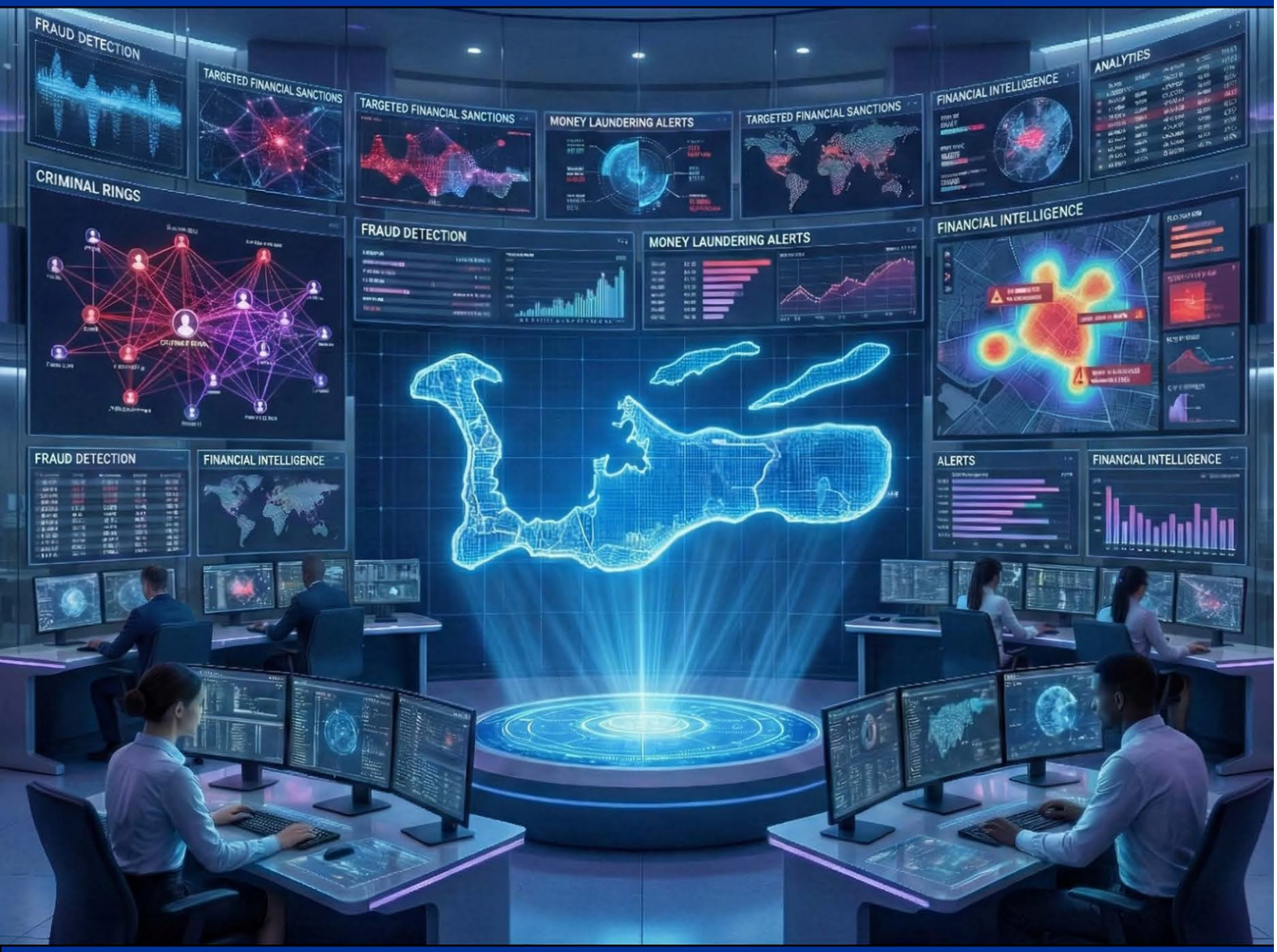
FINANCIAL REPORTING AUTHORITY



2025
ANNUAL REPORT

CAYMAN ISLANDS GOVERNMENT

PORTFOLIO OF LEGAL AFFAIRS

TABLE OF CONTENTS

MESSAGE FROM THE DIRECTOR

I am pleased to report on the operations of the Financial Reporting Authority ("FRA") in this annual report for the 2025 financial year ("the Reporting Period"), which marks the twenty third 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 1,532 cases during the Reporting Period, comprising 1,377 Suspicious Activity Reports ("SARs") from 337 Reporting Entities; 76 Requests for Information and 30 Voluntary Disclosures from 45 overseas Financial Intelligence Units ("OFIUs"); and 49 Requests for Information from Local Law Enforcement Agencies ("LEAs") and Competent Authorities. The number of cases received increased by 10% compared to the number of cases received during 2024 (1,532 vs 1,395).

During 2025 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 438 registered users from 223 Reporting Entities; 868 SARs (63%) were filed using AMLive during 2025 and 509 SARs (37%) were filed using secure email.

During the Reporting Period the FRA performed initial analysis on 1,587 cases. It also issued 175 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 21 requests for information to OFIUs, 16 of which were made to assist LEASs with investigations.

The FRA closed 1,144 cases during the Reporting Period, resulting in 284 disclosures to LEAs or competent authorities, and 254 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 2024, 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; and work in connection with the Russia Sanctions Taskforce. Apart from Russia Sanctions, there was an uptick in CRFs related to other sanctions regimes. 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").

The FRA spent substantial time implementing the Defence Against Money Laundering (DAML) / Consent Regime that came into force on 2nd January 2025, pursuant to the Proceeds of Crime (Amendment) Act, 2023 (Commencement) (Amendment) Order, 2024, sections 11, 12 and 13 of the Proceeds of Crime (Amendment) Act, 2023. The FRA issued an Industry Advisory on 10th January 2025 providing guidance to SAR filers on how to make a DAML / Consent request and how the DAML / Consent Regime will operate.

During the Reporting Period the FRA also spent significant time actively participating in working groups for the National Risk Assessment by providing observations, statistical data and typologies from SARs.

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, OBE
Director

2025 HIGHLIGHTS

Cases Received and Analysed

Actions Taken & Financial Intelligence Disclosures

Global Contribution

Domestic Action

254 Disclosure to Overseas FIUs

Top 3 Recipients of Overseas Disclosures

284 Domestic Disclosures Made

Top 3 Recipients of Domestic Disclosures

Targeted Financial Sanctions

111 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 (2025 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. Pursuant to the Proceeds of Crime (Amendment) Act, 2023 (Commencement) (Amendment) Order, 2024, sections 11, 12 and 13 of the Proceeds of Crime (Amendment) Act, 2023 came into force on 2nd January, 2025. In addition to filing a suspicious activity report (SAR), the amendments to sections 133, 134 and 135 of the Proceeds of Crime Act (POCA) now require SAR filers to have the consent of the Financial Reporting Authority (FRA) to 'commit the act'. This introduced a 'Defence Against Money Laundering (DAML) / Consent regime' to the Cayman Islands and removed the automatic defence contained in sections 133-135 POCA.

2. Misuse of Drugs Act (2026 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 (2025 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 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 111 Financial Sanctions Notices on its website, a slight increase from 102 in 2024. 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 2025 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 2025, a total of 158 Compliance Reporting Forms (CRFs) and 2 Reports by Designated Persons were received by the FRA related to the Russia Sanctions regime. As of 31 December 2025, a total of approximately USD$ 9.50 billion, EUR€230 million, CHF4 million and GBP271,000 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 2025, 23 (compared to 13 in 2024) 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 2025.

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 2025.

1. General Licence – Oil Price Cap (Amended). General Licence 2022/0002 permits certain Cayman Islands entities to make relevant

services available to third country importers and exporters providing that the price paid for Russian oil or oil products is at or below the relevant price cap. It also allows for the processing of payments related to the authorised activities. This General Licence was issued on December 15, 2022 and was amended on March 1 2023 and July 25 2025.

2. General Licence - Legal Services (Issued). General License GL/2025/0002 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 2026. The first Legal Services General Licence GL/2023/0002 was issued on April 14 2023, replaced on November 15 2023 with GL/2023/0003, May 24 2024 with GL/2024/001, December 19 2024 with GL/2024/0002, May 7 2025 with GL/2025/0001 and October 29 2025 with GL/2025/0002.

3. General Licence – Redemption/Withdrawal of investment, basic needs, routine holding and maintenance and payment of legal fees (Amended). General Licence 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 General Licence was issued on October 4 2022 and was amended on April 5 2023, October 6 2023, October 16 2024 and October 16 2025.

4. General Licence – Russian Oil Exempt Projects (Issued). General Licence 2025/0003 permits Cayman Islands persons to continue business operations with a relevant subsidiary of a designated entity, to the extent they are in relation to specific named projects. This General Licence was issued on December 4, 2025 and expires on March 14 2027.

5. General Licence – Shah Deniz Project Activities (Issued). General Licence 2025/0004 allows persons and relevant Cayman Islands institutions to undertake any activity necessary for the continued operation of the Shah Deniz Project, subject to strict conditions. This General Licence was issued on December 4, 2025 and has no expiration date.

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 2025, the FRA had sixteen (16) staff members: a Director, Sanctions Coordinator, Senior Accountant, Senior Policy Analyst, three Senior Financial Analysts, 8 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. ECOFEL Course on Corporate Vehicles and Financial Instruments for the Americas Regional Group FIUs – a staff member attended the in-person training in Lima, Peru in March 2025.

2. Terrorist Financing / Proliferation Financing Training – 13 staff members attended the in-person training in Grand Cayman in March 2025.
3. Egmont Group VASP Risk Based Supervision Training Symposium – a staff member attended the in-person training in Malta in April 2025.
4. OFSI facilitated Terrorism Financing (TF) and Proliferation Financing training (10 staff attended)
5. CFATF Revised FATF Standards and Methodology - 4 staff members attended the in-person training in Grand Cayman in October 2025.
6. Counter Terrorist Finance Forum - a staff member attended an in-person 'Train the Trainer' event in Grand Cayman in November 2025. The event was attended by senior officials from the United Kingdom and British Overseas Territories.
7. ACAMS: The Assembly Caribbean – 2 staff members virtually attended the training in December 2025.
8. Staff completed a number of online training provided by ECOFEL, the UK Office of Financial Sanctions Implementation (OFSI), Canada's Financial Transactions and Reports Analysis Centre and other training providers on a variety of topics, including:
    a. Corporate Vehicles and Financial Products
    b. Introduction to Virtual Assets / Virtual Asset Analysis
    c. OFSI Intelligence Tools Workshop
    d. Project Anton: Insights, case studies, and strategies to combat the illegal wildlife trade and its illicit financial networks.
    e. FIU Communications & Planning
    f. Countering Terrorist Financing
    g. Professional Money Laundering
    h. CTS Guide to Transport Sanctions Investigations Presentation
    i. OTSI and Kharon Webinar: Understanding UK Sanctions and Trade Enforcement

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:

- Three (3) presentations at domestic industry association events.
- Eight (8) presentations at private sector organised events to private entities.
- Three (3) 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.

During the first half of the Reporting Period, the Director spent significant time representing the FRA (and the Caribbean Region) as a Regional Representative (RR) for the Americas Region of the Egmont Group. The Director participated in an Egmont Plenary, Working Group Meetings, Regional Group meetings and

Egmont Committee Meetings. The Regional Representatives liaise between the members in their region and the Egmont Committee and the Egmont Group, and act as advocates for their region. This includes acting as the main contacts for the HoFIU and Egmont Committee on regional issues, mediation of members' issues in the region, and for facilitating training and technical assistance.

The Director also represented the Egmont Group at in person (June in Brasilia) and virtual meetings of the G20 Anti-Corruption Working Group, including a presentation on the work of the Egmont Group.

The Director's term as a RR ended in July 2025. The Director was appointed as a Vice-Chair of the Technical Assistance and Training Working Group (TATWG) in July 2025.

An FRA staff member served as a Regional Support Officer for the Americas Region in relation to the Egmont Secure Web (ESW). Until 31 March 2025.

The Director and 2 members of staff attended Working and Regional Group meetings which were conducted virtually in January 2025. The meetings were attended by 800 delegates representing 145 FIUs, 7 candidate FIUs and 29 observer organizations who gathered through 18 different virtual meetings. Among the Highlights of the meetings were: Identifying new risks, trends, and methods; Policy enhancement to better serve the organization and its members; and Compliance to enforce the resilience of the global network.

The Director virtually attended an EC intersessional meeting held in Baku, Azerbaijan on 17th and 18th May 2025. 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 2025 Working and Regional Group Meetings and in preparation for the 31st Plenary in Luxembourg.

The Director also attended the 31st annual EG Plenary meetings from 6th to 11th July 2025, in Luxembourg. The Plenary was attended by approximately 600 delegates and 18 observer organisations. The 31st Plenary's thematic discussion were organized into three key Plenary sessions: FIU Autonomy and Operational Independence; Resourcing the fight against illicit finance; and Future Egmont Secure Web.

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 did not sign any MOUs. 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 2025: 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 60th CFATF Plenary and Working Group Meetings were held in Port-of-Spain, Trinidad and Tobago from 25th to 30th May 2025. 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 Curacao and Sint Maarten were adopted at the 60th Plenary.

The 61st CFATF Plenary and Working Group Meetings were held in Bridgetown, Barbados from 24th to 28th November 2025. 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. As the 4th Round of assessments was complete, no Mutual Evaluation Reports were adopted at the 61st Plenary.

Staff of the FRA continued to 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, proliferation of weapons of mass destruction and proliferation financing 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 1,377 SARs from 337 different reporting entities, up from the 1,194 SARs from 291 different reporting entities in 2024. This number excludes the 45 overseas FIUs that requested information from the FRA, or voluntarily disclosed information to the FRA. SARs received from the 337 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 Providers	509
Banking	262
Investment Funds and Fund Administrators	246
Fiduciary Services	165
Securities Investment Businesses	28
Money Services Businesses	14
Insurance Services	13
DNFBPs	90
LEAs & Competent Authority	12
Others	38
Requests for Information – Domestic	49
Requests for Information / Spontaneous Disclosures – Overseas	106
Total No of Cases	1,532

The Defence Against Money Laundering (DAML) / Consent Regime that came into force on 2nd January 2025. In addition to filing a suspicious activity report (SAR), the amendments to sections 133, 134 and 135 of POCA now require SAR filers to have the consent of the FRA to 'commit the act'. It remains that a defence against a money laundering offence does not apply to the person who committed or was a party to the act from

which the property derives.

A total of 517 requests for consent to proceed with a transaction or a defence against money laundering were received during the year. These requests comprised:

• DAML SAR – a request for consent submitted as part of a suspicious activity report;

• Supplemental DAML Request – an additional request supplementing an initial consent request; and

• DAML Request ND – a request for consent relating to a previously filed non-DAML suspicious activity report.

The details of those requests including the FRA's response are detailed in the table below.

The Reclassified category means that after further discussion with the SAR filer, it was agreed that a DAML / Consent request was not required and the FRA without granting or refusing a consent communicated that decision to the reporting entity.

Request Type	Granted	Deemed	Refused	Reclassified	Total
DAML SAR	347	64	7	16	434
Supplemental DAML Request	32	8	1	-	41
DAML Request – ND	16	23	1	2	42
	395	95	9	18	517
Case Maker Category					
VASP	194	33	3	3	233
Investment Funds & Fund Administrators	84	35	1	4	124
Banks	56	9	5	8	78
Fiduciary Services	16	8	-	1	25
DNFBPs	15	4	-	1	20
Insurance Services	12	3	-	-	15
Securities Investment Business	7	2	-	1	10
Others	11	1	-	-	12
Grand Total	395	95	9	18	517

Chart 3.1 on the succeeding page shows the total number of reports by financial year since 2018. The FRA received 1,532 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 2025 was 128, compared to 116 in 2024.

A total of 2,587 subjects were identified in cases (see Chart 3.3 on page 22), comprising 1,809 natural persons and 778 legal entities. 131 natural persons and 62 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 431, comprising 300 natural persons (including 16 anonymous subjects) and 131 legal entities.

The number of subjects whose nationality or country of incorporation is not identified declined from 431 to 317 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 113.

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.

Backlog Cases

During the Reporting Period the FRA undertook a specific ‘Backlog Project’, resulting in 387 ‘backlog cases’ being closed as No Further Action. These were cases received prior to 1 January 2022, were identified as receiving a lower assigned priority (priority 3 & 4) and no subsequent SARs were received on or after 1 January 2022. These cases and subjects remain in the FRA’s SARs database and will be re-evaluated should the FRA receive additional information. The cases can also be used for future strategic analysis.

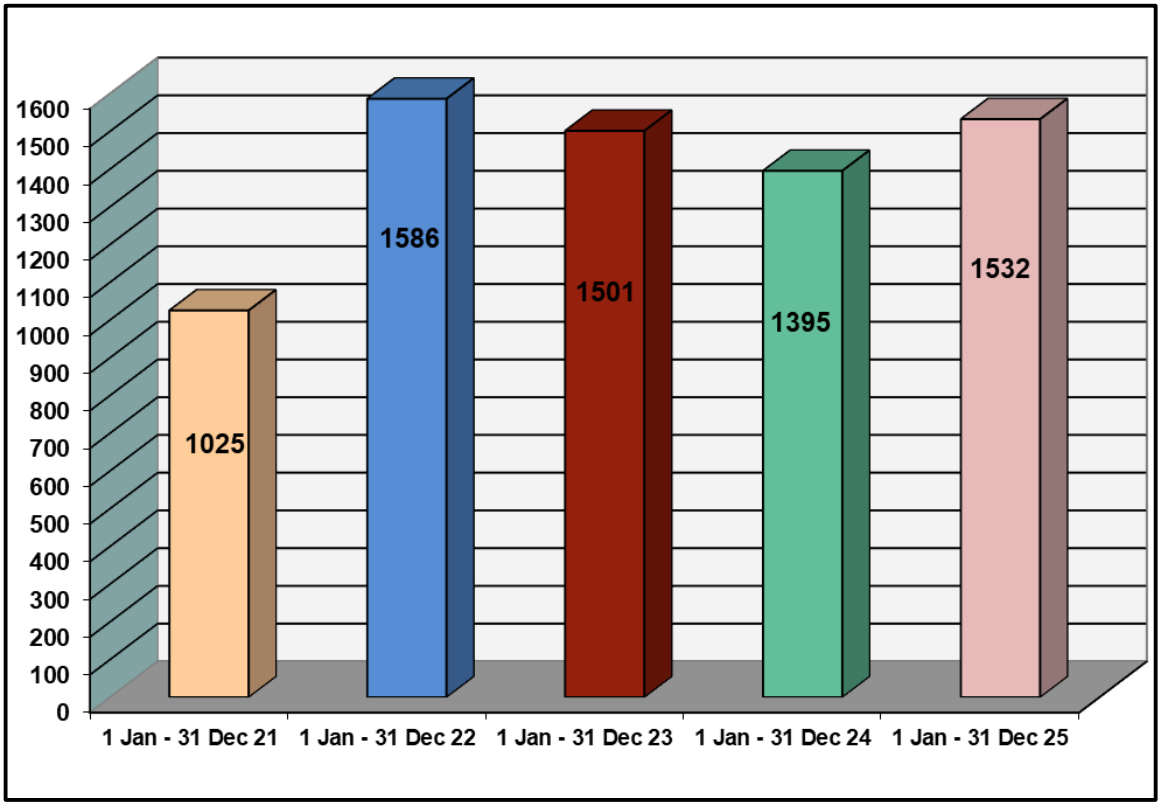


Chart 3.1: Total cases by financial year / Reporting Period

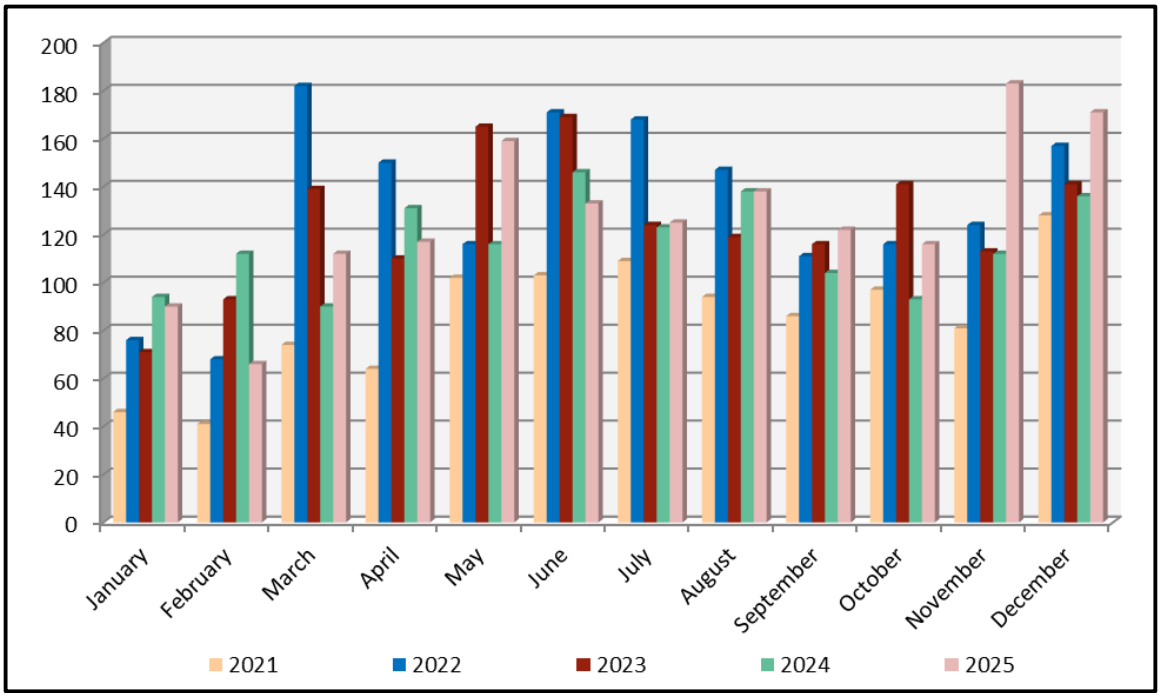


Chart 3.2: Comparison of monthly cases received

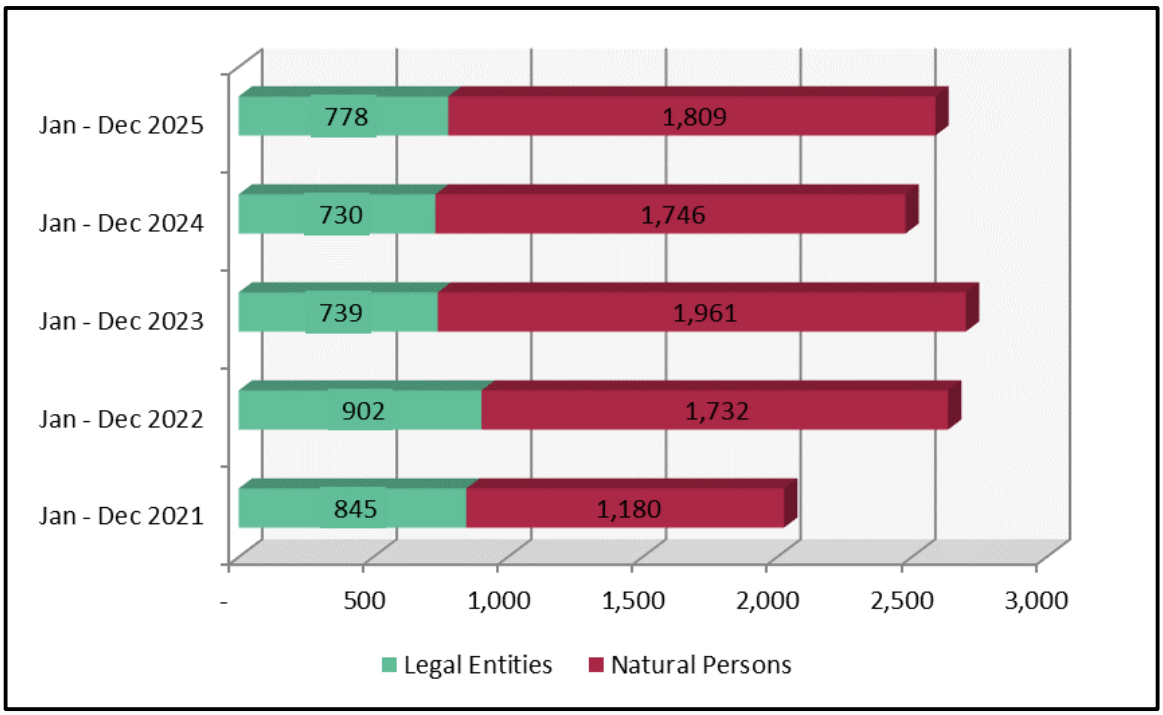


Chart 3.3: Number of subjects by financial year / Reporting Period

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 127 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 392; 75 were Caymanian nationals (natural persons) and 317 were legal entities established in the Cayman Islands. The United States was second largest with 163; 102 natural persons and 61 legal entities. The United Kingdom was the third largest with 126; 88 natural persons and 38 legal entities. Germany was the fourth largest with 121: 118 natural persons and 3 legal entities followed by: Canada with 58 - 47 natural persons and 11 legal entities; China (PROC) with 58 - 57 natural persons and 1 legal entity; Italy with 57 - 53 natural persons and 4 legal entities; Russia with 51 - 48 natural persons and 3 legal entities; Brazil with 49 - 43 natural persons and 6 legal entities; and Jamaica with 46 natural persons. Together these 10 countries account for 1,121 subjects, which represents 43% of the total.

The category "Others" in Chart 3.4 comprises the following countries with 10 or fewer subjects: Afghanistan, Albania, Andorra, Armenia, Azerbaijan, Bahrain, Barbados, Belarus, Belize,

Bermuda, Bolivia, Bulgaria, Cambodia, Cameroon, Cape Verde, Chile, Colombia, Cuba, Czech Republic, Democratic Republic of the Congo, Denmark, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Estonia, Gambia, Georgia, Gibraltar, Guatemala, Guernsey, Guyana, Honduras, Iran, Japan, Jersey, Jordan, Kenya, Kuwait, Kyrgyzstan, Lebanon, Libya, Liechtenstein, Lithuania, Luxembourg, Marshall Islands, Mauritius, Monaco, Mozambique, Namibia, Nepal, New Zealand, Nicaragua, Nigeria, Norway, Oman, Pakistan, Peru, Qatar, Saint Kitts and Nevis, Saint Lucia, Saudi Arabia, Senegal, Serbia, Seychelles, Slovakia, Slovenia, South Africa, Sri Lanka, Tajikistan, Trinidad and Tobago, Turkey, Uganda, Uruguay, Uzbekistan, Vanuatu, Venezuela, and Vietnam.

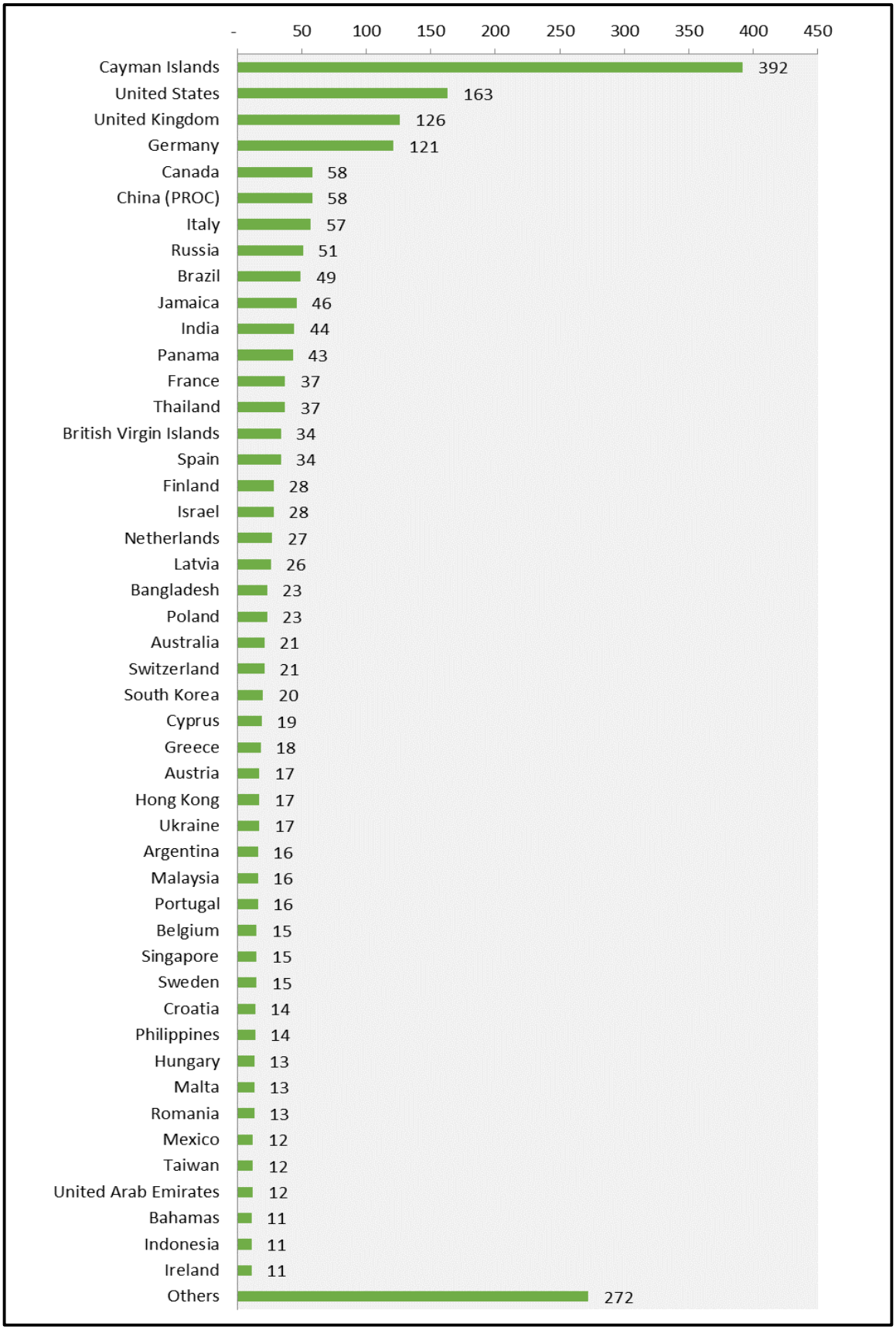


Chart 3.4: Countries of subjects in SARs reported in the Reporting Period

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 – 509
- Banks – 262
- Investment Funds – 160
- Company Managers / Corporate Service Providers – 110
- Overseas Financial Intelligence Units – 106
- Mutual Fund Administrators - 86
- Trust Companies – 55
- Lawyers – 40
- Securities Investment Businesses – 28
- Money Services Businesses – 14

Virtual Asset Service Providers ("VASPs"), Company Managers/Corporate Service Providers, Mutual Fund Administrators and Investment Funds each recorded more than a 30% increase from the 2024 SARs.

Virtual Asset Service Providers ("VASPs") were the largest source of SARs, with 509 cases filed by nine (9) VASPs. In 2024, ten (10) VASPs filed 374 cases.

Banks continue to be a major source of SARs, with 262 cases filed by 19 banks or banking type entities, comprising: 218 cases filed by 7 Class A banks, 43 cases filed by 11 Class B banks and 1 case filed by a Credit Union. This compares to 282 cases filed by 19 banks or banking type entities during 2024, comprising: 222 cases filed by 5 Class A banks and 60 cases filed by 14 Class B banks.

Investment Funds, comprising Mutual Funds and Private Funds, filed 160 cases, 40 more than the 120 cases received in 2024.

Company Managers / Corporate Service Providers and Trust Companies filed 165 SARs during the Reporting Period, compared to 125 in 2024.

Mutual Fund Administrators filed 86 cases during the Reporting Period, compared to 64 in 2024.

Securities Investment Businesses filed 28 SARs during the Reporting Period, compared to 29 in 2024.

MSBs filed 14 cases in 2025, compared to 31 in 2024.

Insurance Businesses filed 13 SARs during the Reporting Period, compared to 20 in 2024.

The largest number of SARs received from DNFBPs came from lawyers (40). Other DNFBPs filing SARs included: accounting professionals, real estate agents / brokers and dealers of precious metal and stones.

Receipt of Threshold Reports from Money Service Businesses and Banks

For the 12-month period ended 31 December 2025, the combined value of bank threshold transfers was approximately US$523.8 billion for outgoing transfers (47,954 transactions) and US$654.0 billion for incoming transfers

(47,468 transactions). 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).

The combined value of MSB threshold transactions for the Reporting Period was approximately US$32.2 million for outgoing remittances (24,863 transactions) and US$540.8 thousand for incoming remittances (345 transactions). The combined value of MSB threshold transactions for 2024 was approximately US$24.9 million for outgoing remittances (20,237 transactions) and US$612.8 thousand for incoming remittances (260 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 will also be used in future strategic analysis projects where relevant.

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

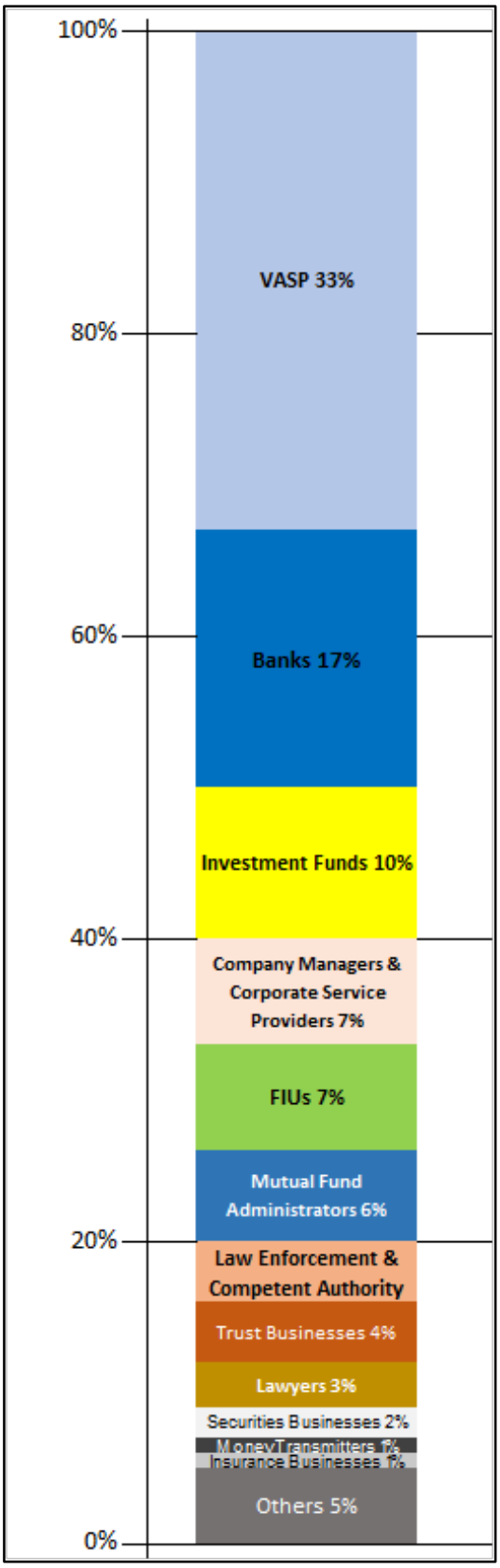


Chart 3.5: Sources of Cases

is the FRA's ability to request and exchange information with Egmont Group members.

Consistent with the provisions of the POCA, the FRA made 175 requests locally to clarify or amplify information received in 167 cases; 108 of these requests were to the SAR filer with the other 67 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.

Twenty-one (21) requests for information were made to fifteen (15) overseas FIUs in connection with nineteen (19) unique cases. All twenty-one (21) were to Egmont member FIUs via the Egmont Secure Web. Sixteen (16) of those requests were made on behalf of local law enforcement agencies or a Competent Authority. 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, proliferation financing 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: (i) any competent authority; (ii) any Supervisory Authority within the Islands, and (iii) such other institutions or persons in the Islands as may be designated in writing by the Steering Group,

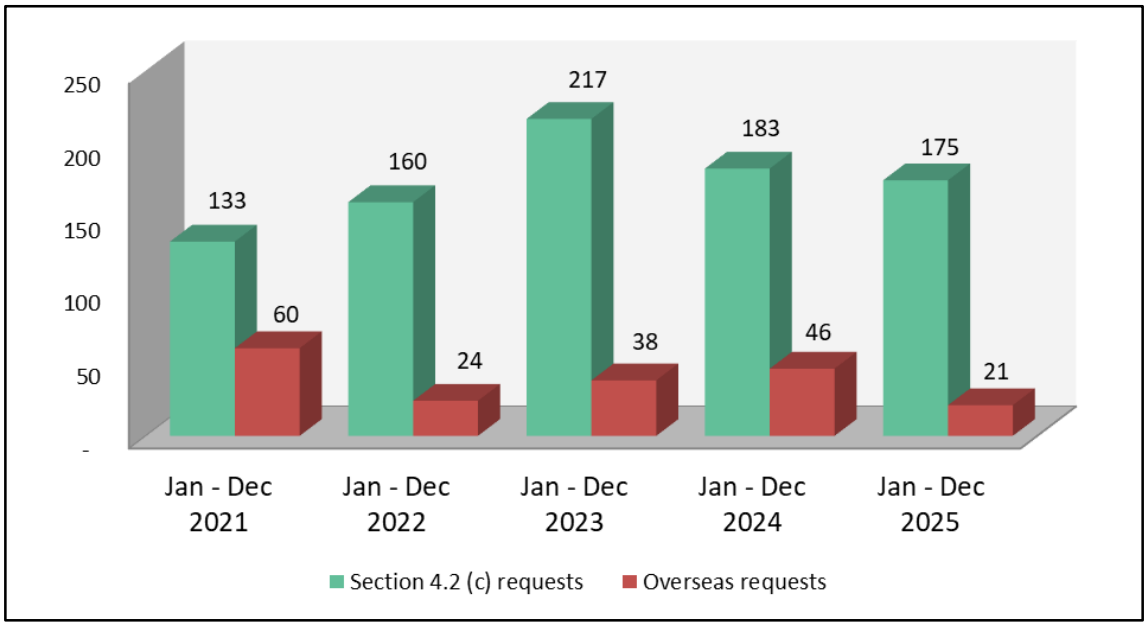


Chart 3.6: Number of requests made locally and overseas

SARs Trend Analysis

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

Reasons	%
Suspicious Activity	66%
Fraud	56%
Money Laundering	18%
Declined Business	8%
Corruption	7%

Sanctions	6%
Tax Evasion	4%
Regulatory Matters	4%
Theft	3%
Drug Offences	3%
Terrorism/Terrorist Financing	3%
Politically Exposed Persons	2%
Others	15%

Table 3.7: Reasons for suspicion

Since 2021 multiple reasons for suspicion for each case have been tracked. For the 1,532 cases received, 2,976 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) **548 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) **189 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) **114 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) **105 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) **27 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) **24 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 2025 859 total reasons for suspicions associated with fraud were recorded for 547 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 where 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 2025, US$1.8 million was lost to these schemes and the attempted misappropriation of a further US$1.3 million was prevented by mitigating procedures. 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.

• 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.

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/)

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 continue to observed 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 2025. A significant number of cases involved direct or indirect transactions with a wallet associated with a Darknet entity, in particular fraud shops. While less than those observed in prior years, the FRA continues to receive several requests from OFIUs regarding frauds in their jurisdictions that involved crypto transactions or a wallet with a Cayman nexus.

During the year the FRA noted an increase in SARs from VASPs involving "cash-back" or reward-farming behaviours that appear to have been exploited by their customers. These "wallet-specific behaviours" like chain peeling, repeating self-trades or circular transfers, using mixers or privacy tools raise suspicious patterns and are considered potential money-laundering indicators. VASPs often treat "cash-back" or reward-farming behaviours as abuse and often cease such relationships.

The FRA has also observed an increasing number of cases from VASPs involving "selfie mismatch". This occurs when the biometric data from a live photo (selfie) does not meet the confidence score required to match the applicant's provided government ID. This is a critical failure point during the Know Your Customer (KYC) process, as it prevents the VASP from confirming the applicant is the same person shown on the documents. These types of scenarios resulted in the VASP declining the

business.

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.

Similar to prior years, 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.

In 2025, in addition to the RFIs from LEAs, Competent Authorities or OFIUs, backlog cases were also excluded from identifying SAR triggers.

SAR Triggers	2025[3]	2024[4]
Adverse information – periodic review	46	126
Adverse information – ongoing monitoring	45	61
Adverse information – onboarding	39	53
Transaction monitoring – ongoing	153	335
Transaction monitoring – periodic review	10	27
Unusual service request made by client or customer	9	8
RFI by LEA or CA (Domestic)	15	21
RFI by LEA or CA (International)	109	62
Specific Business Events	265	166

[3] More than one trigger was identified for 17 cases in 2025

[4] More than one trigger was identified for 23 cases in 2024.

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 1,532 new cases. The FRA completed the review of 649 of these cases, leaving 883 in progress at 31 December 2025. Of the 649 new cases closed, 355 were filed as intelligence, 35 were deemed to require no further immediate action, 194 resulted in a disclosure, 45 were replies to requests from FIUs and 20 were replies to requests from local agencies.

The FRA also completed the review of 73 of the 620 carried over from 2024, 16 of the 467 carried over from 2023, 8 of 466 cases carried over from 2022, 67 of 423 cases carried over from 2021, 73 of 416 cases carried over from 2020, 124 of 621 cases carried over from 2019, 33 of 365 cases carried over from 2018, 37 of the 192 cases carried over from the interim period of 1-Jul-17 to 31-Dec-17, 55 of 228 cases carried over from 2016/17 and 9 of 63 cases carried over from 2015/2016, a total of 495 cases. Of the 495 previous cases that were completed, 19 were filed as intelligence, 401 were deemed to require no further immediate action, 63 resulted in a disclosure, 6 were replies to requests from LEAs and 6 were replies to requests from FIUs.

	Reporting Period									
Disposition	2025	2024	2023	2022	2021	2020	2019	2018	2017	2016-17
Royal Cayman Islands Police Service	189	40	11	8	-	-	-	1	-	-
Cayman Islands Monetary Authority	118	22	7	6	-	-	-	-	-	-
Other Local Law Enforcement Agencies	8	4	-	-	-	-	1	1	1	-
Other Competent Authorities	-	-	-	-	-	-	-	-	-	-
Overseas FIUs	182	36	10	8	-	-	-	1	-	-

Table 3.8: Number of SARs that contributed to disclosures made during 2025

	No. of Cases									
Disposition	2025	2024	2023	2022	2021	2020	2019	2018	1 Jul – 31 Dec 2017	2016-17
Cases Analysed Requiring No Further Action	35	30	45	29	101	321	334	244	258	187
Filed as intelligence	355	253	337	246	209	6	-	-	-	-
Cases Analysed that Resulted in a Disclosure	194	426	506	682	225	242	190	247	107	162
Reply to Domestic Requests	20	47	34	22	33	40	37	17	8	8
Reply to Overseas Requests	45[5]	92[6]	128[7]	149[8]	101[9]	69[10]	80[11]	95[12]	35[13]	71[14]
In Progress (as at 31 December 2025)	883	547	451	458	356	343	497	332	155	173
Total Cases	1,532	1,395	1,501	1,586	1,025	1,021	1,138	935	563	601

Table 3.9 Disposition of cases received as at 31 December 2025

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

Those 63 cases together with the 194 from 2025 comprise the 257 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 2025.

As at 31 December 2025, the FRA had commenced initial analysis on: 392 of the 883 pending 2025 cases; 307 of the 547 pending 2024 cases; 214 of the 451 pending 2023 cases; 168 of the 458 pending 2022 cases; 94 of the 356 pending 2021 cases; 143 of the 343 pending 2020 cases; 158 of the 497 pending 2019 cases; 102 of the 332 pending 2018 cases; 42 of 155 pending Jul – Dec 2017 cases; 46 of 173 pending 2016/2017 cases; 23 of 54 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 in the succeeding table.

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.

Recipient	2025	2024	2023
RCIPS	181[15]	244[16]	214[17]
CIMA	104[18]	150	105
ACC	2	12	3[19]
CBC	24[20]	35[21]	19[22]
CARA	-	-	1
DITC	-	-	2
DCI	-	7	5
GR	-	1	-
Overseas FIUs	254[23]	519[24]	491[25]
Total	565	968	842

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

- fraud – 49%
- money laundering – 21%
- Corruption – 6%
- Drug offences – 6%
- Sexual exploitation – 4%

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

- fraud – 50%

[15] Includes 8 responses to 8 requests
[16] Includes 22 responses to 19 requests
[17] Includes 13 responses to 13 requests
[18] Includes 1 response to 1 request
[19] Includes 1 response to 1 request
[20] Includes 17 responses to 17 requests
[21] Includes 21 responses to 21 requests
[22] Includes 9 responses to 9 requests
[23] Includes 58 responses to 54 RFIs from overseas FIU that disclose substantial information
[24] Includes 98 responses to 98 RFIs from overseas FIU that disclose substantial information
[25] Includes 140 responses to 145 RFIs from overseas FIU that disclose substantial information

- money laundering – 15%
- sanctions matters – 6%
- tax evasion – 6%
- international corruption – 5%

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 196 voluntary disclosures to overseas FIUs from 237 cases completed. Those 237 cases comprise: 182 cases from 2025, 36 cases from 2024, 10 cases from 2023, 8 cases from 2022, and 1 report from 2018.

In 2024 the FRA made 421 voluntary disclosures to overseas FIUs from 476 cases completed. Those 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.

The FRA also provided 58 responses to 54 requests for information from overseas FIUs. Those requests comprise: 48 requests from 2025 and 6 requests from 2024.

In 2024, the FRA also responded to 98 requests for information from overseas FIUs. Those requests comprise: 86 requests from 2024, 10 requests from 2023, and 2 requests from 2021.

Chart 3.10 on the next page details the jurisdictions that voluntary disclosures and responses were sent to in 2025; the 'Others' category comprises 34 jurisdictions that less than 3 voluntary disclosures or responses were sent to.

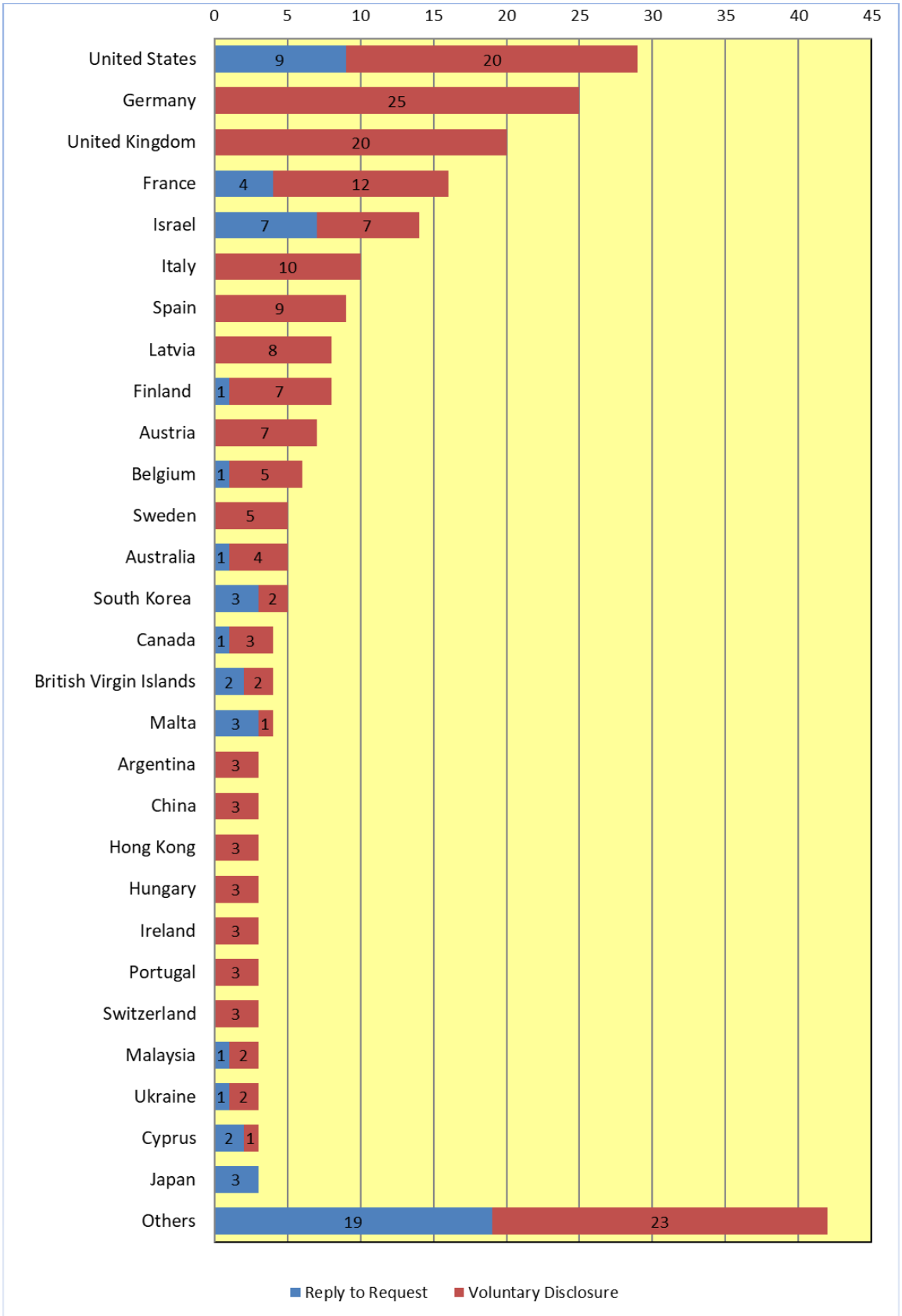


Chart 3.10: Overseas disclosures and replies to request for information

Significant Events

Analysis of Cases

The FRA had 4,046 cases to analyse during the Reporting Period, comprising: 1,532 new cases, 345 cases carried over from 2024, 223 cases carried over from 2023, 298 cases carried over from 2022, 321 cases carried over from 2021, 267 cases carried over from 2020, 435 cases carried over from 2019, 262 cases carried over from 2018, 147 cases carried over from Jul – Dec 2017, 178 cases carried over from 2016/2017 and 38 carried over from 2015/2016. There were also 1,385 cases that were initially analysed, but not completed as they required further analysis, comprising: 275 carried over from 2024, 244 carried over from 2023, 168 carried over from 2022, 102 carried over from 2021, 149 cases carried over from 2020, 186 cases carried over from 2019, 103 cases carried over from 2018, 45 cases carried over from Jul – Dec 2017, 50 cases carried over from 2016/2017, 25 cases carried over from 2015/2016, and 38 cases carried over from 2014/2015.

The FRA staff analysed 1,587 cases, during the Reporting Period, comprising: 1,044 cases from 2025, 106 cases from 2024, 7 cases from 2023, 8 cases from 2022, 59 cases from 2021, 87 cases from 2020, 132 cases from 2019, 40 cases from 2018, 40 case from Jul – Dec 2017, 55 cases from 2016/2017 and 9 cases from 2015/2016. An average of 132 cases were analysed per month in 2025 compared with 110 cases in 2024.

A total of 1,144 cases were closed during the Reporting Period, comprising: 649 cases received in 2025, 73 cases received in 2024, 16 cases received in 2023, 8 cases received in 2022, 67 cases received in 2021, 73 cases received in 2020, 124 cases received in 2019, 33 cases received in 2018, 37 cases received in Jul-Dec 2017, 55 cases received in 2016/2017 and 9 cases received in 2015/2016. On average, 95 cases were completed per month in 2025 compare with 92 cases in 2024.

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:

	2025	
Contents of the Disclosure	**CIBFI**	**CIMA**
Provided new information regarding known subjects	22	71
Provided you with unknown subjects	71	77
Corroborated information already known	7	70
Information disclosed to another agency	3	-
Triggered new investigation	1	-
Use of the Disclosure		
Actionable	11	12
Not Actionable	77	67
Total Feedback Forms provided	**88**	**79**

In 2024 feedback received were as follows:

Contents of the Disclosure	2024 CIBFI	2024 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 111 (2024: 104) 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 9 Specified Ship Sanctions Notices (a total of 438 ships specified) on its website. In 2024, the FRA published 7 Specified Ship Sanctions Notices (a total of 109 ships specified). 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. International Drug Trafficking and Money Laundering

The FRA received a SAR from a VASP in late 2024 reporting that it had received a request for information (RFI) from an overseas law enforcement agency (OLEA) in Country 1 regarding one of its clients, Subject A. The RFI detailed on ongoing money laundering investigation into Subject A for receiving the proceeds of narcotics trafficking. Subject A's account had not previously raised any suspicions.

Subject A declared their source of funds as coming from their construction business and early adoption of digital assets from crypto mining activity. Subject A had not made any fiat deposits into their account and had only transferred or deposited crypto assets into their account.

The VASP would have deemed the account beyond their risk appetite and terminated the client relationship; however, the OLEA requested that the VASP maintain the client relationship and monitor any substantial transactions. The FRA made disclosures to CIBFI, CIMA and the OFIU in Country 1.

Subject A subsequently requested substantial withdrawals in crypto and fiat currency; the withdrawals were unusual for Subject A's transaction history. With the DAML / Consent regime in force, the VASP submitted a supplemental SAR with a DAML / Consent request regarding the transactions.

The FRA made a DAML disclosure to RCIPS, seeking their views on whether to grant or refuse consent; RCIPS was minded to refuse consent and the FRA refused consent. CIBFI subsequently obtained a property freezing order against the assets held by Subject A at the VASP.

The FRA also made supplemental disclosures to CIMA and the OFIU in Country 1.

Indicators:

- Request for information from an overseas law enforcement agency – ongoing money laundering investigation linked to narcotics trafficking
- Unusual withdrawals compared against account history

2. **Fraud – False Representation / Crypto Fraud**

The FRA received a SAR from a Cayman Islands bank reporting that it had been served with a production order issued under mutual legal assistance legislation regarding an account maintained by Subject A, a citizen of Country 1 residing and working in the Cayman Islands on a work permit. The SAR included a DAML / Consent request to facilitate the exit of client relationships and the return of funds held in the clients' respective accounts.

Internal account reviews by the bank identified significant activity outside of Subject A's profile activity over a multi-year period, including substantial inbound transfers inconsistent with Subject A's declared employment and income. The funds were received primarily from overseas financial institutions and payment processors. The bank's review identified additional accounts not included in the production order, including accounts deemed to be held by related parties. One of the related party accounts reflected minimal legitimate income and was largely funded through transfers from Subject A, with expenditures focused on personal and luxury items.

Open source research by the bank identified potential links between Subject A and undisclosed business interests associated with entities referenced in adverse media related to large scale fraud and investment schemes.

The transaction activity and the existence of an active overseas investigation raised concerns that funds held in, or flowing through, the accounts may represent the proceeds of criminal conduct.

The information in the SAR identified that Subject A held accounts at banks in Countries 2 and 3. In conducting its analysis, the FRA identified related SARs that had been disclosed to CIBFI, CIMA, CBC and OFIUs in Countries 1, 2 and 3.

The FRA made a DAML disclosure to RCIPS, seeking their views on whether to grant or refuse consent; RCIPS was minded to refuse consent and the FRA refused consent.

The FRA also made disclosures to CIMA, CBC and OFIUs in Countries 1, 2 and 3 for intelligence purposes.

Indicators

- Subject of a mutual legal assistance treaty request
- Transaction activity inconsistent with declared income or employment profile
- Significant inflows from overseas institutions and payment processors
- Links to entities associated with adverse media and suspected fraudulent schemes

3. Fraud - Business Email Compromise

A Cayman Islands Bank filed a Suspicious Activity Report after their customer confirmed that a returned wire transfer was not authorised by them and advised that their account had been hacked.

The bank advised that they had received instructions to make two payments from the client's account; both transactions were below the bank's threshold required for online call back verifications. The first wire transfer was returned with reason "invalid creditor details"; upon receipt of the notification, the bank contacted the client and was advised the transaction was unauthorised. At the time of filing the SAR the second wire transfer had not been returned, as the ultimate beneficiary bank was awaiting approval of the account holder before returning the funds. The wire transfers were made to banks in Country 1.

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

Indicators

- Returned funds – in this case with reason "invalid creditor details"
- Confirmation from client that the transactions were unauthorised

4. Fraud – Romance Scam

The FRA received a SAR from a Cayman Islands bank reporting that they suspected that Client A was a victim of scam. Client A had contacted the bank about obtaining a credit facility to complete a transaction with an overseas credit union. During its review of the application the Bank noted the hallmarks of a Romance Fraud scheme involving multiple personas and cross-border transactions and advised Client A of their concerns.

The suspected fraud began when Client A was contacted by Subject 1, believed to be an online romantic partner whom Client A had never met in person. Subject 1 claimed to be the recipient of several million dollars in financial compensation and requested Client A's assistance in receiving the funds.

To facilitate this, Client A was introduced to Subject 2, purported to be an Account Officer at Credit Union X in Country 1. Subject 2 instructed Client A to open an account at Credit Union X and provide an initial minimum deposit of several thousand

dollars. Although the funds were supposedly a deposit to open an account at Credit Union X, Client A was directed to wire the money to a bank account at Bank Y in Country 1 held in the name of Company 3. Client A was further instructed to list the wire's purpose as a "family emergency" for Subject 1.

Following the initial payment, a third persona, Subject 4 (purportedly the General Manager of Credit Union X), provided a fabricated screenshot showing a balance of several million dollars. However, Client A was unable to access the funds and was told by Subject 4 that an "Authorisation Code" was required; an additional payment of several thousand dollars, described as a "standard fee" for international wires, was needed to release the "Authorisation Code".

FRA research found that Credit Union X was not a legitimate business and its related website was fake, and stock photos were used for the management team.

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

Indicators

- Conducting high-value transactions on behalf of a third party whom the victim has never met in person
- The purpose of the initial remittance was not in line with the stated reason and went to an unknown third party.
- The fraudsters requested a significantly larger second payment immediately after the first was successful.

5. 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 Country 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

6. "Cash-Back Farming" / Reward-Farming Behaviours

The FRA received a SAR from a VASP reporting that Subject 1 is suspected of engaging in a Cash-Back Farming scheme designed to exploit an online merchant's rewards program.

The VASP reported that over the course of a few months Subject 1 recorded a few thousand transactions, which was considered to be exceptionally high. The majority of these transactions were

directed towards purchase of specific items at an online merchant, indicating concentrated, high-frequency, circular transactions that lack legitimate economic purpose and appear intended solely to generate cash rebates / rewards.

The VASP's internal analysis concluded that the activity was inconsistent with Subject 1's profile established at onboarding. Additionally, Subject 1's country of residence is considered high risk for organised cyber fraud activity.

The VASPs noted that "cash-back" or reward-farming behaviours can be indicative of placement and layering. The VASP sought and was granted consent to exit the relationship.

While the SAR was filed as intelligence, it will be used in the future to develop strategic analysis on cyber enabled fraud.

Indicators:

- Disproportionate "Cash-Back Farming" / Reward Accumulation
- Minimal genuine Economic Activity
- High volume circular transactions
- Country of residence considered high risk for organised cyber fraud

7. VASP SARs triggered by direct requests from overseas LEAs

The FRA received numerous SARs from a VASP in relation to requests from overseas LEAs regarding criminal investigations being conducted in their jurisdictions. The most frequent underlying predicates cited in the requests made by the overseas LEAs included a variety of fraudulent activity and drug trafficking. In the majority of cases, the VASP's review did not identify any suspicious activity.

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

Indicators:

- Direct request from an overseas LEA

8. 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 2025 AND BUILDING ON STRENGTHS IN 2026

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 2025

During 2025 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 2025, the FRA:

   (i) Produced 565 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 88 Feedback forms from the RCIPs and 79 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 of receipt of a relevant SAR, compared to 51% in 2024. The average number of days to complete a request for information from an overseas FIU was 42 days in 2025, compared to 45 days in 2024.

   (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 2025 the majority of outreach and presentations focused on the DAML / Consent regime. The FRA issued an Industry Advisory in relation to POCA amendments that introduced a DAML / Consent regime. Staff of the FRA engaged in the following Outreach events covering one or more of the following topics: Overview of the DAML Regime, functions of the FRA, SAR statistics, SAR reporting obligations, and obligations regarding targeted financial sanctions related to terrorist financing and proliferation financing:

(i) Three (3) presentations at domestic industry association events.

(ii) Eight (8) presentations at private sector organised events to private entities.

(iii) Three (3) 1-on-1 meetings with Money Laundering Reporting Officers (MLROs).

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

During 2025 the FRA issued 10 feedback forms to 7 reporting entities from a cross-section of sectors, with the following quality ratings: (i) Very Poor: 1; (ii) Poor: 1 (iii) Fair: 4; and (iv) Good: 4.

The FRA utilised the features of its new website to publish one (1) Industry Advisory, one (1) fraud alert, and four (4) Public Notices related to targeted financial sanctions in 2025. These notices, advisory and alert allow individuals and businesses to comply targeted financial sanctions developments as well as take necessary precautions in preventing fraudulent transactions or prevent fraudulent transactions from progressing any further. The website was also used to publish 111 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 2025, the FRA:

(i) Operationalised a DAML / Consent regime in the Cayman Islands, a requirement under Recommendation 4 of the FATF Methodology.

(ii) Met deadlines for the Jurisdiction's Follow-Up reporting to the CFATF.

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

(iv) Continued to make meaningful contributions to the Egmont Group as detailed in this Annual Report.

(v) Actively participated in working groups for the National Risk Assessment by providing observations, statistical data and typologies from SARs.

4. High Performing Staff

This priority was largely achieved. Performance expectations for staff are clearly defined and documented. Staff completed analysis on 1,587 cases and closed 1,144 cases.

Staff made significant contributions to the ongoing National Risk Assessment.

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, TRM Labs, 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) In line with Government wide upgrade of Windows 11 Pro 22631 to Windows 11 24H2 versions of i2 iBase and i2 Analyst Notebook were upgraded in November 2025.

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

(iv) 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.

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

Strategic Priorities for 2026

Building on the 2025 priorities and integrating lessons from the latest NRA, FATF guidance, and emerging threats the FRA sets out to achieve the following strategic objectives for 2026:

1. **Delivering Timely, Actionable, and Risk-Focused Financial Intelligence**

   The FRA's core mandate remains the production and dissemination of high-quality financial intelligence that supports law enforcement, regulatory, and international partners in combating money laundering, terrorist financing, and proliferation financing. In 2025, the FRA received 1,532 cases, with virtual asset service providers (VASPs) and banks as the leading sources of suspicious activity reports (SARs). The evolving risk environment—characterized by the proliferation of virtual assets, complex sanctions evasion schemes, and the increasing use of artificial intelligence by both criminals and compliance teams—demands a more agile, risk-based, and technologically enabled approach to intelligence production.

   Key Actions:

   (i) Enhance risk-based prioritization of intelligence production by integrating findings from the 2025–2026 NRA, focusing on high-risk sectors and typologies.

   (ii) Introduce advanced analytics (including exploring artificial intelligence tools) to improve the detection of complex patterns, reduce false positives, and accelerate the triage and analysis of SARs and other disclosures. The FRA will leverage digital transformation best practices as outlined by the Cayman Islands Government, FATF and the Egmont Group.

   (iii) Expand typology analysis and strategic intelligence outputs by publishing periodic reports on emerging threats, sector-specific vulnerabilities, and case studies, including those related to proliferation financing, beneficial ownership misuse, and virtual asset risks.

   (iv) Strengthen the consent regime and SAR feedback mechanisms, ensuring timely responses to DAML / Consent requests and actionable feedback to reporting entities to improve SAR quality.

   (v) Improve and continue to monitor key performance indicators (KPIs) for intelligence production, including timeliness, usefulness, and impact metrics, to support continuous improvement and readiness for the 2027 CFATF mutual evaluation.

2. **Deepening Engagement and Partnership with Reporting Entities**

Effective AML/CFT/CPF systems depend on robust partnerships between the FRA and the private sector, including financial institutions, VASPs, and DNFBPs. The FRA will continue to foster a culture of open communication, feedback, and innovation with reporting entities to enhance the quality of SARs, support compliance, and promote the adoption of new technologies.

Key Actions:

(i) Expand outreach and training programs for reporting entities, with a focus on new and emerging risks (e.g., proliferation financing, virtual assets, and sanctions evasion) and on the effective use of reporting forms (SAR, Threshold, CRF).

(ii) Explore the establishment of public-private partnerships (PPPs) for intelligence sharing, typology development, and joint risk assessments, leveraging sectoral working groups and regular industry consultations.

(iii) Enhance the AMLive Reporting Portal and FRA website to streamline SAR submission, feedback, and communication, ensuring accessibility, security, and user-friendliness for all reporting entities.

(iv) Develop sector-specific guidance and feedback mechanisms for high-risk sectors, including tailored typology reports, case studies, and effective use of reporting forms.

3. **Strengthening International and Domestic Cooperation**

Meeting international standards and demonstrating effective cooperation are central to the FRA's mission and critical for the upcoming 2027 CFATF mutual evaluation. Recent FATF amendments have heightened expectations around beneficial ownership transparency, proliferation financing risk assessment, asset recovery, and the implementation of targeted financial sanctions. The Cayman Islands' role as a global financial hub, coupled with the increasing use of complex legal arrangements and cross-border structures, necessitates robust mechanisms for information sharing, joint investigations, and coordinated enforcement.

Key Actions:

(i) Actively engage and participate in the National Risk Assessment through membership in the different

working groups and providing observations, statistical data and typologies from SARs. Engage with other domestic agencies to integrate findings from the 2025–2026 NRA and ensure that financial intelligence supports law enforcement and regulatory partners in combating money laundering, terrorist financing, and proliferation financing.

(ii) Improve feedback mechanisms to and from users of financial intelligence produced by conducting regular meetings and regular assessments of the feedback provided.

(iii) Participate in joint outreach activities to demonstrate unified messaging and coordination.

(iv) Expand international cooperation and information sharing through active participation in the Egmont Group, CFATF, and other networks.

4. Fostering a High-Performing, Skilled, and Resilient FRA Workforce

The effectiveness of the FRA depends on the expertise, integrity, and resilience of its staff. The rapid evolution of financial crime, the adoption of new technologies, and the increasing complexity of regulatory and intelligence functions demand continuous investment in workforce development, training, and organizational resilience. The 2025–2026 NRA and the FRA's own performance reviews highlight the importance of specialized skills in data analytics, virtual assets, sanctions, and asset recovery, as well as the need for robust succession planning and staff well-being initiatives.

Key Actions:

(i) Develop and implement a comprehensive training and certification program for FRA staff, covering advanced analytics, virtual assets, proliferation financing, sanctions, and international cooperation, leveraging global best practices and partnerships (e.g., ECOFEL, Egmont Group).

(ii) Maintain a culture of excellence, integrity, and innovation by setting clear performance expectations, providing regular feedback, and recognizing outstanding contributions. Encourage cross-functional collaboration and knowledge sharing within the FRA and with external partners.

(iii) Invest in staff well-being, retention and succession planning.

(iv) Enhance organisational resilience and business continuity by developing and testing contingency plans, investing in secure and flexible IT infrastructure, and ensuring the FRA can operate effectively in the face of natural disasters, cyber threats, or other disruptions.

5. **Maximizing the Benefits of Technology, Data Analytics, and Secure Information Infrastructure**

Technology is both a driver of financial innovation and a vector for new risks. The FRA must continue to invest in secure, scalable, and innovative IT infrastructure to support intelligence production, information sharing, and operational resilience. The 2025–2026 NRA, FATF guidance, and recent legislative amendments all highlight the importance of digital transformation, cybersecurity, and data protection in the AML/CFT/CPF ecosystem.

Key Actions:

(i) Upgrade and integrate core IT systems (e.g., AMLive, i2 iBase, Analyst Notebook) to support advanced analytics, secure data storage, and efficient information sharing with domestic and international partners. Ensure systems are interoperable, scalable, and user-friendly.

(ii) Implement robust cybersecurity and data protection measures in line with the Data Protection Act (2021 Revision), FATF guidance, and international best practices. Regularly test and update security protocols to address emerging threats and vulnerabilities.

(iii) Leverage automation and initiate research into artificial intelligence and machine learning to assists in the processing and analysis of SARs, reduce manual workloads, and improve the quality and timeliness of intelligence outputs.

(iv) Leverage secure and efficient channels for information exchange with international counterparts by effective use of the Egmont Secure Web and with domestic law enforcement agencies by using Cayman Islands Government recognised networks, ensuring compliance with confidentiality, data protection, and legal requirements.

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