there appear to be attempts to break transactions into smaller amounts to avoid reporting thresholds.

f) **30 cases regarding high volume transactions:** Reports about high number of transactions occurring, including those involving cash, consist of reports about subjects making multiple transactions (i.e., deposits, withdrawals or remittances); as well as transactions in virtual assets/digital wallets that have a noticeably high volume compared with similar accounts. Most of the time these would also involve suspicions about the sources of funds being deposited.

Fraud

In the 2021 National Risk Assessment ('NRA') conducted by the jurisdiction, fraud featured prominently. With regard to foreign-generated proceeds of crime, fraud received a "High" threat rating and was identified as the number one threat for the risk of money laundering. With regard to domestically generated proceeds of crime, fraud and theft were combined and received a "Medium-Low" threat rating and was ranked number 3 for the risk of money laundering. Fraud was the second most common reason for filing SARs during the Reporting Period and has

consistently featured in the top reasons for filing a SAR for several years.

As stated previously, the FRA now records multiple reasons for suspicion for each case, including different types of fraud. During 2024 773 total reasons for suspicions associated with fraud were recorded for 477 cases. The following is a high level overview of the types of frauds reported.

False Documents or Representations

A high number of cases were filed by a cross-section of FSPs where there is suspicion that the customer / client is providing a false document or misleading representation, usually when conducting due diligence at client take on or while conducting retrospective due diligence. A large portion of those cases involve suspicions about the validity of identification provided at client take on which led to those prospective clients being declined.

There were a handful of cases were perpetrators attempted to use fake cheques purported to be issued by a foreign institution either to make a deposit for a rental property or place funds in escrow. None of these transactions was successful.

Misappropriation and Ponzi/Pyramid Schemes

Many of these cases were as a result of adverse media regarding foreign persons being indicted or under investigation for misappropriation of monies. The cases typically involved misappropriation from investment vehicles they manage or their employer, and them having a nexus to Cayman funds. In most of these cases suspicions are that the money invested by the foreign persons in a Cayman fund could be the proceeds of the misappropriation.

The same was true for Ponzi/Pyramid schemes. In one case the investment manager for a Cayman fund initiated legal claims after discovering that monies it invested were not used for its intended purposes and instead used to pay off earlier investors or diverted to other companies.

Investment/Securities Fraud

Investment/Securities Fraud, including insider trading, stock manipulation and other securities violations, are regularly identified as reasons for suspicion. Most of the cases received during the Reporting Period raised suspicions that assets owned by an individual or entity that has been the subject of adverse reports might be the proceeds of an illegal scheme and that the reporting entity could not confirm or eliminate such possibility. A handful of cases identified a Cayman entity being named as a relief defendant or being associated with a defendant in foreign proceedings

Cyber-Enabled Fraud

In 2023 a joint FATF, Egmont Group and INTERPOL report began referring to many variations of fraud that is enabled through or conducted in the cyber environment as Cyber-Enabled Fraud (CEF). CEF usually involves transnational criminality such as transnational actors and funds flows and involves deceptive social engineering

techniques (i.e., manipulating victims to obtain access to confidential or personal information). Domestically the FRA continues to see significant cases regarding CEF as follows:

• Business Email Compromise (BEC) fraud. This scheme involves targeted persons receiving email instructions that purport to be from their clients or suppliers asking them to transfer funds to new payments accounts. Based on SARs received in 2024, US$2.3 million was lost to these schemes and the attempted misappropriation of a further US$33,000 was prevented by mitigating procedures. In 2023, US$3.3 million was lost to these schemes and the attempted misappropriation of a further US$2.8 million was prevented by mitigating procedures.

• Phishing fraud. Targeted persons are deceived into revealing sensitive information such as personal data, banking details or account login credentials either via emails, SMS or cloned websites. The criminal will then use the information to drain the victim's money from their payment accounts, open new payment accounts or make fraudulent transactions. The most common attempts we have noted are communications purporting to come from local banks.

In 2024 the FRA published an alert about a fake bank website that purported to be regulated by the FRA. The FRA suspects that this was used to mislead and entice people into transferring money or disclosing personal information. This scam is a form of "phishing." Fake bank websites sometimes use the name or logo of Government entities to instil a false sense of security. Details of that alert can be found here: https://fra.gov.ky/fraudulent-representation-of-regulation/

• Social media and telecommunication impersonation fraud: This includes scenarios where targeted persons are contacted via mobile or social media applications by criminals pretending to be government officials, relatives or friends, and prey on the victim's emotions to induce payment or hand over control of payments accounts or to carry out financial activities such as a loan application or an account opening to receive criminal proceeds.

During 2024, the FRA noted an increase in phone scams targeting older adults, where scammers instruct victims to make international wire transfers in order to aid in apprehending the culprits. This appeared to be a variation of the Tech Support scam but instead of claiming to be IT support the scammers are claiming to be from the security team of a bank or credit card provider. The scammers will then ask their victim to set up a transaction using the victim's account. Details of this scheme was published as a fraud alert on the FRA's website. (see https://fra.gov.ky/increase-in-phone-scams-targeting-older-adults/)

Credit Card / Debit Card schemes

After receiving an advisory from the Cayman Islands Bureau of Financial Investigation (CIBFI) the FRA published an alert regarding individuals travelling to the Cayman Islands

to commit credit card fraud against local merchants using Point of Sale (POS) terminals. The FRA had also received SARs from local merchants regarding such schemes. (see https://fra.gov.ky/credit-card-fraud-targeting-local-merchants/)

Though less than in 2023, the FRA continue to receive SARs from banks regarding Credit Card / Debit Card schemes. In these cases it is suspected that overseas vendors were compromised resulting in fraudulent transactions taking place. The FRA also observed fewer cases regarding perpetrators use of brute-force computing to guess a valid combination of credit card number, expiration date and card verification value, or CVV number.

Crypto Frauds

The FRA continues to see significant number of cases identifying frauds involving crypto assets during 2024. A significant number of cases involved direct or indirect transactions with a wallet associated with a Darknet entity, in particular fraud shops. Continuing the trend from 2022, a significant number of requests from OFIUs regarding frauds in their jurisdictions that involved crypto transactions or a wallet with a Cayman nexus.

Sanctions and Politically Exposed Persons ("PEPs")

There was significant overlap on cases with sanctions and PEPs. There continued to be a notable number of cases with sanctions and PEPs as the reason for suspicion, primarily linked to sanctions imposed by the United Kingdom and other countries on Russia in response to the invasion of Ukraine on 24 February 2022.

The vast majority of cases reported that persons designated by OFSI were directly or indirectly, through foreign companies, investors in Cayman funds. A handful of cases reported that designated persons were the beneficial owners of Cayman companies.

A significant number of designated persons were also deemed to be PEPs; however, some cases with PEPs were aligned with foreign corruption.

Corruption

Corruption also featured prominently in the 2021 NRA. With regard to foreign-generated proceeds of crime, corruption/bribery received a High threat rating and was identified as the number two threat for the risk of money laundering. With regard to domestically generated proceeds of crime, corruption received a Medium-Low threat rating and was ranked number 4 for the risk of money laundering.

The ACA, as well as global benchmarks in anti-bribery legislation like the UK's Bribery Act 2010 and the US Foreign Corrupt Practices Act ("FCPA") continue to keep the focus of bribery and corruption firmly in the minds of those operating businesses in the Cayman Islands.

The vast majority of the SARs citing corruption as a reason for suspicion received during the Reporting Period involved foreign corruption. In some cases FSPs reported that individuals and companies that are either under

investigation or have been charged for corruption overseas maintained an account. Reports were also received identifying Cayman domiciled entities whose directors, officers or beneficial owners, or related parties, are linked to overseas investigations.

Also included in this category are requests for information from overseas FIUs regarding corruption investigations, transactions which appear to be linked to bribes or the solicitation of bribes or kick-backs.

Money Laundering

The processes by which proceeds of crime may be laundered are extensive. The financial services industry, which offers a vast array of services and products, is susceptible to misuse by money launderers. While all crimes can be a predicate offence for money laundering, this category is used by the FRA to identify SARs whose reason for suspicion is the act of money laundering.

In 2024, a large portion of SARs in this category came from domestic reporting entities which typically involve adverse media regarding a person who is subject to foreign criminal proceedings, has been charged or is under investigation, or is closely associated with individuals who are under investigation for money laundering.

A smaller portion of cases in this category came from requests for information from overseas FIUs and local law enforcement pertaining to money laundering investigations.

SAR Triggers

During 2024, the FRA started recording 'Triggers' for filing SARs (i.e. the main cause(s) that initiated the filing of a SAR) that were closed during the Reporting Period. As this was implemented partway in 2024, a trigger was not recorded for all cases closed. Additionally, a trigger was not recorded for RFIs from LEAs, Competent Authorities or OFIUs. The table below shows the conditions that initiated filing of SAR[3].

SAR Triggers	2024
Adverse information – periodic review	126
Adverse information – ongoing monitoring	61
Adverse information – onboarding	53
Transaction monitoring – ongoing	335
Transaction monitoring – periodic review	27
Unusual service request made by client or customer	8
RFI by LEA or CA (Domestic)	21
RFI by LEA or CA (International)	62
Specific Business Events	166

[3] More than one trigger was identified for 23 cases.

3. Disseminating Intelligence

Disposition of Cases

The dissemination or disclosure of financial intelligence, resulting from its analysis, is a key function of the FRA. Once information is analysed and the Director has reviewed and agreed with the findings, a determination is made regarding onward disclosure.

Pursuant to section 138 of the POCA, financial intelligence is disclosed to the following designated agencies where the required statutory threshold, suspicion of criminal conduct, has been met:

- ☒ Local law enforcement agencies in the Cayman Islands.
- ☒ Any competent authority, supervisory authority within the Islands and such other institutions or persons in the Islands designated by the Anti-Money Laundering Steering Group.
- ☒ Overseas financial intelligence units.

The statutory purposes of onward disclosure are to:

- ☒ report the possible commission of an offence;
- ☒ initiate a criminal investigation;
- ☒ assist with any investigation or criminal proceeding; or
- ☒ facilitate the effective regulation of the financial services industry.

The POCA was initially amended in December 2017 (and again in 2023) to allow the FRA to disseminate, in its discretion or upon request, information and results of any analysis to the same parties named above.

Cases which do not meet the threshold for disclosure (or are not disclosed under section 4(2)(ca)) are retained in the FRA's confidential SAR database pending future developments. As new cases are received and matched with data in the SAR database, prior cases may be re-evaluated with the receipt of new information.

During the Reporting Period, the FRA received 1,395 new cases. The FRA completed the review of 775 of these cases, leaving 620 in progress at 31 December 2024. Of the 775 new cases closed, 238 were filed as intelligence, 25 were deemed to require no further immediate action, 385 resulted in a disclosure, 86 were replies to requests from FIUs and 41 were replies to requests from local agencies.

The FRA also completed the review of 177 of the 644 carried over from 2023, 14 of 480 cases carried over from 2022, 14 of 437 cases carried over from 2021, 14 of 430 cases carried over from 2020, 9 of 630 cases carried over from 2019, 4 of 369 cases carried over from 2018, 9 of the 201 cases carried over from the interim period of 1-Jul-17 to 31-Dec-17, 6 of 234 cases carried

	Reporting Period									
Disposition	**2024**	**2023**	**2022**	**2021**	**2020**	**2019**	**2018**	**2017**	**2016-17**	**2015-16**
Royal Cayman Islands Police Service	370	131	10	9	5	4	1	-	2	-
Cayman Islands Monetary Authority	295	107	9	7	6	2	-	-	1	-
Other Local Law Enforcement Agencies	30	2	-	-	-	2	1	-	-	-
Other Competent Authorities	13	1	-	1	-	-	-	-	-	-
Overseas FIUs	320	124	10	8	6	6	-	-	1	1

Table 3.8: Number of SARs that contributed to disclosures made during 2024

	No. of Cases									
Disposition	**2024**	**2023**	**2022**	**2021**	**2020**	**2019**	**2018**	**1 Jul – 31 Dec 2017**	**2016-17**	**2015-16**
Cases Analysed Requiring No Further Action	25	44	29	34	248	211	212	222	132	297
Filed as intelligence	238	333	246	209	6	-	-	-	-	-
Cases Analysed that Resulted in a Disclosure	385	495	674	225	242	189	246	106	162	196
Reply to Domestic Requests	41	34	22	33	40	37	17	8	8	3
Reply to Overseas Requests	86[4]	128[5]	149[6]	101[7]	69[8]	80[9]	95[10]	35[11]	71[12]	61[13]
In Progress (as at 31 December 2023)	620	467	466	423	416	621	365	192	228	63
Total Cases	1,395	1,501	1,586	1,025	1,021	1,138	935	563	601	620

Table 3.9 Disposition of cases received as at 31 December 2024

[4] Six of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[5] Three of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[6] Fifteen of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[7] Seventeen of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[8] Twelve of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[9] Ten of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[10] Ten of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[11] One case also resulted in a disclosure, but is not included in the number of cases disclosed to avoid double counting.
[12] Six of these cases also resulted in disclosures, but are not included in the number of cases disclosed to avoid double counting.
[13] One of these cases also resulted in disclosures, but is not included in the number of cases disclosed to avoid double counting.

over from 2016/17 and 85 of 148 cases carried over from 2015/2016, a total of 332 cases. Of the 332 previous cases that were completed, 20 were filed as intelligence, 118 were deemed to require no further immediate action, 170 resulted in a disclosure, 12 were replies to requests from LEAs and 12 were replies to requests from FIUs. Those 170 cases together with the 385 from 2024 comprise the 555 cases disclosed in the manner shown in Table 3.8. The total number of cases disclosed exceeded the number of actual cases, as some disclosures were made to more than one local law enforcement agency and / or overseas FIU.

Table 3.9 shows the disposition of the cases for the past ten reporting periods as at 31 December 2024.

As at 31 December 2024, the FRA had commenced initial analysis on: 275 of the 620 pending 2024 cases; 223 of the 467 pending 2023 cases; 168 of the 466 pending 2022 cases; 102 of the 423 pending 2021 cases; 149 of the 416 pending 2020 cases; 186 of the 621 pending 2019 cases; 103 of the 365 pending 2018 cases; 45 of 192 pending Jul – Dec 2017 cases; 50 of 228 pending 2016/2017 cases; 25 of 63 pending 2015/2016 cases; and 38 of 38 pending cases from 2014/2015.

Financial Intelligence Disclosures

The actual number of financial intelligence disclosures (i.e., the number of letters containing financial intelligence) is presented below.

Recipient	2024	2023	2022
RCIPS	244[14]	214[15]	152[16]
CIMA	150	105	65[17]
ACC	12	3[18]	9[19]
CBC	35[20]	19[21]	9
CARA	-	1	2
DITC	-	2	1
DCI	7	5	1
GR	1	-	-
Overseas FIUs	519[22]	491[23]	374[24]
Total	968	842	613

While some SARs have a direct and immediate impact on investigations both domestic and overseas, some are more useful when coupled with information available in other SARs, as well as law enforcement and regulatory publications. Both instances however assist in the production of financial intelligence.

The top 5 reasons for disclosures made to the RCIPS during the reporting period were:

- fraud – 54%
- money laundering – 11%
- Corruption – 8%
- Drug trafficking – 7%
- Theft – 5%

[14] Includes 22 responses to 19 requests
[15] Includes 13 responses to 13 requests
[16] Includes 14 responses to 17 requests
[17] Includes 3 responses to 3 requests
[18] Includes 1 response to 1 request
[19] Includes 3 responses to 3 requests
[20] Includes 21 responses to 21 requests
[21] Includes 9 responses to 9 requests
[22] Includes 98 responses to 98 RFIs from overseas FIU that disclose substantial information
[23] Includes 140 responses to 145 RFIs from overseas FIU that disclose substantial information
[24] Includes 142 responses to 140 RFIs from overseas FIU that disclose substantial information

The top 5 reasons for disclosures made to Overseas FIUs during the reporting period were:

- fraud – 56%
- money laundering – 10%
- sanctions matters – 8%
- international corruption – 6%
- drug trafficking – 3%

Voluntary Disclosures Overseas

The FRA discloses financial intelligence to its overseas counterparts, either as a result of a suspicion formed through its own analysis, or in response to a request for information. During the Reporting Period, the FRA made 421 voluntary disclosures to overseas FIUs from 476 cases completed. Those 476 cases comprise: 320 cases from 2024, 124 cases from 2023, 10 cases from 2022, 8 cases from 2021, 6 cases from 2020, 26 cases from 2019, 1 report from 2016/2017, and 1 report from 2015/2016.

In 2023 the FRA made 351 voluntary disclosures to overseas FIUs from 499 cases completed. Those 499 cases comprise 304 cases from 2023, 170 cases from 2022, 7 cases from 2021, 6 cases from 2020, 2 cases from 2019, 8 cases from 2018, and 2 cases from 2016/2017.

The FRA also provided 98 responses to 98 requests for information from overseas FIUs. Those requests comprise: 86 requests from 2024, 10 requests from 2023, and 2 requests from 2021.

In 2023, the FRA also responded to 145 requests for information from overseas FIUs. Those requests comprise: 118 requests from 2023, 20 requests from 2022, 6 requests from 2021, and 1 request from 2019.

Chart 3.10 on the next page shows that the 2024 voluntary disclosures and responses went to 82 different jurisdictions.

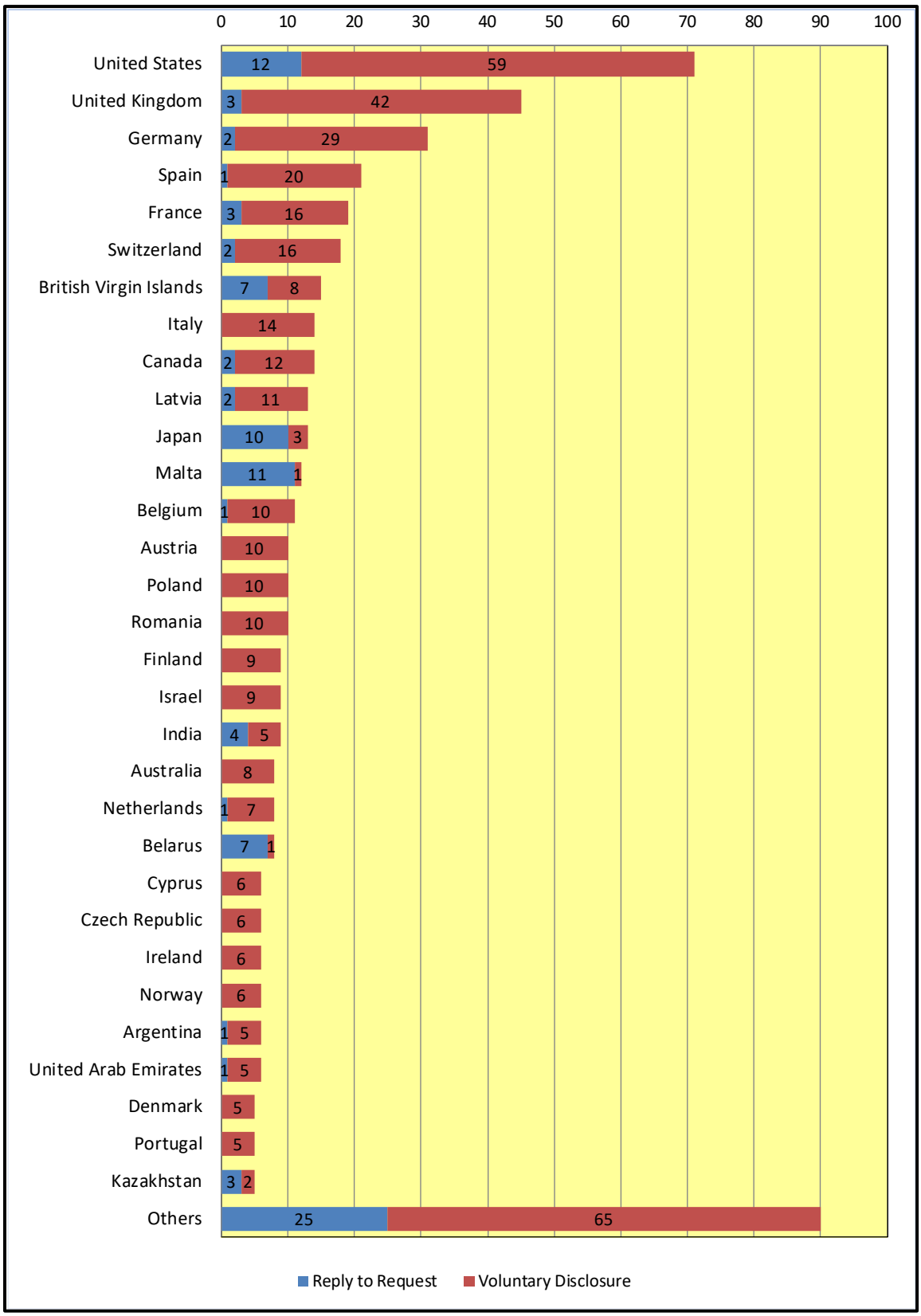


Chart 3.10: Overseas disclosures and replies to request for information

Significant Events

Analysis of Cases

The FRA had 3,843 cases to analyse during the Reporting Period, comprising: 1,395 new cases, 356 cases carried over from 2023, 319 cases carried over from 2022, 347 cases carried over from 2021, 281 cases carried over from 2020, 445 cases carried over from 2019, 265 cases carried over from 2018, 148 cases carried over from Jul – Dec 2017, 184 cases carried over from 2016/2017 and 103 carried over from 2015/2016. There were also 1,162 cases that were initially analysed, but not completed as they required further analysis, comprising: 287 carried over from 2023, 161 carried over from 2022, 90 carried over from 2021, 149 cases carried over from 2020, 185 cases carried over from 2019, 104 cases carried over from 2018, 53 cases carried over from Jul – Dec 2017, 50 cases carried over from 2016/2017, 45 cases carried over from 2015/2016, and 38 cases carried over from 2014/2015.

The FRA staff analysed 1,326 cases, during the Reporting Period, comprising: 1,054 cases from 2024, 118 cases from 2023, 21 cases from 2022, 27 cases from 2021, 15 cases from 2020, 11 cases from 2019, 4 cases from 2018, 1 case from Jul – Dec 2017, 7 cases from 2016/2017 and 68 cases from 2015/2016. An average of 110 cases were analysed per month in 2024 compared with 124 cases in 2023.

A total of 1,107 cases were closed during the Reporting Period, comprising: 775 cases received in 2024, 177 cases received in 2023, 14 cases received in 2022, 14 cases received in 2021, 14 cases received in 2020, 9 cases received in 2019, 4 cases received in 2018, 9 cases received in Jul-Dec 2017, 6 cases received in 2016/2017 and 85 cases received in 2015/2016. On average, 92 cases were completed per month in 2024 compare with 94 cases in 2023.

Results of Disclosures of Information

Feedback from local law enforcement agencies and competent authorities revealed an ongoing use of financial intelligence disclosed by the FRA, including the following:

	2024	
Contents of the Disclosure	**CIBFI**	**CIMA**
Provided new information regarding known subjects	25	-
Provided you with unknown subjects	22	2
Corroborated information already known	14	2
Information disclosed to another agency	1	-
Triggered new investigation	3	-
Use of the Disclosure		
Actionable	23	3
Not Actionable	88	-
Total Feedback Forms provided	**111**	**3**

The FRA also provided assistance to law enforcement by responding to requests from them with any relevant information held by the FRA. Some of these cases also involved

the FRA requesting information from OFIUs on behalf of the local law enforcement agency.

Use of Section 4(2)(b) Powers

During the Reporting Period the FRA did not exercise its powers under section 4(2)(b) of the POCA. The FRA did make one application to the Grand Court seeking permission to exercise the power; however, permission was not granted as the Court was not satisfied that the FRA had reasonable cause to believe that the information contained in the report related to proceeds or suspected proceeds of criminal conduct. In 2023 the FRA used its powers under section 4(2)(b) of the POCA on four (4) occasions ordering entities to refrain from dealing with a person's account for twenty-one days. The assets held by the accounts in question totalled approximately US$1.8 million.

This power is only exercisable after the Grand Court grants permission to do so, having been satisfied that the FRA had reasonable cause to believe that the information contained in the report related to proceeds or suspected proceeds of criminal conduct.

Financial Sanctions

During the Reporting Period the FRA published 104 (2023: 128) Financial Sanctions Notices on its website. The FRA subscribes to the Email Alert provided by the Office of Financial Sanctions Implementation OFSI within UK HM Treasury, advising of any changes to United Nations, European Union and UK financial sanctions in effect.

During the Reporting Period the FRA published 7 Specified Ship Sanctions Notices (a total of 109 ships specified) on its website. The FRA subscribes to the Email Alert provided by the Foreign, Commonwealth & Development Office ("FCDO"), advising of shipping sanctions. A specified ship is prohibited from entering a port in the Cayman Islands, may be given a movement or a port entry direction, can be detained, and will be refused permission to register on the Cayman Islands Shipping Registry or may have its existing registration terminated.

The FRA forwards these notices automatically to local law enforcement agencies and competent authorities, converts it to a Cayman Notice and publishes the Cayman Financial Sanctions Notice on its website. The average turn-around time for converting these notices, distributing them via e-mail and posting them to the FRA's website is between 1-3 hours.

IV. SCENARIOS THAT WOULD TRIGGER FILING OF A SUSPICIOUS ACTIVITY REPORT (TYPOLOGIES)

The following is a compilation of sanitised cases that were analysed and completed during the Reporting Period that we believe illustrate some of the key threats facing the jurisdiction in the fight against money laundering and terrorist financing. These cases have been identified by the primary typology involved, though some of them may involve more than one typology. They are being included here for learning purposes and as a feedback tool for our partners in the fight against money laundering and terrorist financing.

1. FRAUD – Misappropriation of Assets

The FRA received a SAR from a Cayman Islands registered mutual fund ("the Fund") regarding Subject A, a beneficial owner of an investor in the Fund, Company X. The Fund became aware of a press release issued by authorities in Jurisdiction 1, identifying Subject A as one of several individuals accused of defrauding investors in a scheme carried out by Company Y in Jurisdiction 1.

While the press release was recent, the allegations contained therein occurred prior to Company X's investment in the Fund. The press release also alleged that the proceeds of the scheme were dispersed to other entities controlled by Subject A and associates. As such the Fund could not rule out the possibility that the money invested was the proceeds of crime.

FRA analysis showed that while Company X was incorporated in Jurisdiction 2, its sole shareholder was Company Z incorporated in Jurisdiction 1. Further, Subject A's ownership of Company Z was not clearly outlined raising the possibility that the ownership of Company X might not be known to authorities in Jurisdiction 1.

As the possibility that the investment in the Fund was proceeds of crime, the FRA made disclosures to RCIPS, CIMA and the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators:

- Adverse media on a UBO of an existing investor in the Fund
- Timing of the investment coincides with or in close proximity to the alleged criminal activity

2. Fraud – Account Take-Over

The FRA received a SAR from a Cayman Islands Bank regarding Client A being the victim of an account take-over fraud after numerous fraudulent transactions were initiated or attempted. Persons B and C are authorised persons on Client's A account.

The account review was initiated due to a fraudulent request for wire transfer initiated from Person B's online banking profile. Having verified that the request was fraudulent, the intended beneficiary, the IP address and the device used was added to the Bank's internal blocked lists. Person B's online banking profile was recreated.

The Bank's review also showed that it had previously also blocked 3 wire transfers that were initiated via Person C's online banking profile and via email. The Bank's call-back procedures caught the attempted transfers and Person C's online banking profile was recreated.

The Bank again caught a further attempt for wire transfer made from Person B's online banking profile suggesting that their devices had been compromised. The Bank decided that to secure the customer's account their online banking profile would be restricted to "view only" access. After another attempted wire payment was received by the Bank and rejected by its fraud team, Person B's profile was completely blocked for security purposes.

A few days later the Bank noted another payment was held up by its monitoring team. The Bank discovered that the payment was not initiated online or via email, but was set up as a standing instruction that was created online prior to the account being blocked. Four instructions were set up to wire funds to four beneficiaries overseas. Three of the wires were rejected by the receiving banks for invalid beneficiaries and the fourth wire was recalled.

The accounts of the intended beneficiaries of the transfer / attempted transactions were at financial institutions located in Jurisdictions 1, 2 and 3.

FRA research noted that one of the intended beneficiaries had previously been linked to BEC scams in Jurisdiction 1.

Disclosures were made to RCIPS and OFIUs in Jurisdictions 1, 2 and 3 for intelligence purposes.

Indicators

- Numerous attempted fraudulent transactions identified by call-back procedures
- Compromised online banking profiles
- Use of standing instructions to by-pass user account restrictions
- Intended beneficiary linked to BEC frauds and a jurisdiction considered a high risk for scams

3. Fraud - Business Email Compromise

A Cayman Islands Bank filed a Suspicious Activity Report after their customer requested the recall of three wire transfers initiated using the Bank's online banking facility. It was identified that email instructions to change banking

account details received by the customer from its major supplier were fraudulent. The customer had received an email from its long-standing major supplier providing information about a new bank account and gave instructions to send payments to the new account going forward; the customer made payment for three invoices to the new bank account at a financial institution in Jurisdiction 1.

The fraud was discovered when the supplier followed up on the outstanding invoices. Afterwards the customer noted that it was unusual that the supplier failed to acknowledge receipt of each of the payments made, which it usually did prior to the change in bank details. It was subsequently determined that the email of one of the supplier's employees had been compromised.

Disclosures were made to RCIPS and the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators

- Sudden change in bank account details communicated via email
- Unusual change in customer / vendor behaviour (e.g., failure to issue acknowledge / issue receipts for payment when it had previously done so).

4. Fraud - Credit Card Scheme

A jewellery store filed a SAR regarding a suspected credit card fraud after chargebacks were received from a Cayman Islands Bank. A chargeback is when the card issuer returns funds to the account due to a disputed charge. The Jewellery store reviewed details of transactions on the date of the transaction and identified a potential Subject, a visitor from Jurisdiction 1.

A review of the store cameras showed that the Subject entered the store wearing a jacket with a hoodie and appeared to be avoiding the direction of the cameras. The Subject made an initial purchase and attempted to pay with a mobile payment service, which was unsuccessful. The Subject claimed they would have to enter a code and asked to personally enter this in the credit card machine. After being given access to the credit card machine the sale was completed. While waiting for a certificate of authenticity, the Subject identified another piece of jewellery and asked for the initial purchase to be refunded so that the second item could be purchased. The second item was twice the amount of the first item selected. Similar to the first instance the Subject requested access to the credit card machine to enter a code.

A subsequent review by the jewellery store shows that the Subject manually entered a credit card number and did not use a mobile payment service.

In performing its analysis, the FRA identified a similar scheme where three

individuals from Jurisdiction 1 were charged and subsequently pleaded guilty to obtaining property by deception in relation to several fraudulent purchases made in Grand Cayman using stolen credit card details. Among the items seized by police were jewellery, perfumes, and electronics. The FRA was able to match the likeness and identity details of the Subject to one of three individuals charged.

Disclosures were made to RCIPS and the OFIU in Jurisdiction 1 for intelligence purposes.

RCIPS and the FRA published a fraud alert in April 2024 regarding individuals travelling to the Cayman Islands to commit credit card fraud against local merchants using Point of Sale (POS) terminals. https://fra.gov.ky/credit-card-fraud-targeting-local-merchants/

Indicators:

- Claims of use of mobile payment service but payment is completed using manually entered credit card details
- Repeated request to access / control credit card machine and personally enter details after incomplete / failed transactions
- Unusual behaviour, including attempting to conceal face via clothing and avoiding in store cameras

5. Fraud – Romance Scam

The FRA received a SAR from a Cayman Islands Bank regarding Subject A and Company X in connection with a suspected romance fraud. The victim, a client of the Bank, met Subject A on a dating platform; Subject A, claimed to be a businessperson from Jurisdiction 1.

Subject A made excuses to avoid video chats or meeting in person but continued to communicate with the victim via instant messaging applications. After some time, Subject A claimed to be in financial difficulty while on an overseas trip to Jurisdiction 2. Subject A claimed to have been fined and detained after withdrawing from a major business deal and needed urgent financial assistance to leave the country. Under a formalised loan agreement involving purported legal representatives, the victim provided financial support.

After the initial transfer, Subject A made repeated requests for additional funds, including for alleged medical expenses. The victim sent multiple wire transfers to an account at a bank in Jurisdiction 1 held by Company X. The victim became sceptical when Subject A gave instructions to contact lawyers for repayment of the loan. Further, when the victim contacted the lawyers, the lawyers demanded a retainer. The victim's research showed that the law firm had ceased operations several years prior.

The victim advised the Bank of the wire transfers and reported the matter to relevant regulatory and law enforcement authorities in Jurisdiction 1.

The FRA made disclosures to RCIPS and the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators

- Online relationship but avoids face-to-face meetings; solely uses text, email, or messaging services for communication
- Sudden request for funds or loan to pay for unforeseen emergency; continuing request for funds after initial request was granted
- Alleged use of an intermediary firm to give the impression of legitimacy

6. **Fraud – Fraudulent Representation / Debt Collection Scam**

The FRA received SARs from four law firms and one real estate agent in the Cayman Islands regarding a pattern of attempted fraud involving fictitious entities and individuals utilising dubious payment methods such as bank drafts and cashier's cheques originating from Jurisdictions 1 and 2, which were inconsistent with the stated business activities.

The reported SARs followed a common pattern in which fraudsters approached professional service providers with seemingly legitimate requests, such as debt collection or real estate transactions, only to introduce suspicious elements upon further review. These included forged or altered documentation, discrepancies in identification details, unverified business entities, and attempts to circumvent due diligence requirements. Payment instruments, often high-value bank drafts or cashier's cheques, were issued from institutions unrelated to the supposed business transactions, further raising concerns.

Of note, one of the law firms carried out a comprehensive analysis of the parties and information received, resulting in a detailed, very high-quality SAR filing that added significant value to the FRA's analysis

One notable trend was the use of encrypted messaging applications or unconventional communication methods, along with pressure to expedite transactions without proper verification. Additionally, funds were often directed to third parties with no clear connection to the transaction.

Although the business was declined by the reporting entities, their SAR filings provided very useful information.

Disclosures were made to RCIPS, DCI and OFIUs in Jurisdictions 1 and 2 for intelligence purposes.

Indicators:

- Fraudulent or altered documentation,

including identification documents
- Geographical inconsistencies in documentation and transactions
- High-value transactions requiring expedited processing
- Payments from unrelated third parties
- Communication through unconventional and encrypted channels
- Use of non-corporate email addresses
- Non-compliance with KYC requirements

7. Fraud – Use of Virtual Assets

The FRA received a SAR from a VASP reporting that its customer, Subject A, was named as a wanted person in Jurisdiction 1 in relation to a fraud investigation. The VASP did not find anything suspicious about Subject A's transactions. As supporting documentation, the VASP provided Subject A's transaction history and a list of IP addresses used to access Subject A's crypto wallet.

The FRA's review of the information identified that Subject A's crypto-debit card transactions and the associated IP addresses were occurring from Jurisdiction 2, although all other documents provided suggested residence in Jurisdiction 1.

The FRA made disclosures to RCIPS, CIMA and OFIUs in Jurisdictions 1 and 2 for intelligence purposes. RCIPS requested the FRA's permission, which was granted, to send the intelligence to the Interpol Fugitive Desk.

Indicators:
- Adverse media regarding fraud / wanted persons
- Account accessed regularly from unrelated jurisdiction

8. Money Laundering

The FRA received SARs from three law firms in relation to Subject A being linked to fraudulent activity and money laundering. Subject A holds dual nationality, including Jurisdiction 1.

Law Firm 1 was acting for parties that were purchasing a property; Subject A was the vendor. Law Firm 1 became suspicious as Subject A exhibited nervous and hyperactive behaviour while completing paperwork related to the sale. Subsequent due diligence checks disclosed that Subject A is a defendant in a local fraud case involving a significant monetary amount. Other adverse information linking Subject A to the importation of a controlled drug, evading customs duties and labour related offences.

Law Firm 2 had previously assisted Subject A with the purchase of other properties a few years ago. Law Firm 2 reported similar adverse media findings which raised concerns about the

legitimacy of the funds used to purchase the properties, including one funded in cash by Subject A.

The FRA also identified a prior SAR filed by Law Firm 3 concerning a land sale that failed to be completed; one of reasons the transaction was not completed was outstanding due diligence documents. Concerns were raised regarding the lack of transparency regarding the ownership of Company X, the purchaser, which eventually led to forfeiture of the deposit. The FRA subsequently determined that Company X was controlled by Subject A.

The concerns raised by the three SARs suggested that Subject A may be laundering the proceeds of illicit activities through the real estate transactions.

Disclosures were made to RCIPS, DCI and the OFIU in Jurisdiction 1.

Indicators:

- Adverse media related to fraud and illicit drugs
- Due diligence concerns regarding transparency of ownership
- Subject displaying suspicious behaviour
- Cash purchase of property

9. International Corruption and Money Laundering

The FRA received four SARs from various service providers in relation to an international corruption and money laundering matter involving a number of subjects. Subject A together with other individuals were charged in Jurisdiction 1 with corruption and money laundering. Subject A is the UBO of Company X. Subject A relocated to the Cayman Islands and owned property in the name of Company X. A number of the subjects were residents or nationals of Jurisdiction 2.

Among the concerns raised by different service providers were:
Use of trust in overseas jurisdictions that appears to obscure beneficial ownership
Incomplete information about source of funds
Existence of dated adverse information about corruption and money laundering

The FRA's analysis found that while the charges were dated it was still an active matter in Jurisdiction 1. Further, asset recovery measures had been initiated. The FRA also identified other entities domiciled in the Cayman Islands linked to Subject A during its analysis.

The FRA issued Section 4(2)(c) Directives to the registered offices of the Cayman Islands entities linked to Subject A and results indicated that Subject A held various assets in entities through trusts established in Jurisdiction 3.

Given an active criminal matter and asset recovery measure, suspicions arose that the assets beneficially owned by Subject

A and others might be the proceeds of crime.

Disclosures were made to RCIPS, CIMA and the OFIUs in Jurisdictions 1, 2 and 3.

Indicators:

- Use of trust in overseas jurisdictions that appears to obscure beneficial ownership information
- Incomplete information/ reluctance to provide information about source of funds
- Adverse information about corruption and money laundering
- Asset recovery measures

10. Drug Trafficking

The FRA received a SAR from a Money Services Business ("MSB") regarding Subject A who was making numerous cash remittances to individuals in Jurisdiction 1. The MSB noted that a substantial portion of Subject A's remittances were sent to two individuals and that Subject A appears to have kept the remittances below the threshold amounts to avoid providing information on source of funds. The destination of the remittances in Jurisdiction 1 added to the suspicion, as it was a known area for drug and money laundering activities.

The FRA's analysis observed the following:

- Subject A had been previously arrested for numerous drug related offences in the Cayman Islands
- Subject A's earnings were not commensurate with the remittances

A disclosure was made to RCIPS.

Indicators:

- Numerous remittances to individuals in a known high-risk area
- Remittances not commensurate with Subject A's earnings
- Appears to be avoiding reporting threshold

11. Drug Trafficking

The FRA received a SAR from a Cayman Island Bank regarding a customer, Subject A, after a routine review identified a match between Subject A's name and publicly available information regarding possession of a controlled substance with intent to supply and consumption of a controlled substance. Additionally, media reports indicated that the subject and an associate had been arrested and charged with possession of criminal property.

In conducting its analysis, the FRA identified another SAR naming a person suspected to be associated with Subject A with similar adverse media. That case was previously disclosed to RCIPS.

A disclosure was made to RCIPS for intelligence purposes.

Indicators:

- Adverse media referencing criminal

activity
- Name match identified during a routine review

12. Child Abuse – Virtual Asset

The FRA received a SAR from a VASP after identifying that Subject A had directly transacted with a crypto wallet associated with child abuse related material. Subject A resides in Jurisdiction 1.

The FRA made disclosures to RCIPS, CIMA and the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators:
- Direct transaction with a crypto wallet associated with child abuse related material

13. Darknet Crypto Transactions

The FRA received numerous SARs from a VASP in relation to direct and indirect transactions conducted by subjects resident in various countries with wallets associated with Darknet Markets. The Darknet Markets included: fraud shops; sale of illicit drugs; sale of credit card information or other personal identification; and entities sanctioned in another jurisdiction.

The FRA made disclosures to RCIPS, CIMA and the relevant OFIUs for intelligence purposes.

Indicators:
- Transaction with a crypto wallet linked associated with a Darknet Market

These examples are based on actual information we have received and sanitised to protect the identities of the individuals or entities concerned.

Further typologies can be found at www.Egmontgroup.org or www.FATF-GAFI.org or www.cfatf-gafic.org.

V. STRATEGIC PRIORITIES: PERFORMANCE FOR 2024 AND BUILDING ON STRENGTHS IN 2025

The FRA plays a crucial role in the jurisdiction's fight against being used for money laundering, terrorist financing, proliferation financing and other financial crime. It is also a vital agency in the Cayman Islands' efforts to demonstrate compliance with the FATF 40 Recommendations and prove effective implementation of those Recommendations.

Performance 2024

During 2024 our main priorities were:

1. **Produce useful intelligence reports in a timely manner**

   This priority was largely achieved. Through its analysis of information collected under the POCA reporting requirements, the FRA developed specific financial intelligence disclosures and provided strategic insights into trends and patterns of financial crime.

   During 2024, the FRA:

   (i) Produced 968 financial intelligence reports (disclosures) for use by local law enforcement agencies, CIMA and other Supervisors, and overseas FIUs. Overall, positive feedback was received from local law enforcement agencies, CIMA and overseas FIUs regarding the usefulness of disclosures by the FRA. The FRA also periodically met with local agencies and obtained formal feedback on the usefulness of our intelligence reports. The FRA received 111 Feedback forms from the RCIPs and 3 Feedback forms from CIMA.

   (ii) Continued to disseminate information in a timely manner. With the FRA actively monitoring the timeliness of our disclosures, 51% of disclosures to local law enforcement were made within 35 days, compared to 53% in 2023. The average number of days to complete a request for information from an overseas FIU was 45 days in 2024, compared to 42 days in 2023.

   (iii) Produced trends and patterns of financial crime impacting the Cayman Islands, which are featured in this Annual Report.

2. **Promote cooperative relationships with Reporting Entities**

   This priority was largely achieved. Throughout the Reporting Period we maintained and developed cooperative working relationships with reporting entities.

During 2024, Staff of the FRA engaged in the following Outreach events covering one or more of the following topics: functions of the FRA, SAR statistics, SAR reporting obligations, and obligations regarding targeted financial sanctions related to terrorist financing and proliferation financing:

(i) Two (2) presentations at international and domestic industry association events, or other international events.

(ii) Two (2) 1-on-1 meetings with Money Laundering Reporting Officers (MLROs).

(iii) One (1) meeting with a MLRO to demonstrate AMLive Reporting Portal functionalities.

During 2024 the FRA issued 45 feedback forms to 22 reporting entities from a cross-section of sectors, with the following quality ratings: (i) Poor: 1; (ii) Fair: 1 (iii) Good: 20; and (iv) Very Good: 23.

The FRA utilised the features of its new website to publish three (3) fraud alerts in 2024. These alerts allow individuals and businesses to take necessary precautions in preventing fraudulent transactions or preventing them from progressing any further. The website was also used to publish 102 Financial Sanctions Notices.

3. Continue to meet International Standards and Enhance Cooperation with Domestic and International Counterparts

This priority was achieved. The FRA continued to work closely with all stakeholders to ensure robust AML/CFT/CFP legislation, policies and programmes are effectively implemented in the Cayman Islands.

During 2024, the FRA:

(i) Initiated a project to draft regulations and develop the infrastructure in relation to POCA amendments that will introduce a DAML / Consent regime in the Cayman Islands.

(ii) Met deadlines for CFATF HoFIUs reporting requirements and contributed to relevant Egmont Group working group activities by completing surveys and questionnaires.

(iii) The Director continued to make meaningful contributions to the Egmont Committee as detailed in this Annual Report.

4. High Performing Staff

This priority was achieved to a significant extent. Performance expectations for staff are clearly defined and documented. Staff completed analysis on 1,326 cases and closed 1,107 cases.

Staff were kept up to date with developing issues in AML/CFT/CFP

and in the Financial Industry through training events and workshops facilitated by international and domestic presenters, as detailed earlier in this Annual Report.

5. **Enhance benefits of New Information Technology Infrastructure**

This priority was achieved to some extent. The following were undertaken to maximise the benefits of the FRA's Information Technology Systems and Infrastructure:

(i) Members of staff received guidance on various technologies utilised by the FRA (Egmont Secure Web, ShareFile, i2 iBase and Analyst Notebook). For i2 iBase and i2 Analyst Notebook; this included running queries and creating browse definitions as well as using different datasheets for records.

(ii) Upgraded versions of i2 iBase and i2 Analyst Notebook to a newer version that is compatible with the new Windows operating systems rolled out by the Computer Services Department.

(iii) Continued with periodic evaluation of the infrastructure for sharing intelligence and communicating with Competent Authorities.

(iv) Completed the subscription for a cloud based Blockchain analytical tool.

(v) A limited amount of information was migrated from the old SAR database to the i2 iBase database; work is ongoing to complete the migration.

(vi) Continued liaison with the Office of the Chief Information Security Officer (CISO) to ensure robust preventative measures are in place and to address / respond to all security alerts.

(vii) Effectively used the functionality of the FRA's website to publish Sanctions Notices and Fraud Alerts.

Strategic Priorities for 2025

During 2025 we will continue to build on our strengths and seek to continuously improve performance. Our main priorities for the year will remain unchanged, namely:

1. **Produce useful intelligence reports in a timely manner**

An ongoing key priority for the FRA is to provide timely and high quality financial intelligence that meets the operational needs of local law enforcement agencies, CIMA and other Supervisors, and overseas FIUs.

Through its analysis of information collected under the POCA reporting requirements, the FRA aims to develop specific financial intelligence

disclosures and provide strategic insights into trends and patterns of financial crime.

To deliver on this priority, we will:

(i) Formally write to Competent Authorities and Supervisors to better understand their operational priorities and plan our workflows accordingly.

(ii) Continue to periodically assess the intelligence reports we produce to ensure that they are useful to the recipients.

(iii) Meet regularly with local agencies and obtain formal feedback on the usefulness of our intelligence reports. Feedback will also be sought from overseas FIUs.

(iv) Actively monitor the timeliness of our disclosures, with the aim of continuously improving disclosure times.

(v) Publish trends and patterns of financial crime impacting the Cayman Islands at least annually.

2. Promote cooperative relationships with Reporting Entities

The quality of our disclosures hinges directly on the quality of the SARs / information we receive. We are committed to developing and maintaining cooperative working relationships with all reporting entities, by encouraging an open line of communication to discuss matters of mutual interest, with a view to enhancing the quality of information we receive. The effective and efficient use of the AMLive Reporting Portal is integral to the accomplishment of this priority.

To deliver on this priority, we will:

(i) Engage with reporting entities utilising the feedback mechanism on the redeveloped website for general feedback and the AMLive feedback mechanism for feedback specific to a SAR submission.

(ii) Foster effective and efficient use of the AMLive Reporting Portal by actively responding to AMLive users inquiries or request for assistance; and by continuing to conduct virtual meetings as needed.

(iii) Make regular presentations at industry association organised events, as well as to individual entities at their request on their obligations under the POCA and the work of the FRA.

(iv) Increase the number of 'One-on-One' meetings with MLROs to give specific feedback on SAR quality, and discuss trends and other relevant matters.

(v) Continue to make use of the FRA's website to provide

reporting entities with a useful AML / CFT / CFP resource.

3. Continue to meet International Standards and Enhance Cooperation with Domestic and International Counterparts

The FRA will continue to work closely with the AMLSG, the Inter-Agency Coordination Committee (and its subcommittees), and divisions within the Cayman Islands Government to ensure that robust AML/CFT/CFP legislation, policies and programmes are effectively implemented in the Cayman Islands.

Internationally the FRA will continue active participation on CFATF and Egmont Group activities

To deliver on this priority, we will:

(i) Undertake relevant project work to improve effectiveness for the 5th Round MEP.

(ii) Coordinate all actions required to continue meeting the FRA's responsibilities under the relevant international standards.

(iii) Meet deadlines for any reporting requirements and contribute to relevant CFATF / Egmont working group activities.

(iv) The Director will continue to make meaningful contributions to the Egmont Group.

(v) Ensure that records, reports and publications showing the implementation and effectiveness of applicable acts and regulations are prepared and maintained.

(vi) Meet regularly with domestic law enforcement agencies and competent authorities to better understand their operational needs.

4. High Performing Staff

The FRA seeks to promote and create a culture of excellence and integrity that inspires exceptional teamwork, service and performance. The development of staff by ensuring they are kept up to date with developing issues in AML/CFT/CFP is therefore critical to the effective operation of the FRA.

To deliver on this priority, we will:

(i) Continue to evaluate whether staff has sufficient access to appropriate data and software applications to respond to developing trends and patterns of financial crime impacting the Cayman Islands.

(ii) Continue to provide training opportunities in use of i2 iBase and i2 Analyst Notebook – this year's focus will be on effective use of new record types created and utilising the case

management capabilities of iBase.

(iii) Ensure that IT issues raised by staff are appropriately addressed.

(iv) Continue to provide relevant training to staff on new or emerging AML/CFT methods and trends, good practices, primarily using online resources.

(v) Develop skills to make the most effective and timely use of methods, tools and techniques to search for publicly available information on multiple platforms.

(vi) Continue to define clear performance expectations and provide timely feedback to staff.

5. Enhance benefits of Information Technology Infrastructure

Protecting information received from reporting entities is a critical function of the FRA. A layered approach to security has been adopted for the FRA's office and computer systems. Security measures include monitoring systems and advanced firewalls to prevent unauthorised access to our database.

The upgrades to the FRA's systems and infrastructures improved our overall security environment and provided opportunities for more effective and efficient operations. New technological tools are also being made available via the Egmont Secure Web.

In order to maximise the benefits of our Information Technology Systems and Infrastructure the following are to be completed:

(i) Complete upgrades to AMLive to incorporate requirements for the DAML / Consent Regime and make it more efficient for reporting entities to submit information on subjects and their associations.

(ii) Complete data migration from the old database to the new i2 iBase database, including retiring the former database and servers.

(iii) Provide relevant training on changes to software / technologies utilised by staff (Egmont Secure Web, ShareFile, blockchain tool, iBase and Analyst Notebook).

(iv) Provide feedback mechanism for staff to make suggestions on how technology could better assist in their analysis.

(v) Continue to assess and improve infrastructure for sharing intelligence and communicating with Competent Authorities.

(vi) In consultation with the CISO, formally implement procedures for a well-planned incident response program.

4th Floor Government Administration Building
George Town, Grand Cayman
Cayman Islands

Mailing Address
P.O. Box 1054
Grand Cayman KY1-1102
Cayman Islands

Telephone: 345-945-6267
E-mail: financialreportingauthority@gov.ky
Visit our Web site at: www.fra.gov.ky