FINANCIAL REPORTING AUTHORITY

2023 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 2023 financial year ("the Reporting Period"), which marks the twenty first 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 1,501 cases during the Reporting Period, comprising 1,290 Suspicious Activity Reports ("SARs") from 292 Reporting Entities; 129 Requests for Information and 47 Voluntary Disclosures from 47 overseas Financial Intelligence Units ("OFIUs"); and 35 Requests for Information from Local Law Enforcement Agencies ("LEAs"). The number of cases received decreased by 5% compared to the number of cases received during 2022 (1,501 vs 1,586).

During 2023 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 393 registered users from 201 Reporting Entities; 954 SARs (63%) were filed using AMLive during 2023 and 542 SARs (36%) were filed using secure email.

During the Reporting Period the FRA performed initial analysis on 1,492 cases. It also issued 217 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 38 requests for information to OFIUs, 16 of which were made to assist LEASs with investigations.

The FRA closed 1,133 cases during the Reporting Period, resulting in 349 disclosures to LEAs or competent authorities, and 491 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 FRA exercised its powers under section 4(2)(b) of the POCA on two (2) occasions to obtain orders from the Court to order four (4) 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.

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 the Ukraine on 24 February 2022. Although workflows declined significantly compared to 2022, it was another challenging year for the FRA, 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; reviewing and commenting on changes to regulations and Orders in Council; and work in connections with the Russia Sanctions Taskforce. Apart from Russia Sanctions, the FRA also continued the actions taken to address recommended actions in the Caribbean Financial Action Task Force ("CFATF") 4th Round Mutual Evaluation Report ("MER") directly related to Targeted Financial Sanctions ("TFS") for terrorist financing ("TF") and proliferation financing ("PF").

In December 2023 the FRA launched a new website with a modern, clean and simplified format. The new website features easy to find information on key functions of the FRA as well as a dedicated page for Financial Sanctions. It showcases a suite of new features which include fraud alerts, a quick link to forms and documents and how to file a SAR.

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

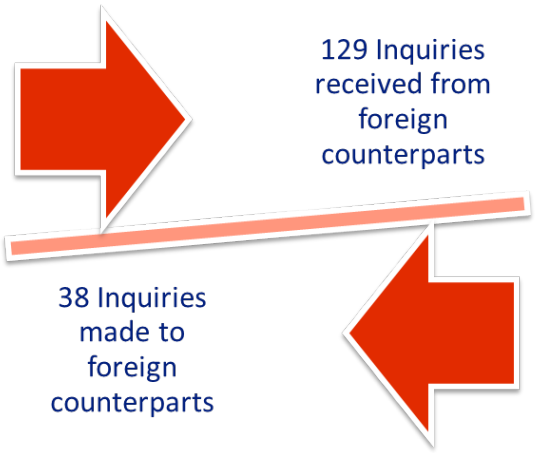
RJ Berry
Director

2023 HIGHLIGHTS

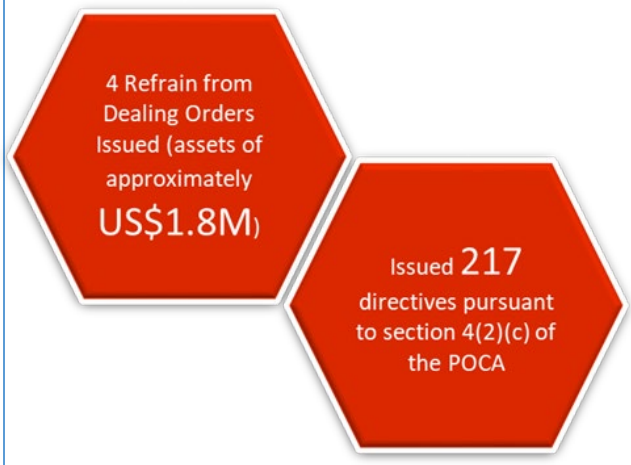
Cases Received and Analysed

Actions Taken & Financial Intelligence Disclosures

Global Contribution



Domestic Action



491 Disclosure to Overseas FIUs

Top 3 Recipients of Overseas Disclosures

FinCEN (US)	NCA (UK)	JAFIC (Japan)
78	44	37

349 Domestic Disclosures Made

Top 3 Recipients of Domestic Disclosures

RCIP-FCU/CIBFI	CIMA	CBC
214	105	19

Targeted Financial Sanctions

128 Financial Sanctions Notices Issued

I. LEGAL FRAMEWORK

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

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

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

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

The POCA also governs the operations of the FRA.

In late 2023, parliament passed the Proceeds of Crime (Amendment) Act, 2023. When this comes into force, it will introduce a 'consent regime' to the Cayman Islands and removes the automatic defence contained in sections 133-135 POCA. Work and discussion are currently underway to draft regulations and develop the infrastructure for receiving, processing and responding to consent requests.

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

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

obtained assets in relation to all qualifying criminal proceedings and investigations.

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

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

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

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

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

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

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

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

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

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

The AMLRs came into force in January 2023 and repealed and replaced the Money

Laundering Regulations (2020 Revision). They align the anti-money laundering framework in the Cayman Islands with the FATF Recommendations.

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

The 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 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 128 Financial Sanctions Notices on its website, a decrease from 193 in 2022. 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.

Russia Sanctions

The FRA continued to see a number of sanctions being imposed by the United Kingdom (and other countries) in 2023 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.

Since February 2022, there have been 22 amendments with 1 revocation (2023:5, 2022:17), covering various measures to the UK's Russia (Sanctions) (EU Exit) Regulations. Of these, 18 amendments (2023:4, 2022:14) have been extended to the Cayman Islands reflected in the 6 amendments (2023:2, 2022:4) to Russia (Sanctions) (Overseas Territories) Order.

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 2023, a total of 237 Compliance Reporting Forms (CRFs) were received by the FRA related to the Russia Sanctions regime. As of 31 December 2023 a total of approximately USD$ 8.32 billion and EUR€230 million held by or on behalf of persons designated under the Russia Sanctions regime were 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 2023, 13 (2022: 22) formal application 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 2023.

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 2023:

1. Originally issued on October 4 2022 and amended on April 5 2023 and on October 6 2023: General Licence GL/2022/0001 allows a Relevant Investment Fund or Fund Manager to redeem, withdraw or otherwise deal with an Investment Interest and make payments for basic needs, routine holding and maintenance and legal fees from frozen accounts. This is due to expire on October 6 2024.
2. Originally issued on December 15 2022 and amended on March 1 2023: General Licence GL/2022/0002 implements the Oil Price Cap which came into force on December 15 2022. This measure will deprive Russia of access to excess oil revenues by constraining its ability to sell at global market prices, while still enabling Russian oil to flow to the third countries that need it. This licence is of an indefinite duration.
3. General License GL/2023/0001 was issued on March 21 2023. General License GL/2023/0001 permits any activity (subject to the conditions) that may be undertaken by a Person necessary to terminate an arrangement between them and a Designated Person for that Person to provide Trust Services. This expired June 20 2023.
4. General licence GL/2023/0002 originally issued on April 14 2023 and replaced on November 15 2023 with GL/2023/0003: General License GL/2023/0003 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 May 15 2024.

These General Licenses 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 of the Financial Reporting Authority 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 2023, the FRA had sixteen (16) staff members: a Director, Legal Advisor, Sanctions Coordinator, Senior Accountant, 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. ACAMS Anti-Financial Crime/CFT Symposium – Grand Cayman 2023 (6 staff attended)
2. Overseas Territories Countering the Financing of Terrorism Forums (1 staff attended)
3. Online training provided by the Egmont Group / Egmont Centre for FIU Excellence and Leadership (ECOFEL) and other training providers on a variety of topics, including:
    a. Modern Slavery
    b. Corporate Vehicles and Financial Products
    c. Financial Instruments used in Money Laundering
    d. Virtual Asset Analysis
    e. Designated Non-Financial Businesses and Professions
    f. FIU – LEA Cooperation
    g. Financial Sanctions
    h. Cyber Security Awareness

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:

- Five (5) presentations at international and domestic industry association events, or other international events.
- Five (5) presentations at private sector organised events, to private entities or to public entities
- Two (2) 1-on-1 meetings with Money Laundering Reporting Officers (MLROs).
- Two (2) meetings 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 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 166 countries. 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 Egmont 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.

The Director attended the Egmont Group (EG) Working and Regional Group meetings in Dakar, Senegal from January 30 to February 2, 2023. The meetings were attended by 287 delegates representing Egmont members and 12 observers and international partners who gathered through 15 different meetings to enhance EG member capabilities, improve information sharing among them, and work toward accomplishing the EG'S development mission, cooperation, and sharing of expertise.

The Director also attended the 29th annual Egmont Group Plenary meetings from July 3-7, 2023, in Abu Dhabi, United Arab Emirates. The Plenary was attended by 533 delegates (including 12 observers and one international partner). The 29th Plenary's Thematic Discussion "Use of Advanced IT Technologies by FIUs to Enhance their Operations" focused on the opportunities and challenges that new technologies bring to the AML/CFT ecosystem in general, and to the daily operations of FIUs in particular. Among the topics explored were the use of privacy enhancing technologies, the use of block-chain technology, and the use of artificial intelligence to enhance FIU operations, creative models of collaboration, and strategic effectiveness.

At the 29th Plenary meetings the Director was elected to a two-year term as Regional Representative for the Americas Region of the Egmont Group. 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 contact for the HoFIU and Egmont Committee on regional issues, mediation of members' issues in the region, and for facilitating training and technical assistance.

A FRA staff member volunteered to be a Regional Support Officer for the Americas Region in relation to the Egmont Group's transition to the new Egmont Secure Web (ESW). This role involved assisting other FIUs to set up their Egmont user accounts, providing introduction and guidance on new ESW processes and functionalities, and serving as first level support on troubleshooting any IT issues encountered. The staff member continues to provide support as requested.

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.

The FRA did not enter into any new MOUs with

OFIUs during the Reporting Period; however, it is currently in discussion with four (4) OFIUs to sign an MOU. The FRA has signed and exchanged MOUs with the following 21 FIUs as of 31 December 2023: Australia, Canada, Chile, Guatemala, Guernsey, Honduras, Indonesia, Israel, Jamaica, Japan, Mauritius, Nigeria, Panama, Poland, Republic of Korea (South Korea), the Russian Federation, Saint Vincent and the Grenadines, South Africa, 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 fulfills 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 56th CFATF Plenary and Working Group Meetings were held in Port-of-Spain, Trinidad and Tobago from 28th May 2023 to 1st June, 2023. 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 the Commonwealth of Dominica was adopted at the 56th Plenary.

The 57th CFATF Plenary and Working Group Meetings were held in Aruba from November 29th to December 1st 2023. Three (3) staff attended various working group meetings, including the HoFIUs meeting, which is the focus for the FRA, as well as the Plenary sessions. The Mutual Evaluation Reports for the British Virgin Islands and St. Vincent and the Grenadines were adopted at the 57th Plenary.

The Director was the Chair of the CFATF Heads of FIUs Forum for the period November 2022 to November 2023. In addition to the two in-person meetings during the CFATF Plenary and Working Group meetings, the Director also introduced and chaired two virtual CFATF Heads of FIUs Forums during 2023.

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 Recommendations (2012) ("the Recommendations") have been revised to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

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. Therefore, the Methodology comprises 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 are reviewed and amended periodically. The Recommendations and Methodology were last updated in October 2023 and June 2023 respectively.

III. PERFORMANCE REPORTING

1. Receiving Information - Suspicious Activity Reports (SARs)

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

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

During the Reporting Period, the FRA received 1,290 SARs from 292 different reporting entities, down from the 1,365 SARs from 368 different reporting entities in 2022. This number excludes the 47 overseas FIUs that requested information from the FRA, or voluntarily disclosed information to the FRA. SARs received from the 292 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
Banking	392
Virtual Asset Service Provider	282
Investment funds and fund Administrators	206
Fiduciary services	141
Securities investment businesses	56
Insurance services	40
Money transmitters	31
DNFBPs	88
LEAs & Competent Authority	29
Others	25
Requests for Information – Domestic	35
Disclosures & Requests for Information – Overseas	176
Total No of Cases	1,501

Anyone who files a SAR currently has a defence to any potential related money laundering or terrorist financing offences. SARs filed under the POCA do not breach the Confidential Information Disclosure Act, 2016, nor do they give rise to any civil liability. An important exception to this rule is that it is no defence to such liability, if the person making the report is also the subject of the report.

Chart 3.1 on the succeeding page shows the total number of reports by financial year since 2018. The FRA received 1,501 new cases during the Reporting Period. Since fiscal year 2013/2014, the FRA has used its existing risk ranking for cases to determine which reports 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 2023 was 125, compared to 132 in 2022.

A total of 2,700 subjects were identified in cases (see Chart 3.3 on page 20), comprising 1,961 natural persons and 739 legal entities. 112 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 reports 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 381, comprising 294 natural persons (including 97 anonymous subjects) and 87 legal entities.

The number of subjects whose nationality or country of incorporation is not identified declines from 381 to 294 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 138.

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 20.

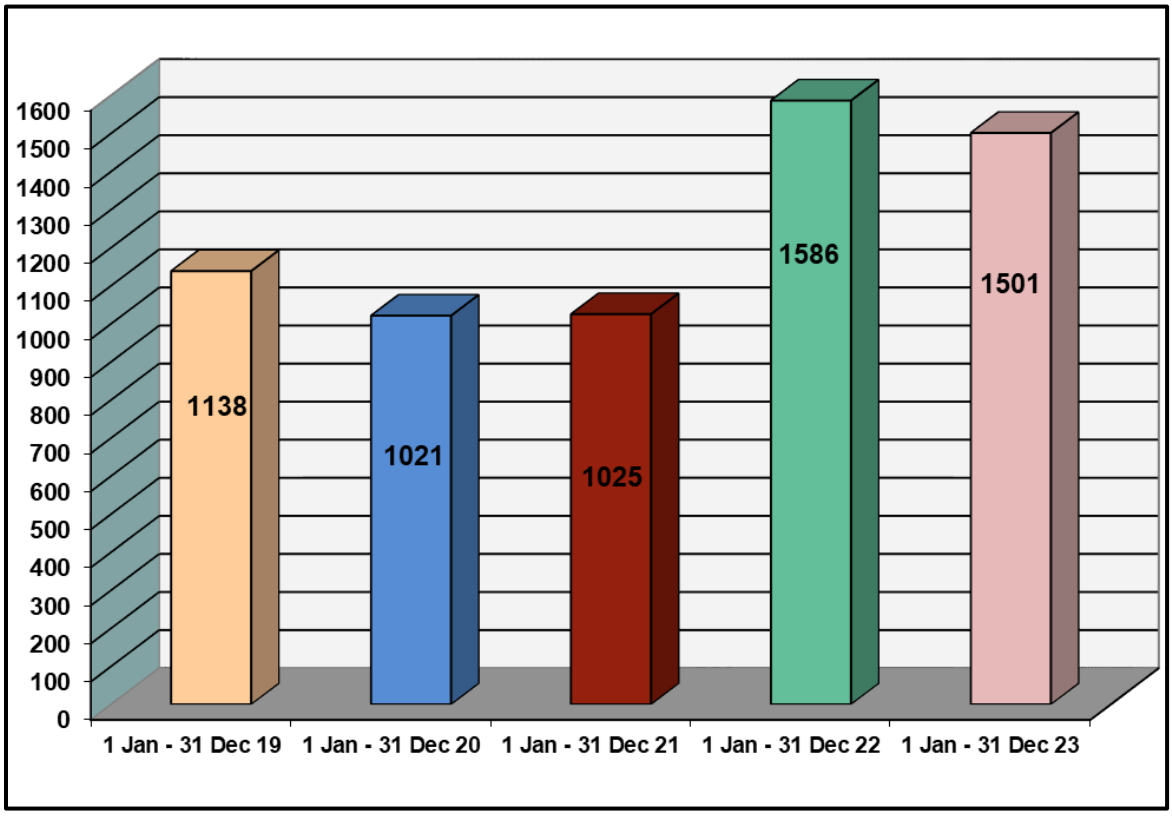


Chart 3.1: Total cases by financial year / Reporting Period

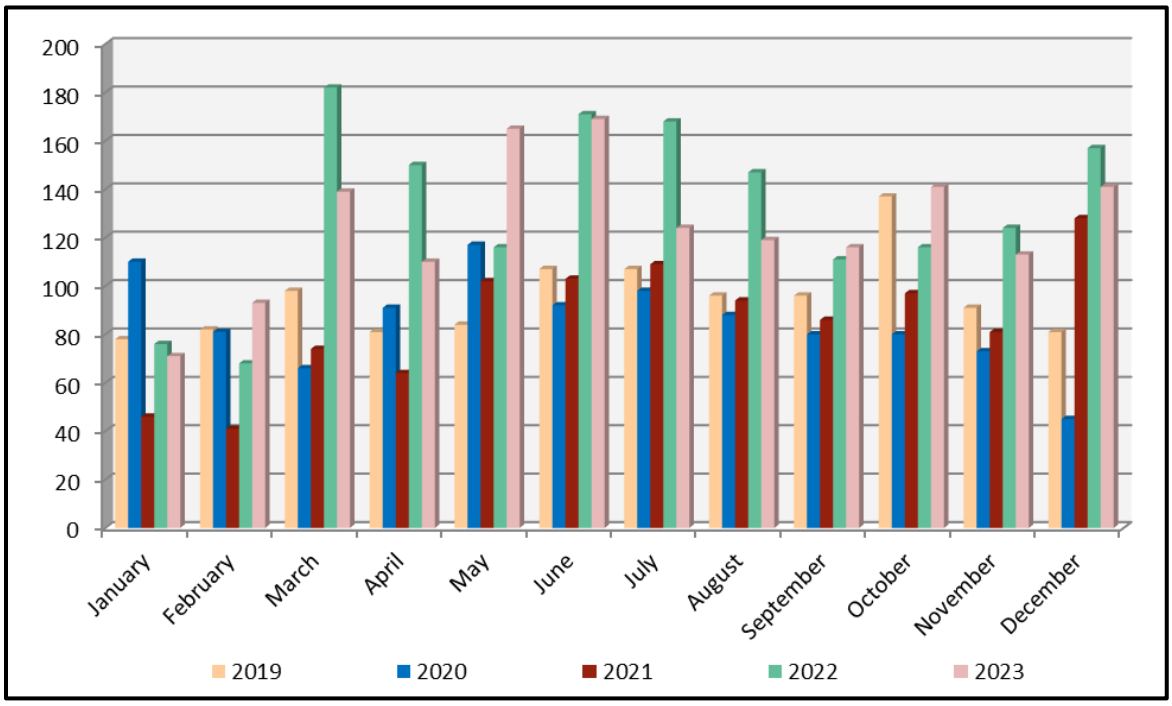


Chart 3.2: Comparison of monthly cases received

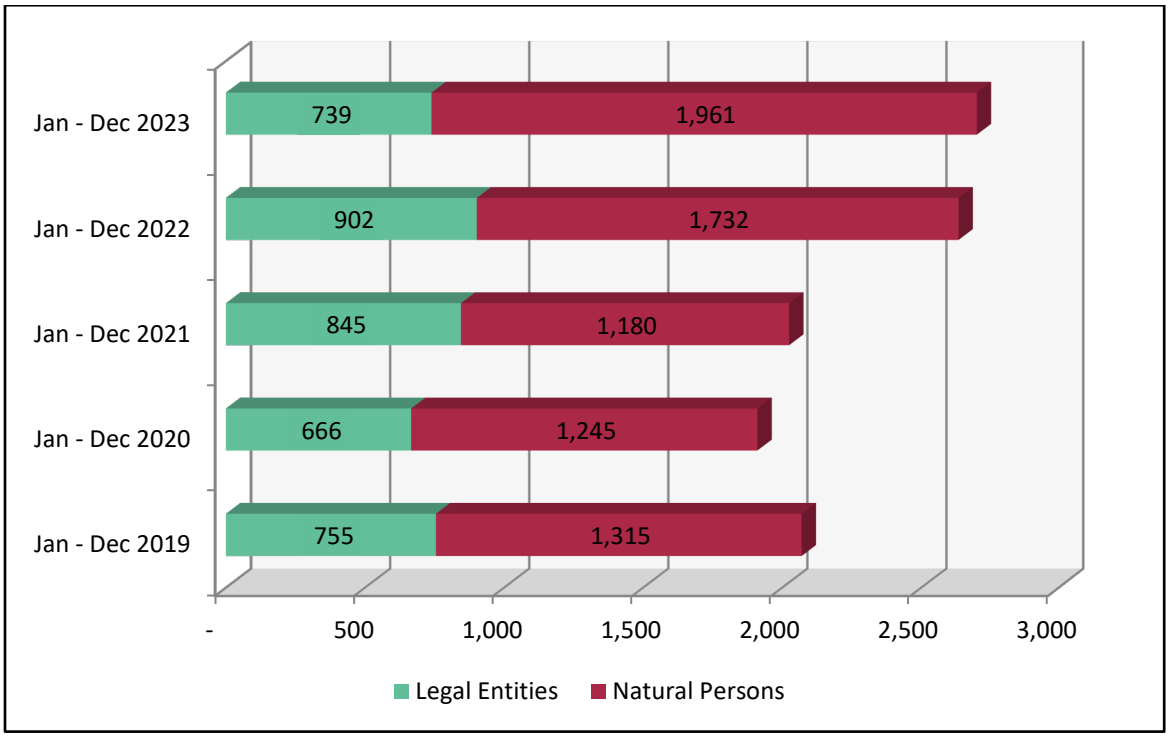


Chart 3.3: Number of subjects by financial year / Reporting Period

Countries of Subjects Reported

The international scope of the Cayman Islands' financial services industry is reflected in the wide range of subjects' countries reported in cases. The "Countries of Subjects" chart on the succeeding page lists 128 different countries for the subjects of the reports. 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 423; 88 were Caymanian nationals (natural persons) and 335 were legal entities established in the Cayman Islands. The United States was second largest with 163 natural persons and 49 legal entities. The United Kingdom was the third largest with 167 natural persons and 24 legal entities followed by: Italy comprising 154 natural persons and 2 legal entities; Germany comprising 127 natural persons and 4 legal entities; France comprising 101 natural persons and 5 legal entities; Russia with 65 natural persons and 1 legal entity; Canada with 56 natural persons and 4 legal entities; Brasil with 44 natural persons and 10 legal entities and the British Virgin Islands with 53 legal entities. Together these 10 countries account for 1,452 subjects, which represents 54% of the total.

The category "Others" in Chart 3.4 comprises the following countries with 6 or fewer subjects: Angola, Antigua and Barbuda, Argentina, Armenia, Australia, Azerbaijan, Bangladesh, Barbados, Belarus, Belize, Bermuda, Bosnia and

Herzegovina, Botswana, Bulgaria, Cambodia, Colombia, Croatia, Cuba, Curacao, Czech Republic, Dominican Republic, East Timor, Egypt, El Salvador, Equatorial Guinea, Estonia, Finland, Gabon, Gambia, Georgia, Ghana, Gibraltar, Greece, Grenada, Guernsey, Guyana, Haiti, Hungary, Iceland, Iraq, Isle of Man, Ivory Coast, Jordan, Kazakhstan, Kenya, Kuwait, Liechtenstein, Lithuania, Malaysia, Moldova, Morocco, Namibia, Nepal, New Zealand, North Macedonia, Norway, Oman, Palestine, Panama, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent & Grenadines, Saudi Arabia, Serbia, Slovakia, Slovenia, South Korea, Sri Lanka, Tanzania, Thailand, Turks & Caicos, United Arab Emirates, Uruguay, Uzbekistan and Zimbabwe.

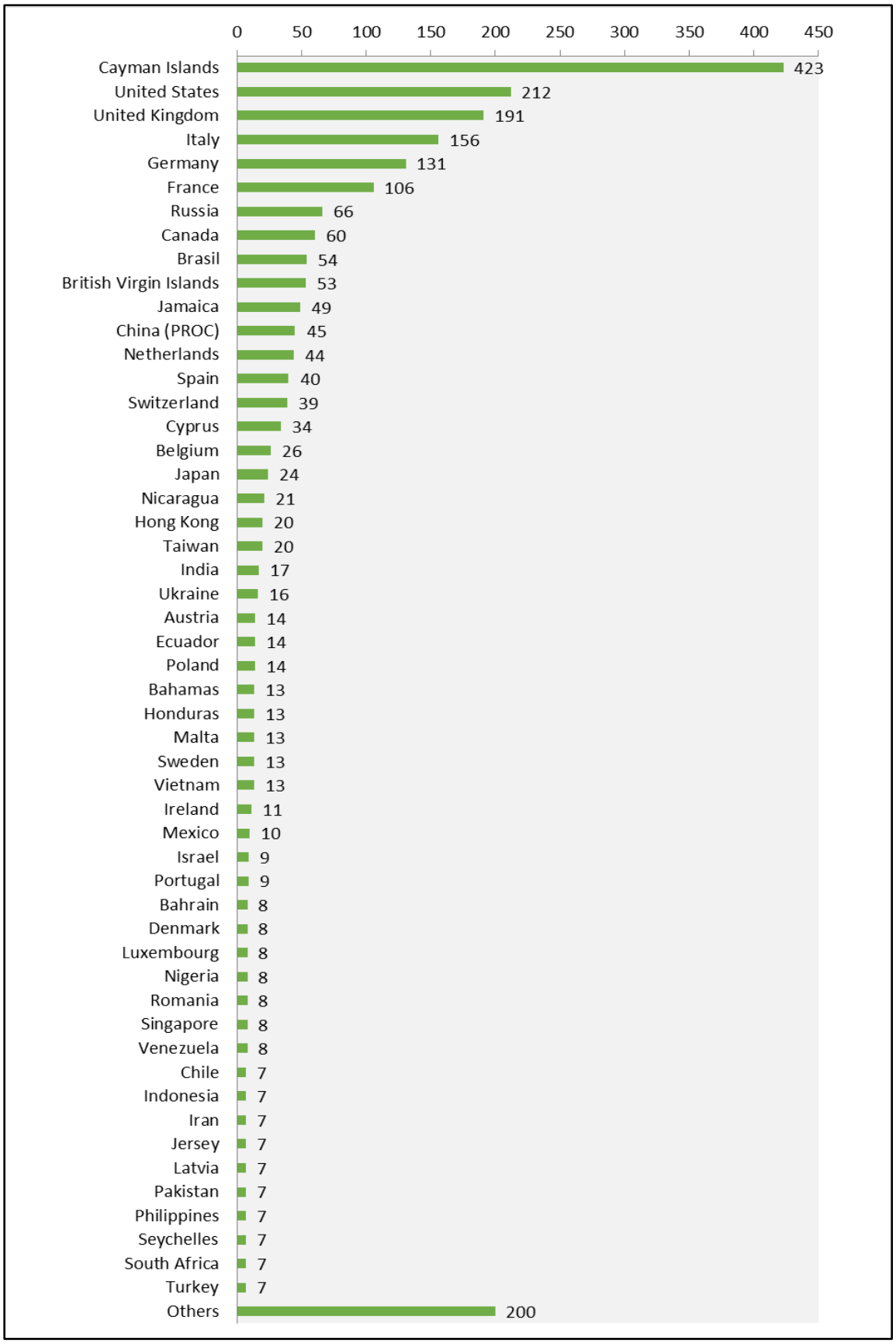


Chart 3.4: Countries of subjects in SARs reported in the Reporting Period

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:

- Banks – 392
- Virtual Asset Service Provider – 282
- Overseas Financial Intelligence Units – 176
- Investment Funds – 130
- Company Managers / Corporate Service Providers – 110
- Mutual Fund Administrators - 76
- Securities Licensees – 56
- Lawyers – 55
- Insurance Businesses – 40
- Trust Companies – 31
- Money Transmitters – 31

Banks regained their rank as the primary source of SARs, with 392 reports filed by 24 banks or banking type entities, comprising: 333 cases filed by 8 Class A banks; 52 cases filed by 15 Class B banks; and 7 cases filed by a Credit Union. This compares to 239 reports filed by 27 banks or banking type entities during 2022, comprising: 178 cases filed by 6 Class A banks; 58 cases filed by 18 Class B banks; and 3 cases filed by a Credit Union. MSBs filed 31 reports in 2023 compared with 6 reports filed in 2022.

Almost all other sectors registered a decline in SARs filed. This decline might be partially attributable to the decrease in the number of new sanctioned individuals under the Russia Sanctions Regime. In 2023 8% of SARs filed listed 'Sanctions' as a reason for suspicion, compared to 17% in 2022.

Virtual Asset Service Providers continue to be a major source of SARs, with 282 reports filed by six (6) VASPs. In 2022, four (4) VASPs filed 374 reports.

Investments Funds, comprising Mutual Funds and Private Funds, filed 130 reports, 32% less than the 190 reports received in 2022.

Company Managers / Corporate Service providers and Trust Companies continue to be a significant source of SARs with a combined 141 SARs filed during the Reporting Period, compared to 221 in 2022.

Mutual Fund Administrators filed 76 reports during the Reporting Period, a 33% decrease compared to 113 in 2022.

Securities Licensees was the only other sector that registered an increase with 56 SARs during the Reporting Period, compared to 45 in 2022.

Insurance Businesses filed 40 SARs during the Reporting Period, compared to the 51 in 2022

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

Receipt of Threshold Reports from Money Service Businesses and Banks

On 1 March 2022, the Anti-Money Laundering (Class A and Class B Bank Threshold Reporting) Regulations, 2022 were approved by Cabinet. The Regulations required that a monthly report of threshold transactions carried out by a bank or a nil report in case a bank does not carry out a threshold transfer within the reporting period be submitted to the Financial Reporting Authority.

For the 12 month period ended 31 December 2023, the combined value of bank threshold transfers was approximately US$767 billion for outgoing transfers (97,053 transactions) and US$329 billion for incoming transfers (13,463 transactions). For the 10 month period ended 31 December 2022, the combined value of bank threshold transfers was approximately US$2.35 trillion for outgoing transfers (71,377 transactions) and US$1.11 trillion for incoming transfers (30,301 transactions)

The combined value of MSB threshold transactions for the Reporting Period was approximately US$25.7 million for outgoing remittances (21,974 transactions) and US$674 thousand for incoming remittances (350 transactions). The combined value of MSB threshold transactions for the Reporting Period was approximately US$24.9 million for outgoing remittances (20,531 transactions) and US$448,000 for incoming remittances (189 transactions).

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

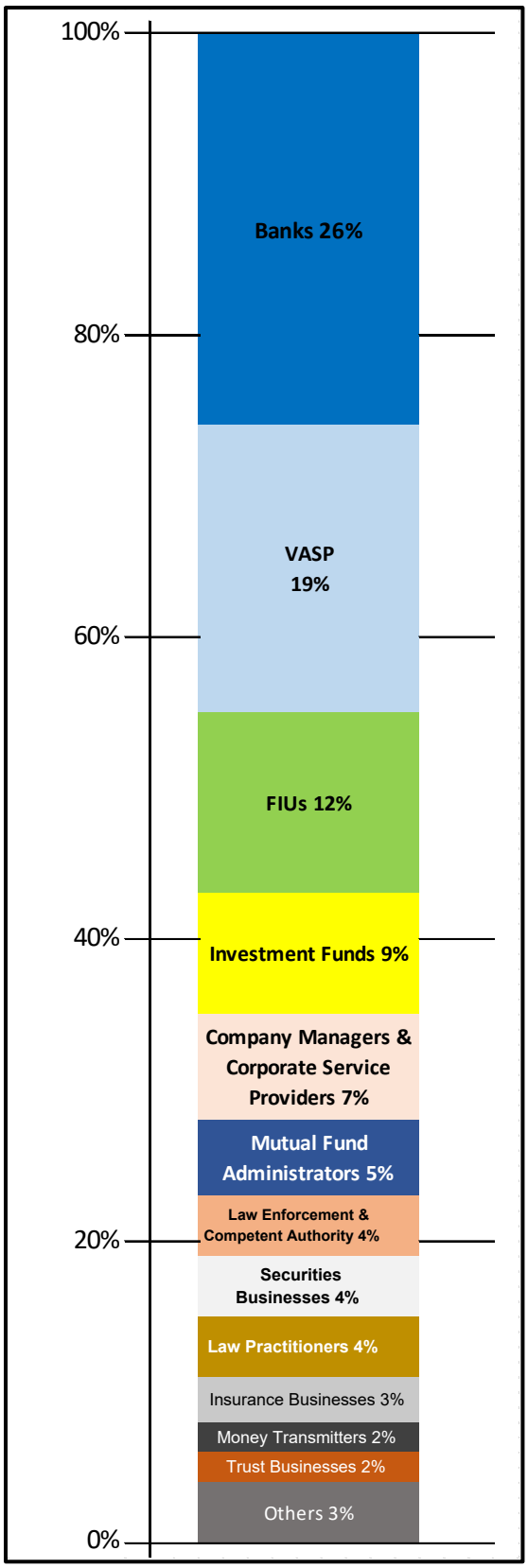


Chart 3.5: Sources of Cases

2. Analysing Information

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

Consistent with the provisions of the POCA, the FRA made 217 requests locally to clarify or amplify information received in 187 cases; 96 of these requests were to the SAR filer with the other 121 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.

Thirty eight (38) requests for information were made to twenty four (24) overseas FIUs in connection with twenty five (25) unique cases. All thirty eight (38) requests were to Egmont member FIUs via the Egmont Secure Web. Sixteen (16) of those requests were made on behalf of local law enforcement agencies. These requests greatly assisted the FRA in

determining whether to make disclosures to local law enforcement, as well as to overseas FIUs, or to assist local law enforcement with their investigations. Chart 3.6 below shows the number of requests made locally and overseas by financial year since 2020.

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

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

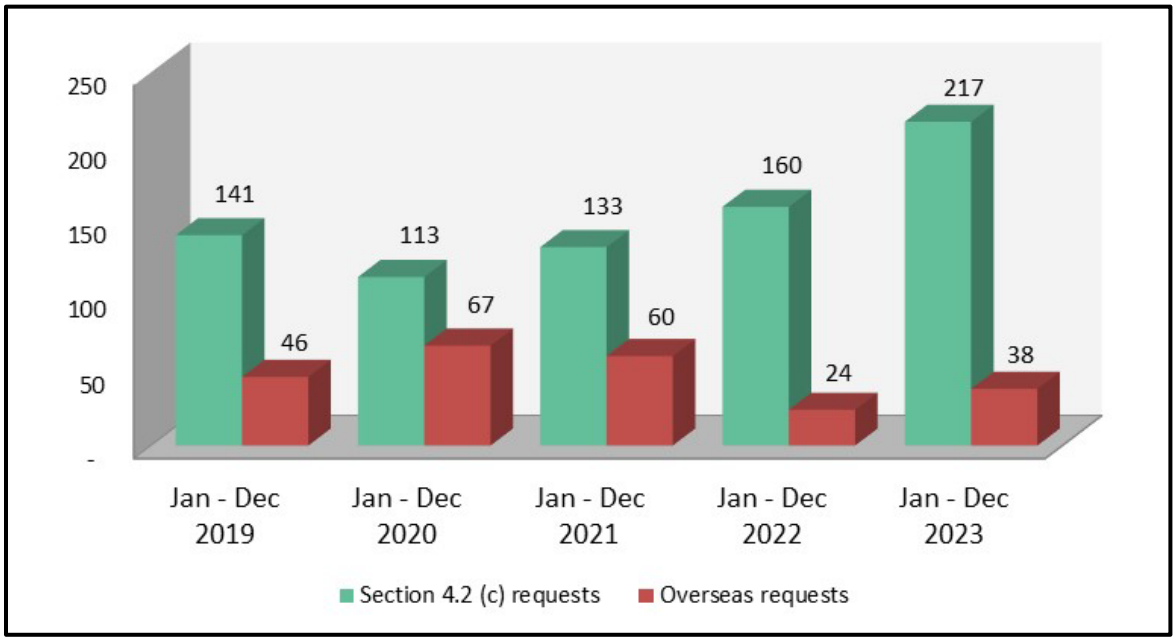


Chart 3.6: Number of requests made locally and overseas

SARs Trend Analysis

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

Reasons	%
Suspicious Activity	1,005
Fraud	720
Money Laundering	235
Sanctions	121
Declined Business	81
Tax Evasion	78
Corruption	76
Theft	52
Politically Exposed Persons	44
Regulatory Matters	44
Drug Trafficking	29
Unlicensed Regulated Activity	15
Others	168

Table 3.7: Reasons for suspicion

Since 2021 multiple reasons for suspicion for each case have been tracked. For the 1,501 cases received, 2,668 reasons for suspicion were recorded

Suspicious Financial Activity

A large number of reports 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 reports by the most recognizable of the activities as follows:

a) **522 reports 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 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) **201 reports regarding inadequate and / or inconsistent information:** Reports 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) **119 reports about activities that appear to lack economic purpose**: Reports about activities that appear to lack economic purpose include reports from VASPs about customer transactions that appear to just pass though digital wallets (top-up, conversion followed by withdrawal); reports from banks about customer transactions that appear to just pass though accounts.

d) **107 reports about transactions inconsistent with client profile:** Reports 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) **31 reports 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) **25 reports regarding high volume transactions:** Reports about high number of transactions occurring, including those involving cash, consist of reports about subjects making multiple cash transactions (i.e., deposits, withdrawals or remittances); as well as transactions in virtual assets/digital wallets that have a noticeable 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 2023 720 total reasons for suspicions associated with fraud were recorded for 397 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.

There were a handful of cases where foreign individuals attempted to deposit a fake cheque purported to be issued by a Cayman bank at a foreign institution. None of these transactions were successful.

There were also a small number of cases reported where a foreign-service provider, typically an investment manager, issued false or misleading information to investors.

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 a handful of cases the misappropriation was from a Cayman fund.

The same was true for Ponzi/Pyramid schemes. In one case the investment manager for a Cayman fund allegedly misled the funds' investors, auditors, and administrator about the funds' trading practices, risk, and performance.

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 reports 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. A smaller portion of reports are about actual transactions that give rise to suspicion of trading on insider information or schemes that manipulate stock values.

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 reports 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 2023, US$3.3 million was lost to these schemes and the attempted misappropriation of a further US$2.8 million was prevented by mitigating procedures. In 2022, US$472 thousand was lost to these schemes and the attempted misappropriation of a further US$2.1 million was prevented by mitigating procedures.

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

have noted are communications purporting to come from local banks.

• 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.

Though not directly affecting Cayman Islands companies, the FRA received reports about Ransomware, a type of malicious software, or malware that prevents users from accessing their computer files, systems, or networks and demands a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data. We have received reports that a Cayman Islands fund had invested in companies that have experienced ransomware attacks.

Credit Card / Debit Card schemes

This year the FRA noted an increase in 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. In other cases, perpetrators use 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 2023. A significant number of cases involved direct or indirect transactions with a wallet associated with a Darknet entity, in particular fraud shops. Continuing the trend from 2022, a significant number of requests from OFIUs regarding frauds in their jurisdictions that involved crypto transactions or a wallet with a Cayman nexus.

Sanctions and Politically Exposed Persons

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, which in some cases owned Cayman flagged luxury yachts.

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 into 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.

Almost three quarters of the cases in this category are requests for information from overseas FIUs and local law enforcement pertaining to money laundering investigations.

SARs received from domestic reporting entities in this category 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.

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.
- ☐ CIMA, DITC and any public body to whom the Cabinet has assigned the responsibility of monitoring compliance with money launder regulations under section 4(9) of the POCA.
- ☐ 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 amended in December 2017 to allow the FRA to disseminate, in its discretion or upon request, information and results of any analysis to CIMA, any public body to whom the Cabinet has assigned the responsibility of monitoring compliance with money laundering regulations under section 4(9) of the POCA, and any law enforcement agency within the Islands (section 4(2)(ca)). A further amendment was made to the POCA in December 2018 removing the requirement to obtain the consent of the Hon. Attorney General for the FRA to disseminate information to an overseas FIU.

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 1,501 new reports. The FRA completed the review of 857 of these reports, leaving 644 in progress at 31 December 2023. Of the 857 new reports closed, 313 were filed as intelligence, 38 were deemed to require no further immediate action, 363 resulted in a disclosure, 118 were replies to requests from FIUs and 25 were replies to requests from local agencies.

The FRA also completed the review of 210 of 690 reports carried over from 2022, 21 of 458 reports carried over from 2021, 10 of 440 reports carried over from 2020, 4 of 634 reports carried over from 2019, 23 of 392 reports carried over from 2018, 2 of the 203 reports carried over from the interim period of 1-Jul-17 to 31-Dec-17, 3 of 237 cases carried over from

	Reporting Period									
Disposition	2023	2022	2021	2020	2019	2018	2017	2016-17	2015-16	2014-15
Royal Cayman Islands Police Service	353	177	10	8	3	9	-	3	1	-
Cayman Islands Monetary Authority	251	123	3	3	2	7	-	2	1	-
Other Local Law Enforcement Agencies	17	4	-	-	1	-	-	-	-	-
Other Competent Authorities	4	2	1	2	-	-	-	1	-	-
Overseas FIUs	304	170	7	6	2	8	-	2	-	-

Table 3.8: Number of SARs that contributed to disclosures made during 2023

	No. of Cases									
							1 Jul – 31 Dec			
Disposition	2023	2022	2021	2020	2019	2018	2017	2016-17	2015-16	2014-15
Cases Analysed Requiring No Further Action	38	25	33	241	210	210	213	128	213	311
Filed as intelligence	313	246	209	6	-	-	-	-	-	-
Cases Analysed that Resulted in a Disclosure	363	664	215	237	181	244	106	160	195	161
Reply to Domestic Requests	25	22	32	38	37	17	8	8	3	-
Reply to Overseas Requests	118[1]	149[2]	99[3]	69[4]	80[5]	95[6]	35[7]	71[8]	61[9]	58
In Progress (as at 31 December 2023)	644	480	437	430	630	369	201	234	148	38
Total Cases	1,501	1,586	1,025	1,021	1,138	935	563	601	620	568

Table 3.9 Disposition of reports received as at 31 December 2023

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

2016/17 and 3 of 151 reports carried over from 2015/2016, a total of 276 reports. Of the 276 previous reports that were completed, 33 were deemed to require no further immediate action, 216 resulted in a disclosure and 27 were replies to requests from FIUs. Those 216 reports together with the 363 from 2023 comprise the 579 reports 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 reports for the past ten reporting periods as at 31 December 2023.

As at 31 December 2023, the FRA had commenced initial analysis on: 287 of the 644 pending 2023 cases; 161 of the 480 pending 2022 cases; 90 of the 437 pending 2021 cases; 149 of the 430 pending 2020 cases; 185 of the 630 pending 2019 cases; 104 of the 369 pending 2018 cases; 53 of 201 pending Jul – Dec 2017 cases; 50 of 234 pending 2016/2017 cases; and 45 of 148 pending 2015/2016 cases.

Financial Intelligence Disclosures

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

Recipient	2023	2022	2021
RCIPS	214[10]	152[11]	173[12]
CIMA	105	65[13]	47[14]
ACC	3[15]	9[16]	3
CBC	19[17]	9	9
CARA	1	2	1
DITC	2	1	-
DCI	5	1	-
Overseas FIUs	491[18]	374[19]	241[20]
Total	842	613	463

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

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

- fraud – 49%
- sanctions & regulatory matters – 8%
- Corruption – 7%
- money laundering – 6%
- Drug trafficking – 5%

[10] Includes 13 responses to 13 requests
[11] Includes 14 responses to 17 requests
[12] Includes 41 response to 34 requests
[13] Includes 3 responses to 3 requests
[14] Includes 3 responses to 3 requests
[15] Includes 1 response to 1 request
[16] Includes 3 responses to 3 requests
[17] Includes 9 responses to 9 requests
[18] Includes 140 responses to 145 RFIs from overseas FIU that disclose substantial information
[19] Includes 142 responses to 140 RFIs from overseas FIU that disclose substantial information
[20] Includes 104 responses to 79 RFIs from overseas FIU that disclose substantial information

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

- fraud – 58%
- sanctions & regulatory matters – 9%
- international corruption – 9%
- money laundering – 6%
- tax evasion – 4%

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

In 2022 the FRA made 232 voluntary disclosures to overseas FIUs from 468 reports completed. Those 468 reports comprise 419 reports from 2022, 36 reports from 2021, 4 reports from 2020, 7 reports from 2019, 1 report from 2016/2017, and 1 report from 2015/2016.

The FRA also provided 140 responses to 145 requests for information from overseas FIUs. Those requests comprise: 118 requests from 2023, 20 requests from 2022, 6 requests from 2021, and 1 request from 2019.

In 2022, the FRA also responded to 140 requests for information from overseas FIUs. Those requests comprise: 129 requests from 2022, and 11 requests from 2020.

Chart 3.10 on the next page shows that the 2023 voluntary disclosures and responses went to 66 different jurisdictions.

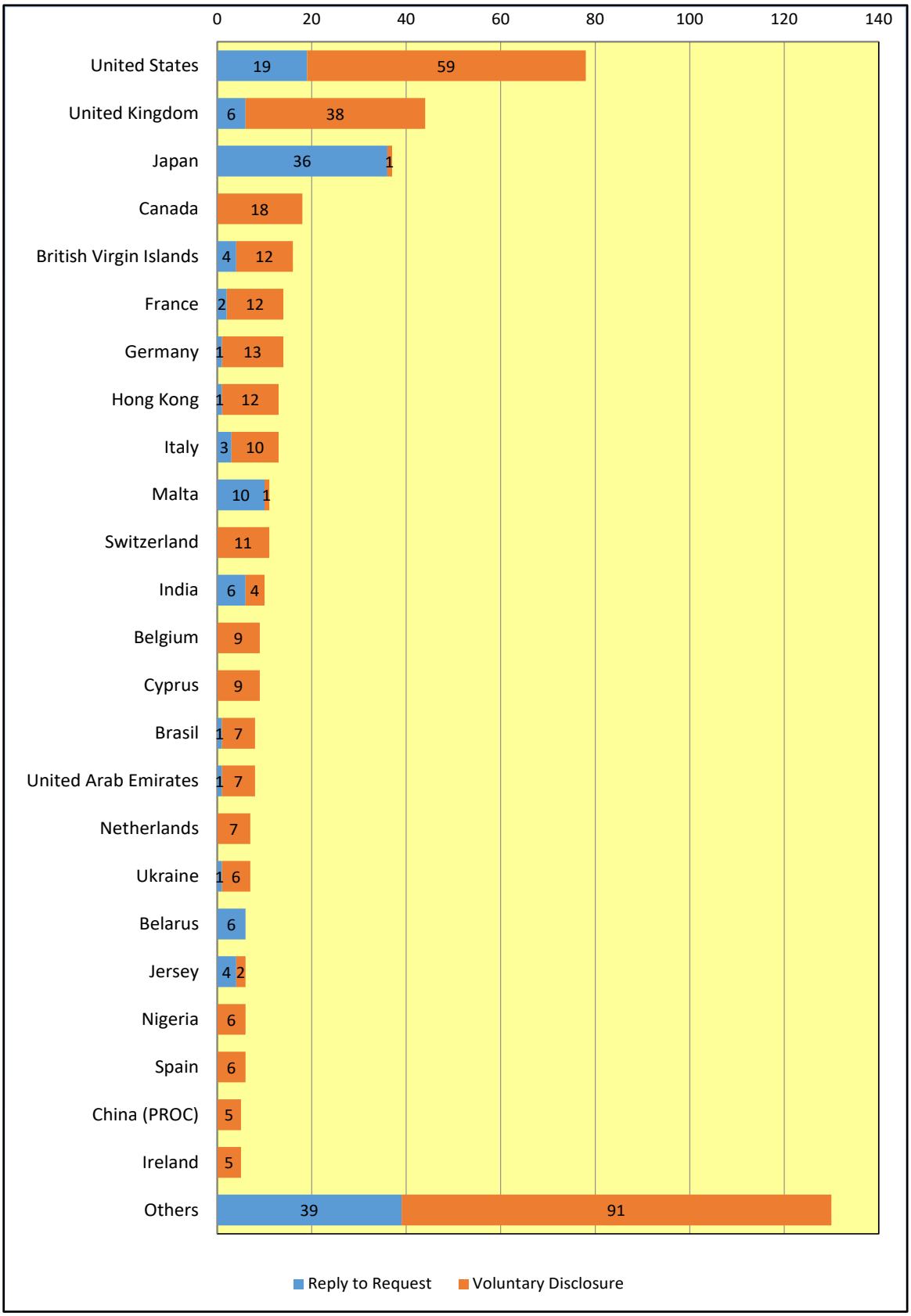


Chart 3.10: Overseas disclosures and replies to request for information

Significant Events

Analysis of Reports

The FRA had 4,744 reports to analyse during the Reporting Period, comprising: 1,501 new reports, 520 reports carried over from 2022, 387 reports carried over from 2021, 289 reports carried over from 2020, 458 reports carried over from 2019, 278 reports carried over from 2018, 157 reports carried over from Jul – Dec 2017, 191 reports carried over from 2016/2017 and 113 carried over from 2015/2016. There were also 850 reports that where initially analysed, but not completed as they required further analysis, comprising: 170 carried over from 2022, 71 carried over from 2021, 151 reports carried over from 2020, 176 reports carried over from 2019, 114 reports carried over from 2018, 46 reports carried over from Jul – Dec 2017, 46 reports carried over from 2016/2017, 38 reports carried over from 2015/2016, and 38 reports carried over from 2014/2015.

The FRA staff analysed 1,492 reports, during the Reporting Period, comprising: 1,145 reports from 2023, 206 reports from 2022, 44 reports from 2021, 14 reports from 2020, 24 reports received from 2019, 29 from 2018, 11 from Jul – Dec 2017, 9 reports from 2016/2017 and 10 reports from 2015/2016. An average of 124 reports were analysed per month in 2023 compared with 96 reports in 2022.

A total of 1,133 reports were closed during the Reporting Period, comprising: 857 reports received in 2023, 210 reports received in 2022, 21 reports received in 2021, 10 reports received in 2020, 4 reports received in 2019, 23 reports received in 2018, 2 reports received in Jul-Dec 2017, 3 reports received in 2016/2017 and 3 reports received in 2015/2016. On average, 94 reports were completed per month in 2023 compare with 83 reports in 2022.

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:

	2023	
Contents of the Disclosure	**CIBFI**	**CIMA**
Provided new information regarding known subjects	31	3
Provided you with unknown subjects	57	12
Corroborated information already known	14	2
Information disclosed to another agency	3	-
Triggered new investigation	11	3
Use of the Disclosure		
Actionable	54	6
Not Actionable	106	10
Total Feedback Forms provided	**160**	**16**

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 also used financial intelligence to exercise its powers under section 4(2)(b) of the POCA on four (4) occasion 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 128 (2022: 193) 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. The FRA forwards these notices automatically to local law enforcement agencies and competent authorities, converts it to a Cayman Notice and publishes the Cayman Financial Sanctions Notice on its website. The average turn-around time for converting these notices, distributing them via e-mail and posting them to the FRA's website is between 1-3 hours.

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

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

1. Fraud - Misappropriation

The FRA received a SAR from a Cayman Islands Bank & Trust Company ("FSP 1") reporting that a client, Subject A, is under investigation by law enforcement agencies in Jurisdiction 1. Subject A is the founder and sole director of two Cayman Islands registered companies, Company X and Company Y, and is the sole shareholder and director of Company Z, domiciled in Jurisdiction 2. Company X and Company Y maintain custody accounts with FSP 1.

FSP 1 received a request from Subject A regarding a swap of assets: FSP 1 would receive assets held in the name of Company Z at a bank in Jurisdiction 3 and FSP 1 would send assets to the bank in Jurisdiction 3. When queried about the transaction, Subject A did not provide sufficient reasoning for the swap of securities and advised FSP 1 not to proceed.

As part of their due diligence in reviewing the request, FSP 1 conducted internet searches and became aware of publicly available information that law enforcement agencies in Jurisdiction 1 have registered a case against a number of persons, including Subject A, for a significant fraud.

The FRA made requests to the OFIUs in Jurisdictions 1, 2, and 3 to amplify its analysis. The FRA also issued s.4(2)(c) directives to the General Registry, FSP 1 and FSP 2.

Given the nature of the allegations against Subject A, the FRA made an immediate disclosure to RCIPS. The FRA also exercised its powers under section 4(2)(b) and 4(3) of the Proceeds of Crime Act (2020 Revision) to order FSP 1 and FSP 2 to refrain from dealing with the accounts associated with Subject A for a period not exceeding twenty-one days.

As a result of the FRA's Directive, FSP 2 filed a SAR which, among other things, reported that Company X holds an account at FSP 3 and that Subject A requested the sale of all of Company X's assets held by FSP 3 and to wire the funds to Subject A. The FRA also became aware that Subject A that subject A holds an account at FSP 4.

As a result, the FRA exercised its powers under section 4(2)(b) and 4(3) of the Proceeds of Crime Act (2020 Revision) to order FSP 3 and FSP 4 to refrain from dealing with the accounts associated with Subject A for a period not exceeding twenty-one days.

The FRA's analysis of the information received identified that Subject A or associated companies held accounts in Jurisdiction 4, 5, 6, 7 and 8. The FRA made RFIs to the OFIUs in these jurisdictions.

Key findings noted by the research and analysis performed by the FRA:

- Subject A holds a Cayman Islands work permit for a Special Economic Zone company, but has only visited the Cayman Islands; of note, Subject A and utilises a Cayman Islands address on a number of bank accounts (both locally and internationally), despite not residing in the Cayman Islands
- A review of Subject A's account activity highlighted receipt of funds from third parties; structuring; and transactions inconsistent with the stated purpose of the account.
- Responses to FRA Directives indicated that Subject A changed e-mail address to one that is not directly identifiable to the individual. Subject A also requested verification of employment income be made via an e-mail address that appears to not be associated to the employer's domain. Further, the contact information for Subject A's accountant was at a domain which also appeared to be personal in nature.
- An incoming wire transfer reported pursuant to the Anti-Money Laundering (Class A And Class B Bank Threshold Reporting) Regulations, 2022

The FRA made 3 disclosures to RCIPS (an initial disclosures plus two supplemental disclosures) and a disclosure to the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators:

- Unusual transfer requests indicative of layering funds and evasive responses to FSP queries
- Adverse media regarding large-scale fraud investigation overseas
- Suspicious transactions indicative of structuring and transactions that appear inconsistent with the purpose of the account

2. Fraud - Ponzi scheme:

The FRA received a number of SARs from various FSPs regarding a suspected Ponzi scheme involving Company A, an Investment Manager (IM) domiciled in Jurisdiction 1 that acts as IM for a number of Cayman funds.

A Cayman director of one of the Cayman funds received a complaint from a managed account holder of Company A about its failure to fulfil a redemption request. It was further alleged, that

other investors had requested redemptions and received unsigned cheques from Company A. The Cayman director asked why the complaints were addressed to him and was informed that he was named as a director of Company A on its website.

The Cayman director reached out to Company A to have his name removed, and also enquired about the complaints that had been brought to his attention. The explanations provided included that a bank in Jurisdiction 1 had placed Company A's account on hold without explanation and that Company A was switching banking relationships as they had payment processing issues with another bank. The banking issues together with the redemption complaints raised concerns about the financial stability of Company A.

SARs were also received from other FSPs reporting significant delays in the launch of any of the Cayman funds, absence of instructions for any of the funds and for unpaid professional fees. Subsequently a Regulatory Agency domiciled in Jurisdiction 1 filed a case against Company A and a number of its funds, alleging that the owners of Company A were running a Ponzi scheme.

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

Indicators:

- Financial stability concerns (e.g., failure to fulfil a redemption request or receiving unsigned cheques in lieu of payment)
- Unexplained issues with banks or payment processors
- Significant delay in launch of funds and lack of any instructions regarding the funds
- Adverse information alleging subject's involvement in a Ponzi scheme

3. Fraud - Business Email Compromise

The FRA received a SAR from a Cayman Islands registered Fund ("Fund A") after it became aware that a payment was made using fake wire details.

Fund A was advised that the email of an employee of one of its service providers ("Company B") had been compromised. Fund A's administrator received an email advising that payment instructions for an outstanding invoice for Company B had to be changed, as there was an ongoing audit of the bank account and any payments to it risk being rejected.

The payment was made to an account in Jurisdiction 1 based on a revised invoice. The account details were later found to be fraudulent.

Fund A advised that their administrator confirmed the changes to the account directly with the email that sent the revised account details.

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

RCIPS contacted law enforcement in Jurisdiction 1, who in turn contacted the bank where the payment was received and a partial recovery of funds was made. Individuals linked to the crime were identified and the investigation is ongoing.

Indicators:

- Change in banking details communicated via email with suspect reasoning
- No independent verification of change in wire transfer details
- Use of little known bank in a foreign jurisdiction

4. Fraud - Business Email Compromise / CEO Fraud:

The FRA received a SAR from a Bank regarding a successful business email compromise / CEO fraud committed against one of its clients, Company A.

The Bank reported that a director of Company A notified them that the company had fallen victim to a business email compromise fraud. They received an invoice that was believed to have originated from their Chief Executive Officer (CEO), and settled the invoice by making a wire transfer to a bank in Jurisdiction 1.

When the error was discovered, Company A requested a recall of the funds; however, the recall was unsuccessful as the funds had already been withdrawn. Company A reported the incident to both local and overseas law enforcement agencies.

A review of the fraudulent invoice showed inconsistencies in fonts used and misaligned columns. There was also a spoofed link that does not match the official site of the issuer of the invoice.

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

Indicators:

- Invoice containing inconsistencies in fonts used and misaligned columns and spoofed website
- Request for payment made with urgency

5. Fraud - Phishing / Spoofing

The FRA received a SAR from Bank A regarding a phishing / spoofing incident report by one of its customers.

The customer reported receiving a message stating they had been connected with Individual A from Bank A. The message was followed by a call from Individual A, who advised that the customer’s account had been compromised and enquired whether they had made any charges with certain online shopping vendors.

Individual A also stated he worked for a security firm for all banks on the Island and asked the customer to confirm if they maintained an account at Bank B, which the customer confirmed. Individual A proceeded to advise the customer that the account at Bank A was not safe and that they should transfer funds to the account at Bank B. Although the customer was initially uneasy, Individual A assured the customer they could visit any of Bank A's branches to verify the information; the customer provided full online details to effect the transfer to Bank B.

The customer subsequently received an alert of funds being fraudulently transferred from their account at Bank B.

In order to amplify its analysis, the FRA issued a section 4 (2) (c) directive to Bank B to obtain account statements and details of specific transactions. Analysis of the information revealed that the fraudulent transfers were made to individuals with accounts in Jurisdiction 1.

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

Indicators:

- Messages / calls purporting to come from a bank advising an account had been compromised
- Request for the customer's personal information and online banking credentials via telephone.

6. Fraud – Securities Violations / Fronting the sale of securities

The FRA received a SAR from a Securities Investment Business on a client, Subject A, who was suspected of assisting individuals in circumventing trading prohibitions. The suspicion was prompted by a request from Subject A to wire proceeds in the account to an account that is held jointly with Subject A's spouse, Subject B.

Standard checks on Subject B revealed a significant judgement levied by a regulator in Jurisdiction 1, which concluded they were guilty of insider trading and resulted in the individual being banned from trading for several years and ordered to disgorge a significant amount.

The brokerage account was held solely by Subject A; however, Subject B was actively involved in the opening of the account and was copied on all communications even though they did not have any association with the brokerage account.

The funds held in the brokerage account were proceeds of the sale of the stock of Company X. On further review, it was discovered that another individual, Subject C, had 'sold' the stock in Company X to Subject A through a stock purchase agreement on the basis that Subject C would receive a substantial portion of the proceeds of any sale of the stock of Company X directed by Subject A. Standard checks on Subject C revealed an action by a regulator in Jurisdiction 2.

Further review showed that Subject A had previously entered a similar stock purchase arrangement for the stock of Company X with another individual. It was thus noted that Subject A, who has no financial background, had been entering into complex stock purchase agreements.

Given the facts above, the Securities licensee suspected that Subject A was either an unwitting or a willing participant to circumvent the prohibitions placed upon Subject B and Subject C.

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

Indicators:

- An individual with no direct association to an account being actively involved with its opening and management
- Wire transfer request to a bank account jointly held with an individual banned from investing
- Adverse media regrading counterparties and associated individuals for securities violations
- Sale of securities for a third party on a contingency basis

7. Fraud – Elderly Fraud / False Representation

The FRA received a SAR from a Cayman Islands Company Manager regarding suspicious behaviour and inconsistent information provided by a prospective client, Subject A. The Company Manager was approached by Subject A's lawyer / representative to set up a Cayman Islands registered company. The Company Manager declined the business, as their due diligence on Subject A revealed a number of red flags, including:

- Subject A's age and claims of more than 10 year of industry experience appear inconsistent (not old enough to have the stated experience)
- The residential tenancy agreement, provided as evidence of address in Jurisdiction 1, contained questionable information as to one party's legal capacity to enter into a contract as well as unusual terms.
- The address provided in Jurisdiction 1 is not residential in nature.
- Source of funds is difficult to verify.
- The reference letter for Subject A appears to be from a related party.
- The type of company Subject A requested be established was suddenly changed from a Virtual Asset Service Provider to a Financial Management Consultancy Company with no explanation.

The FRA's analysis noted the following:

- Subject A is the registered owner of Company X, a not-for-profit company in Jurisdiction 1.
- Subject A's declared source of funds is from the sale of his business, Company Y domiciled in Jurisdiction 1.
- FRA's research conflicts with Subject A's claims about the nature of business of Company Y.
- A review of the bank statements provided shows funds being received prior to alleged transactions and inconsistent with the claims of subject A
- The websites for Company Y and Subject A's alleged employer are very similar in nature, and contain errors and spelling mistakes.
- Adverse information later became available claiming Subject A and Company Y are running a scam and employing abusive customer practices preying on the elderly.

Information obtained by the FRA was indicative that Subject A is involved in an ongoing law enforcement investigation in Jurisdiction 1.

A disclosure was made to the OFIU in Jurisdiction 1 for intelligence purposes.

Indicators:

- Inconsistent identity and residence information
- Irregularities in the documents provided suggesting spurious nature
- Large payments that don't align with alleged agreements
- Adverse media regarding fraudulent scheme

8. Fraud – False Representations

The FRA received SARs from Cayman Islands registered Funds in relation to Subject A, Subject B and Subject C ("the Subjects") being linked to an alleged financial fraud in Jurisdiction 1. The Subjects were invested in the Funds via a Nominee Investor based in Jurisdiction 2. The Nominee Investor had requested a redemption to be paid via a payment service provider. On the dealing date the payment service provider cancelled the transfer and afterwards the nominee investor did the same.

The Funds queried the cancellation with the Nominee Investor and were informed that the Subjects were former executives of Company A in Jurisdiction 1, and had their assets frozen by the Securities Regulator in Jurisdiction 1 pending an investigation of their alleged involvement in a massive financial fraud involving misstatement of Company A's financial position.

The Subjects had significant amounts invested and the Funds proceeded to freeze their accounts and filed SARs.

FRA analysis indicated that the monies invested in the Funds originated from banks in Jurisdiction 1 and could possibly be the

proceeds of crime. It was also noted that asset recovery measures are ongoing in Jurisdiction 1.

The FRA made disclosures to RCIPS and the OFIUs of Jurisdictions 1 and 2 for intelligence purposes.

Indicators:

- Sudden cancellation of scheduled redemption or transfer
- Initial investments originated from a jurisdiction where criminality is alleged
- Adverse media regarding financial fraud
- Asset recovery measures in a foreign jurisdiction

9. Attempted Fraud – False Documents / Potential Advanced Fee Scheme

The FRA received a SAR from a Bank regarding fraudulent documents received from an individual, Subject A, who claimed to have an account with the Bank.

Subject A, a citizen of Jurisdiction 1, arrived in the Cayman Islands and visited the Bank to enquire whether his application for a business account in the name of Company X was established. Subject A informed the Bank that they were expecting US$ 20 million dollars by wire transfer to be deposited to an account under the name of Company X. The Bank's searches revealed that neither Subject A nor Company X held accounts with them.

Subject A visited the Bank shortly thereafter to confirm if the funds had been received. The Bank stalled the customer while they contacted RCIPS; however, Subject A left the Bank before RCIPS could arrive.

Subject A presented documents allegedly from the Cayman Islands Registry, an international organisation, the Treasury Department in a foreign jurisdiction and a copy of a Swift Messaging text as proof that the money will be deposited. The documents presented were identified to be forgeries. The Bank noted that Subject A might also be a victim of fraud.

FRA analysis and review identified the following:

- Company X is not registered in the Cayman Islands and the certificate of incorporation was fictitious.
- Among the documents presented by Subject A were communications and confirmation from a fictitious officer of the Bank.
- Based on the supporting documents, the funds were to be sent from an account held by Entity Y, domiciled in Jurisdiction 2, from a bank also based in Jurisdiction 2. In addition, it appears the Entity Y also has an office in Jurisdictions 3 and 4.

Disclosures were made to RCIPS and the OFIUs in Jurisdictions 1 to 4 for intelligence purposes.

Indicators:

- Claims about substantial incoming funds supported by suspect documents.
- The transactions referred to are not ordinarily within the remit or would not be made by the organisations issuing them.
- Originator and beneficiary of the wire transfers are from the same Jurisdiction with no explanation for the need of a Cayman bank account
- Documents identified to be signed by fictitious individuals.

10. Money Laundering – Political Exposed Person

The FRA received a number of SARs from a licensed Cayman Islands Mutual Fund Administrator and a Fund regarding investments held by Company X and Company Y, domiciled in Jurisdiction 1 and Jurisdiction 2 respectively, and their ultimate beneficial owner Subject A, resident in Jurisdiction 3.

Through the course of an ongoing review, adverse media identified that Subject A was linked to a money laundering scheme that facilitated significant funds to flow from companies in a high risk jurisdiction into other jurisdictions globally.

The SARs were submitted on the suspicion that the investments might have been funded from the money laundering scheme; the SAR also identified significant transactions with entities with similar names to the entities associated with Subject A. Accounts at institutions operating in Jurisdictions 4 and 5 were identified.

Disclosures were made to RCIPS, CIMA and the OFIUs in Jurisdiction 1 to 5 for intelligence purposes.

Indicators:

- Transactions involving countries deemed high risk or non-cooperative by the Financial Action Task Force.
- Complex group structures with no apparent economic purpose
- Adverse media regarding involvement with a significant global money laundering scheme
- Transactions with unusual patterns involving transactions to entities with similar name of sender

11. Money Laundering - Illegal Foreign Gambling

The FRA received a SAR from a Cayman Islands regulated Private Fund ("the Fund") regarding an investment held by Company X, domiciled in Jurisdiction 1, and its ultimate beneficial owner Subject A following receipt of information that Subject A was arrested by authorities in Jurisdiction 2 for offences relating to money laundering, illegal running of gambling operations and illegal betting activities in casinos.

There was no adverse information on Company X or Subject A at the time of executing the Subscription Agreement. Since the initial

subscription, the Fund received additional subscriptions and made distribution payments to Company X's bank account in Jurisdiction 2.

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

Indicators:

- Adverse media regarding money laundering and running illegal gambling operations
- Uncertainty about source of funds

12. Drug Trafficking

The FRA received a SAR from a Bank regarding two customers, Subject A and Subject B, as a result of becoming aware of publicly available information that they were recently charged with the importation of illegal drugs and money laundering.

There was no indication that Subject A and Subject B were associated with each other. The Bank had previously processed a request for information from local law enforcement regarding the account held by Subject B. The Bank's review of Subject B's account revealed that it had not been operating within its intended purpose; of note there had been no deposits from the identified employer for salary and a number of cash deposits had been made on the same day but at different branches.

A disclosures were made to RCIPS for intelligence purposes.

Indicators:

- Request for information from local law enforcement
- Account not operating within its intended purpose
- Cash deposits on the same day and different branches
- Adverse media regarding drug trafficking and money laundering

13. Child Abuse – Virtual Asset

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

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

Indicators:

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

14. 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 2023 AND BUILDING ON STRENGTHS IN 2024

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 2023

During 2023 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 2023, the FRA:

   (i) Produced 840 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 160 Feedback forms from the RCIPs and 16 Feedback forms from CIMA.

   (ii) Continued to disseminate information in a timely manner. With the FRA actively monitoring the timeliness of our disclosures, 53% of disclosures to local law enforcement was made within 35 days, compared to 46% in 2022. The average number of days to complete a request for information from an overseas FIU was 42 days in 2023, compared to 40 days in 2022.

   (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 2023, Staff of the FRA engaged in the following Outreach events covering

one or more of the following topics: functions of the FRA, SAR statistics, SAR reporting obligations, and obligations regarding targeted financial sanctions related to terrorist financing and proliferation financing:

(i) Five (5) presentations at international and domestic industry association events, or other international events.

(ii) Five (5) presentations at private sector organised events, to private entities or to public entities.

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

(iv) Two (2) meetings with MLROs to demonstrate AMLive Reporting Portal functionalities.

During 2023 the FRA issued 43 feedback forms to 29 reporting entities from a cross-section of sectors, with the following quality ratings: (i) Fair: 4; (ii) Good: 19; and (iii) Very Good: 20.

In December 2023 the FRA launched a new website with a modern, clean and simplified format. The new website features easy to find information on key functions of the FRA as well as a dedicated page for Financial Sanctions. It showcases a suite of new features which include fraud alerts, a quick link to forms and documents and how to file a SAR.

3. Ongoing CFATF / FATF Work

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.

The Hon. Attorney General of the Cayman Islands served as Chair of the CFATF for the period November 2022 to November 2023; the Director of the FRA served as Chair of the CFATF Heads of FIUs Forum for the same period. In addition to the two in-person meetings during the CFATF Plenary and Working Group meetings, the Director also introduced and chaired two virtual CFATF Heads of FIUs Forums in 2023.

4. High Performing Staff

This priority was achieved to a significant extent. Performance expectations for staff are clearly defined and documented. Staff completed analysis on 1,492 cases and closed 1,133 cases, both of which are the highest for any reporting period.

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 the 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 using functionalities of i2 iBase and i2 Analyst Notebook. This included running queries and creating browse definitions as well as using different datasheets for records.

(ii) Members of staff received training in AMLive on how to create SARs. The training involved hands on exercises of creating SARs in the FRA's online reporting platform.

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

(iv) Evaluation of Blockchain analytical tools was started and will be finalised in 2024.

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

(vi) Continued liaision with the Office of the Chief Information Security Officer to address / respond to all security alerts.

Strategic Priorities for 2024

During 2024 we will continue to build on our strengths and seek to continuously improve performance. Our main priorities for the year will remain unchanged, namely:

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

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

Through its analysis of information collected under the POCA reporting requirements, the FRA aims to develop specific financial intelligence disclosures and provide strategic insights into trends and patterns of financial crime.

To deliver on this priority, we will:

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

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

(iii) Meet regularly with local agencies and obtain formal feedback on the usefulness of our intelligence reports.

Feedback will also be sought from overseas FIUs.

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

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

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

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

To deliver on this priority, we will:

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

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

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

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

(v) Continue to enhance the new website to provide reporting entities with a useful AML / CFT / CFP resource.

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

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

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

To deliver on this priority, we will:

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

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

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

(iv) The Director will continue to make meaningful contributions to the Egmont Committee as a Regional Representative for the Americas Region.

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

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

4. High Performing Staff

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

To deliver on this priority, we will:

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

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

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

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

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

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

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

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

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

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

   (i) Complete data migration from the old database to the new i2 iBase database, including retiring the former database and servers.
   (ii) Provide relevant training on changes to software / technologies utilised by staff (Egmont Secure Web, ShareFile, iBase and Analyst Notebook).
   (iii) Provide feedback mechanism for staff to make suggestions on technology could better assist in their analysis.
   (iv) Continue to assess and improve infrastructure for sharing intelligence and communicating with Competent Authorities.
   (v) Complete the evaluation of Blockchain analytical tools and procure the most useful tool for the FRA to enhance analysis of cases involving crypto assets.
   (vi) Develop a well-planned incident response program to address any Security Incidents that arise from security alerts from monitoring systems and other security breaches.

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
Fax: 345-945-6268
E-mail: financialreportingauthority@gov.ky
Visit our Web site at: www.fra.gov.ky