PREFACE

The FIA was established on the basis of Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) international standards created by the Financial Action Task Force (FATF). It employs ten (10) members of staff and its operations are funded mainly by government subventions. It is an independent body with its own legal identity under supervision of a Board chaired by the Deputy Governor.

Statistical data recorded during the year include one hundred and fifty-three (153) Suspicious Activity Reports (SARs) representing a decline of 19.9% when compared with the one hundred and ninety-one (191) reports received in the previous year. Of the one hundred and fifty-three (153) SARs filed during the year, one hundred and fifty-one (151) were classified as proactive while two (2) were recorded as reactive. As usual, Trust and Company Services Providers (TCSP) accounted for the majority of the reports followed by banking institutions. The majority of reports were fraud and money laundering related activities while a very small number were linked to AML/CFT compliance related issues.

The fraudulent activities the reports were linked mostly to "Ponzi Schemes". Ponzi schemes are fraudulent investment operations that pay returns to its investors from their own money or the money paid by subsequent investors, rather than from profit earned by the individuals or organizations running the operations. While many large schemes surfaced at the very beginning of the global economic recession, a number of smaller schemes have appeared more frequently in recent times. Some of these schemes, albeit a very small percentage, have had a nexus to our financial services sector by way of bogus offshore entities often claiming to be licensed and regulated in the British Virgin Islands.

As a consequence of the decline in the number of SARs received during the reporting period, the number of onward disclosures of financial intelligence also decreased. There were fifty-four (54) onward disclosures during the reporting year compared with fifty-eight (58) the previous year. Of the fifty-four (54) disclosures initiated during the year, thirteen (13) were made to the Royal Virgin Islands Police Financial Investigations Unit (RVIPFIU) for further investigations while the remaining forty-one (41) were sent to our Egmont Group counterparts.

The agency also received sixty-two (62) Mutual Legal Assistance Requests (MLARs) compared to seventeen (17) received during the previous year. The majority of these requests originated from Russia and involved the theft and embezzlement of funds from Russian state-owned companies where BVI registered entities or BVIBCs were allegedly used to hide the embezzled funds.

Additionally, the agency recorded seven hundred and two (702) requests for financial and other information representing a 1.73% increase when compared to the number of

requests received in 2010. The majority of these requests originated from our Egmont Group partners.

Though statistical data collected for 2011 shows a slight decline in some areas; i.e SARs, the overall numbers are still relatively high which suggest that the volume of financial crimes occurring worldwide remains high.

As is customary, staff at the FIA also participated in several international meetings organized by the Egmont Group and the Caribbean Financial Action Task Force (CFATF). These meetings are held biannually to focus on issues ranging from international cooperation between law enforcement agencies, to challenges associated with countering money laundering and terrorist financing, and compliance with global anti-money laundering and terrorist financing standards created by international organizations such as the Financial Action Task Force (FATF).

During the year the Agency signed a number of bilateral agreements or memoranda of understanding (MOUs) with some of our Egmont partners. These agreements, some of which were being negotiated since 2010, were able to deliver practical results in expanding and systematizing the flow of intelligence while fostering closer collaboration between agencies.

As is customary, staff training was a main focus throughout the year. Staff members received ongoing training by attending several AML/CTF related courses, seminars, and workshops. These courses, seminars and workshop were aimed at enhancing the staff's knowledge and expertise in AML/CTF related issues.

With the publication of the revised FATF Standards adopted in 2012, countries will be challenged to place an even greater emphasis on strengthening their domestic framework through the introduction of national risk assessments focusing on money laundering, terrorist financing as well as proliferation of weapons of mass destruction (WMDs). These risk assessments will have to be updated continuously based on ongoing analysis of risks and vulnerabilities in their domestic financial sectors.

As I look toward the coming year and beyond I expect there to be many challenges. These challenges will be directly related to the additional responsibility of supervising and monitoring Non-Profit Organizations (NPOs) and Designated Non-Financial Businesses and Professionals (DNFBPs) operating within the territory. In an effort to overcome these challenges, our focus will be on capacity building. I am confident that building a strong organization will help us to overcome the challenges that lie ahead.

Errol GEORGE, Director

Reporting year at a glance

Combating Money Laundering and the Financing of Terrorist related Activities and offences

Receipt and collection of information

- Number of SARs received = 153

Analysis and dissemination

- Number of SARs processed = 153
- Number of SARs cleared = 145
- Number of SARs carried over into 2012 = 8
- Number of SARs referrals to the Royal Virgin Islands Police Force Financial Crimes Investigation Unit = 13
- Number of SARS disseminations to foreign FIU's = 41

Working with domestic regulator and law enforcement authorities

- Interaction with the Financial Services Commission (FSC), BVI Customs, and Royal Virgin Islands Police Investigation Unit
- Number of requests for information received from following domestic agencies:

  FSC= 60
  BVI Customs = 4
  RVIPF = 176

International collaboration to combat ML/TF

- Number of Letters of Requests for Mutual Legal Assistance received = 62
- Number of Letters of Requests for Mutual Legal Assistance processed = 56
- Total number of FIU/Law Enforcement requests for information received = 702
- Number of foreign FIU/Law Enforcement Requests for information processed = 511
- Number of FIA requests sent to foreign FIUs = 16

Our continued growth

- Continued to develop our IT systems to include an offsite information back-up and storage system to facilitate business continuation in the event of a natural or manmade disaster.
- Advertised and filled the position of in-house Legal Counsel to advise the Agency on all legal matters relating to the territory's AML/CTF Framework.
- Commenced preliminary work to take on AML/CFT supervision/monitoring of DNFBPs and NPOs.

Local and international training seminars

- The Agency participated in three (3) in-house training seminars organized by reporting entities within the local financial services sector.
- Agency staff attended various AML/CFT training seminars in an effort to raise their awareness and increase their AML/CFT knowledge and expertise.
- Regular attendance and participation in plenary and working group meetings organized by the Egmont Group of Financial Intelligence Units and the CFATF.

The FIA at the Glance

Our Vision

To provide an effective, professional, and transparent, international co-operation and financial investigation service that fosters public confidence and promotes the reputation of the British Virgin Islands as a centre of law enforcement excellence.

Our Mission

The Financial Investigation Agency acknowledges that it has a vital role to play in helping to maintain a high degree of transparency in the local financial services sector.

To this end, we will work closely with the Financial Services Commission as well as local and foreign law enforcement, and regulatory agencies whose common goal is to implement domestic and international strategies to counter the threats of money laundering and the financing of terrorism.

The Agency also recognises the importance of working closely with stakeholders in the private sector.

To this end, the Agency will make it a priority to provide the necessary technical support and advice to reporting institutions regarding their reporting obligations under the Proceeds of Criminal Conduct Act, 1997.

Recognizing that the success of the Agency in carrying out its core functions largely depends on the degree of knowledge and competencies of its staff, the Agency will continue to ensure that staff members receive the necessary training to equip them with the knowledge and skills to perform effectively in their roles.

Our Core Functions

To receive Suspicious Activity Reports (SARs) from regulated entities in accordance with their statutory obligations under domestic legislation.

Conduct timely and in-dept analysis of information provided in reports, and provide feedback to reporting institutions in an effort to increase the quality of information provided in the reports.

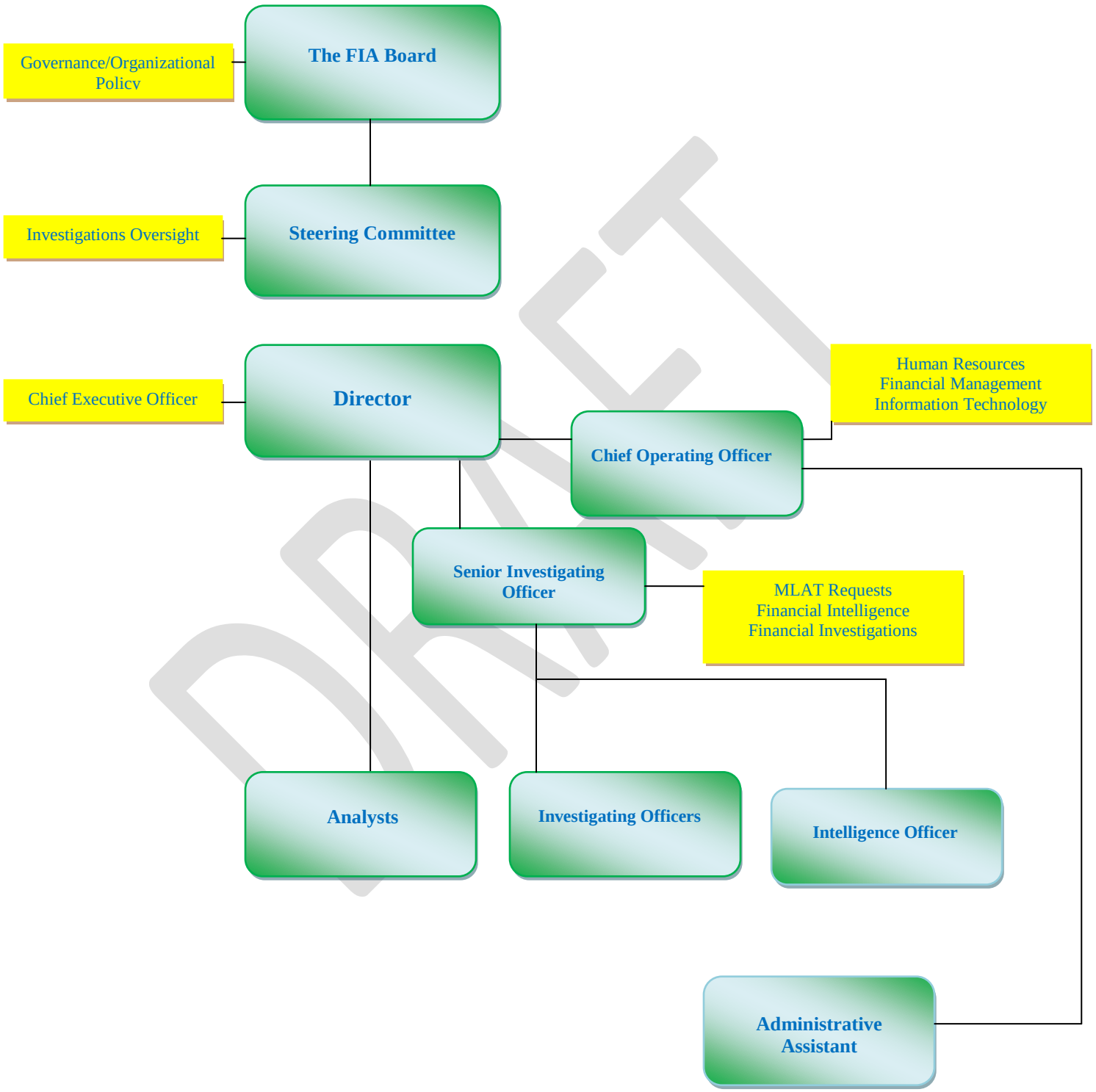
Analyze information obtained from various sources with a view to identifying new and emerging trends and indicators in money laundering, terrorist financing and types of financial crime.

Identify and record money laundering and terrorist financing trends and indicators which can be used in the creation of a cohesive national AML/CFT policy.

Identify money laundering and terrorist financing threats that could pose a potential risk to the Territory's financial services sector.

Raise public awareness concerning the harmful effects money laundering and terrorist financing could have on the Territory's financial services sector if allowed to take root.

Our Organization



What is Money Laundering

Money laundering refers to the process of concealing the source of illegally obtained money. It involves three (3) stages.

Placement: This is the first stage which involves placing the monies into the financial system. This can be done by depositing the monies in small amounts directly into the money launderer's account or comingling the cash with monies generated by legitimate businesses.

Layering: This is the first attempt to conceal or disguise the source of the ownership of the funds. This is done by purposely creating a complex web of financial transactions aimed at concealing any audit trail as well as the source and ownership of funds.

Integration: This is the final stage in the process whereby the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned. By this stage, it is exceedingly difficult to distinguish legal and illegal wealth.

What is Terrorist Financing

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity.

Terrorist groups, like any other criminal organization, build and maintain an infrastructure to facilitate the development of sources of funding, to channel those funds to the providers of materials and or services to the organizations, and, possibly, to launder the funds used in financing the terrorist activity or resulting from that same activity.
Terrorist organizations derive income from a variety of sources, often combining both lawful and unlawful funding. The agents involved do not always know the illegitimate end of that income. The forms of financing can be grouped into two types:

1. *Financial support* – In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organizations, or from individuals.

2. *Revenue generating activities* - Income is often derived from criminal activities such as kidnapping, extortion, drug trafficking, smuggling or fraud.

Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

Financial Investigation Agency

Financial Intelligence Units (FIUs) have existed for many years and more than 120 have been admitted into the Egmont Group, a formal organization or association of FIUs. While many countries are still in the process of establishing FIUs others continue to develop those that are already in existence in order to make them more efficient.

In an era when intelligence plays a key role in helping to unearth crimes and those who perpetrate them, law enforcement agencies are increasingly turning to FIUs to provide vital financial information which is often needed to expose money launderers, terrorist financiers and other perpetrators of financial crimes.

The Agency was formed in 2003 as a specialized government agency to act as a buffer between financial institutions and law enforcement agencies for collecting, analyzing, and disseminating financial and other information particularly linked to suspicious or unusual financial activities, which could have a nexus to crime.

The Egmont Group defines a Financial Intelligence Unit as *" a central national agency responsible for receiving, and as permitted, requesting, analyzing, and disseminating to competent authorities, disclosures of financial information concerning (i) suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation in order to combat money laundering and terrorism financing*".

The Financial Action Task Force also calls on countries to *establish a FIU that serves as a national centre for receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated with predicate offences and terrorist financing, and for disseminating of results of that analysis.*

The Agency was formed as an independent statutory body to strengthen the territory's AML/CFT framework. The Agency's operations are guided by the provisions of the Financial Investigation Agency Act.

The Agency's mandate, first and foremost, is to protect the territory's vital financial services sector from internal and external abuse. We work to achieve this by collaborating closely with our partners at home and abroad. Our collaboration includes:

- The production and sharing of information and intelligence linked to money laundering, terrorist financing, and other types of criminal offences.

- Processing requests for mutual legal assistance where documentary evidence is gathered and provided to requesting authorities overseas for the purpose of assisting in the investigation and prosecution of criminal offences which took place outside the British Virgin Islands.
- Gathering and recording data which is useful in helping us to identify trends in various types of financial crimes.
- Interaction with stakeholders
- Raising public awareness about financial crimes and the possible effect on our financial services industry and society as a whole.

Suspicious Activities reporting

Suspicious Activity Reporting is a key component of the British Virgin Islands Anti-Money Laundering and Countering the Financing of Terrorism framework. The Proceeds of Criminal Conduct Act, 1997 places a statutory obligation on financial and other designated institutions operating in the territory of the Virgin Islands to file Suspicious Activity Reports (SARs) linked to money laundering and terrorist financing. These reports are submitted to the FIA as the designated Reporting Authority. The information contained in SARs is analyzed and disseminated to partner agencies to assist in combating **money laundering**, **terrorist financing** and other types of financial crime.

The Agency is committed to maintaining strict confidentiality of financial and other information held in its database. Unauthorized disclosure of information is a criminal offense to the proceeds of Criminal Conduct Act. Additionally, the Financial Investigation Act (sec. 9) contains specific rules which govern the management of information held within the Agency.

The Agency's operation is also subject to strict security measures, which includes an integrated security system which aims to protect our physical premises, our information security systems, and our physical records which are protected by an added layer of security. The Agency's staff is also expected to maintain a high degree of integrity and confidentiality both on and off the job.

The issue of confidentiality is also extended to reporting entities. Any employee of a regulated entity who suspects that a customer is involved in criminal activity is trained to discuss the suspicion only with their supervisors, and no one else, including the customer who is under suspicion. The fact that a SAR has been filed is required to be kept confidential.

Additionally, an individual or organization is also precluded from discovering the existence of a SAR filed that includes their name. As part of their internal procedures regulated entities undertake an investigation process of their own prior to filing. This is done to ensure that the information reported in the SAR is appropriate, complete, and

accurate. This process will often include review by senior management officials who oversee compliance and/or attorneys or other trained professionals prior to filing.

As previously indicated the agency received one hundred and fifty-three (153) SARs during the reporting year which represents a decrease of 19.9% relative to the previous year. The total number of reports was below the average 190 SARs of the previous three years. There could be a number of reasons for this fluctuation. It could be purely statistical in nature on one hand. On the other hand, it could be attributed to a 90.3% decline in the number of SARs categorized as reactive/defensive SARs filed by reporting institutions during the current reporting period relative to the previous year. Reactive/defensive reporting by institutions is triggered when reporting institutions are in receipt of requests for information from either the Agency or FSC. The decline in reporting could also be directly related to the fact that the number of single cases that triggered multiple SARs during the current reporting period is significantly lower than those reported during the previous reporting period 2009-2010.

Chart 1- Shows a monthly breakdown of SARs received in 2011

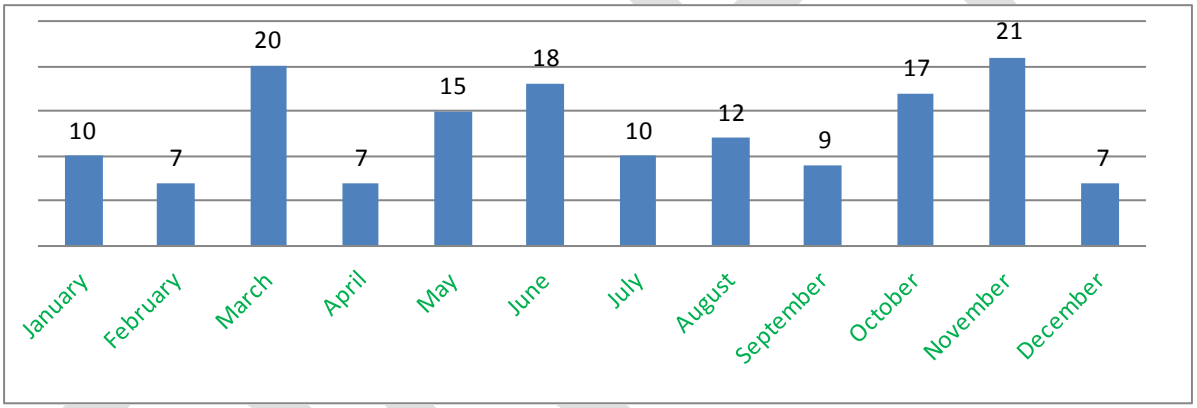


Table 1: Breakdown indicating grounds for suspicion for SARs reported during 2011

Grounds for suspicion	Number
(Fraud) Insider Trading	1
General Fraud	32
Money Laundering	88
Terrorist Financing	1
Drug Trafficking	1
Bribery and Corruption (PEPs)	1
Sanctions Listing	5
Compliance KYC/CDD related issues	20
Reactive/Defensive Reports	3

Chart 2: Shows the number of SARs received between the periods 2008-2011

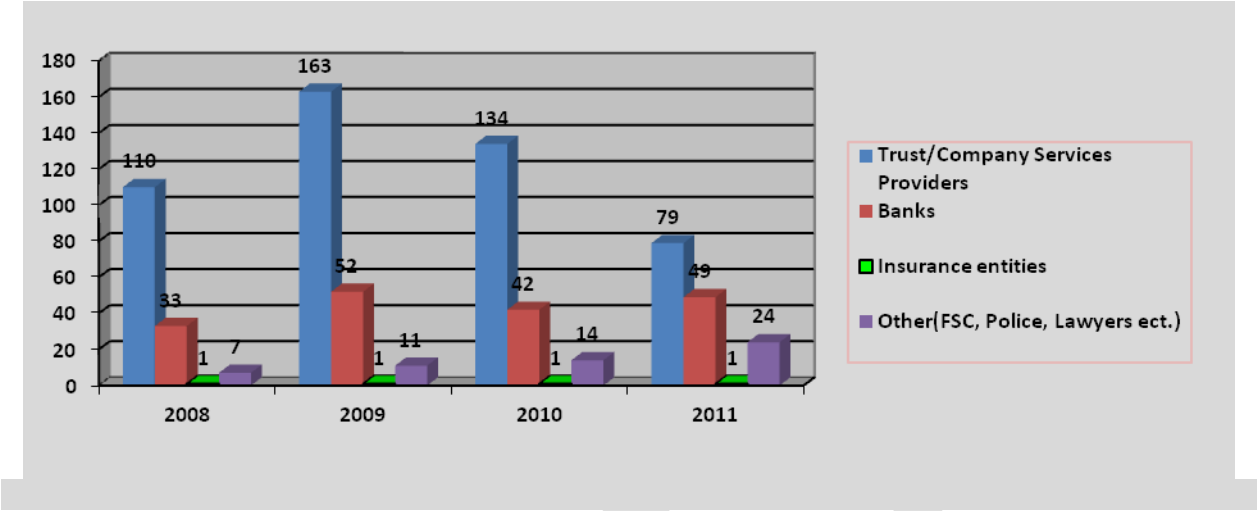


Table 2: Shows a breakdown of how the SARs/STRs received were disposed of during the reporting year 2010

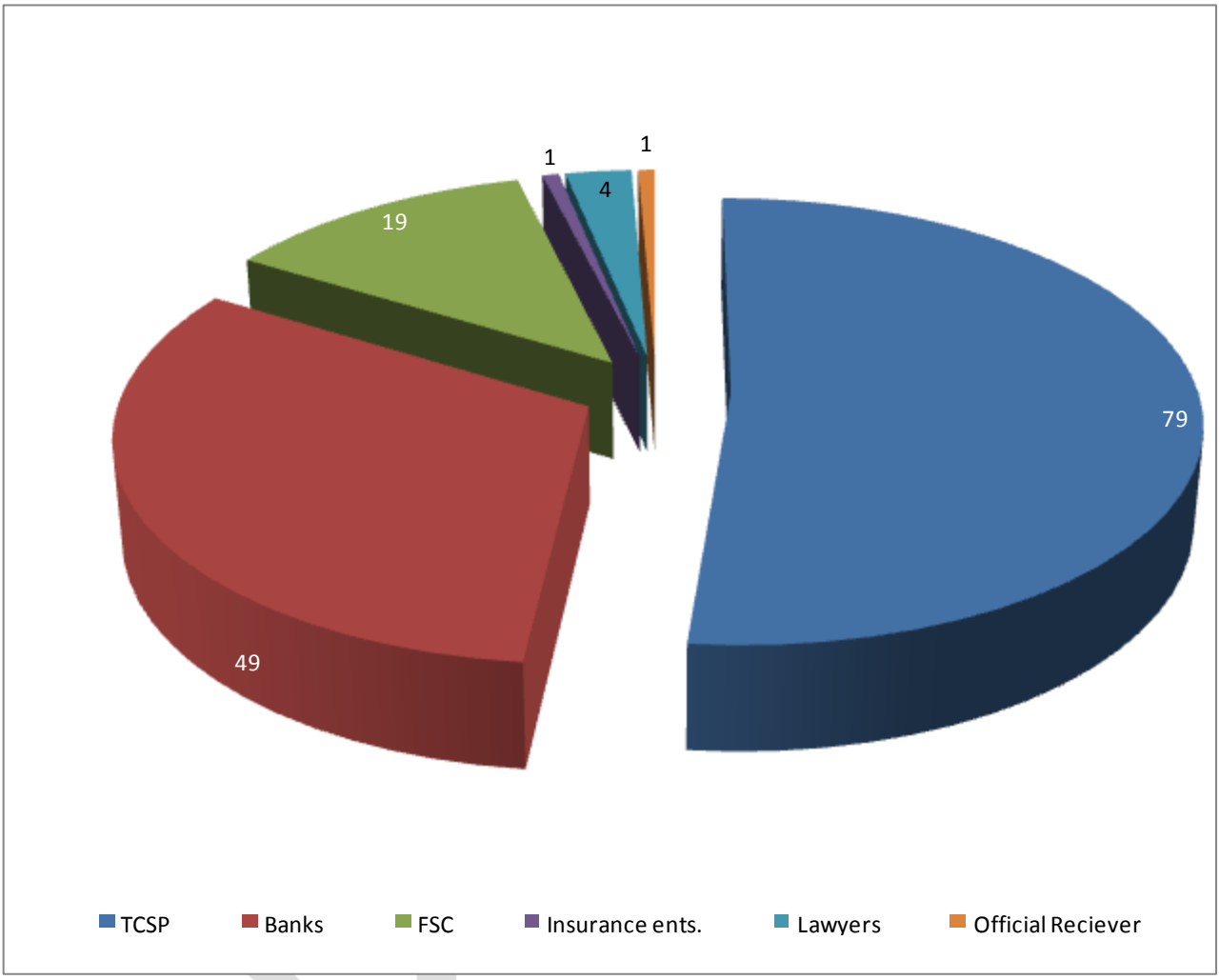
Category	2008	2009	2010	2011
SARs Received	153	227	191	152
SARs/STRs Analyzed	104	227	191	152
SARs/STRs Disseminated Domestic Law Enforcement	6	2	12	13
SARs/STRs Disseminated to international Law Enforcement Agencies and FIUs	12	15	24	41

As previously mentioned, there was a 19.9% decrease in the overall number of SARs filed by reporting institutions during the reporting year, particularly by Trust and Company Services Providers. There were few differences in the reasons for filing these reports when compared to previous reporting years. Much like the previous years, the majority of reports submitted were linked to fraud and money laundering related offences. Though the number of SARs filed by TCSPs were lower than the previous year, they still accounted for the majority of SARs submitted followed by banking institutions.

Something of importance to note is that the number of SARs linked to issues related to non-compliance with certain aspects of Know Your Customer (KYC)/ Customer Due Diligence (CDD) requirements represents 13.1% of the total number of SARs reported

during the current reporting year. These particular SARs were all filed by TCSPs. This could indicate that some members of this sector are failing to fulfill their AML/CFT obligations, which has the potential to bring the territory's reputation into disrepute.

Chart 3: The pie chart below represents a breakdown of number of SARs filed by reporting institutions



Mutual Legal Assistance

The need for affective cooperation among countries is key to tackling transnational-crime. Cooperation should not be limited to investigation, prosecution and recovery of assets but should also provide the ability to conduct joint investigations and to transfer criminal proceeds between cooperating jurisdictions when necessary.

Police - to - police enquiries, known sometimes as Mutual Administrative Assistance, can be used to initiate enquiries abroad to trace assets in other jurisdictions. Such contacts, together with enquiries made via other law enforcement – to - law enforcement contact

such as through Interpol enable countries to discover whether Mutual Legal Assistance to further the investigation or recovery of assets is needed.

Mutual Legal Assistance is the provision of assistance on a formal legal basis, usually in the gathering and transmission of evidence, by an authority in one country to an authority in another, in response to a request for assistance. "Mutual" simply denotes the fact that assistance is usually given in the expectation that it would be reciprocated in like circumstances, although reciprocity is not always a precondition to the provision of assistance.

Mutual legal assistance is a vital tool that aids in the prosecution of criminals who perpetrate criminal activities that extend beyond the borders of individual countries. The Territory's mutual legal assistance regime is an important tool in its fight against crime, both foreign and domestic, including financial crimes. It remains a vital avenue through which the Territory continue to share information and evidence with foreign countries to assist in the prosecution of financial and other types of crimes.

During the year under review the agency received some sixty-two (62) Mutual Legal Assistance Requests. This represents a 264% increase relative to the number of Mutual Legal Assistance Requests received the previous year. These requests originated from twenty-three (23) different countries as indicated in the bar chart on the following page. The majority of these requests originated from the Russian Federation followed by the United Kingdom, Ukraine, and Australia. Much like the previous year, these requests were mainly linked to investigations and prosecutions of fraud and money laundering related offences. As is customary, these requests involved British Virgin Islands registered entities linked to alleged criminal activities in the requesting jurisdictions.

Table 3: Shows a breakdown of Mutual Legal Assistance Requests received between 2008-2011

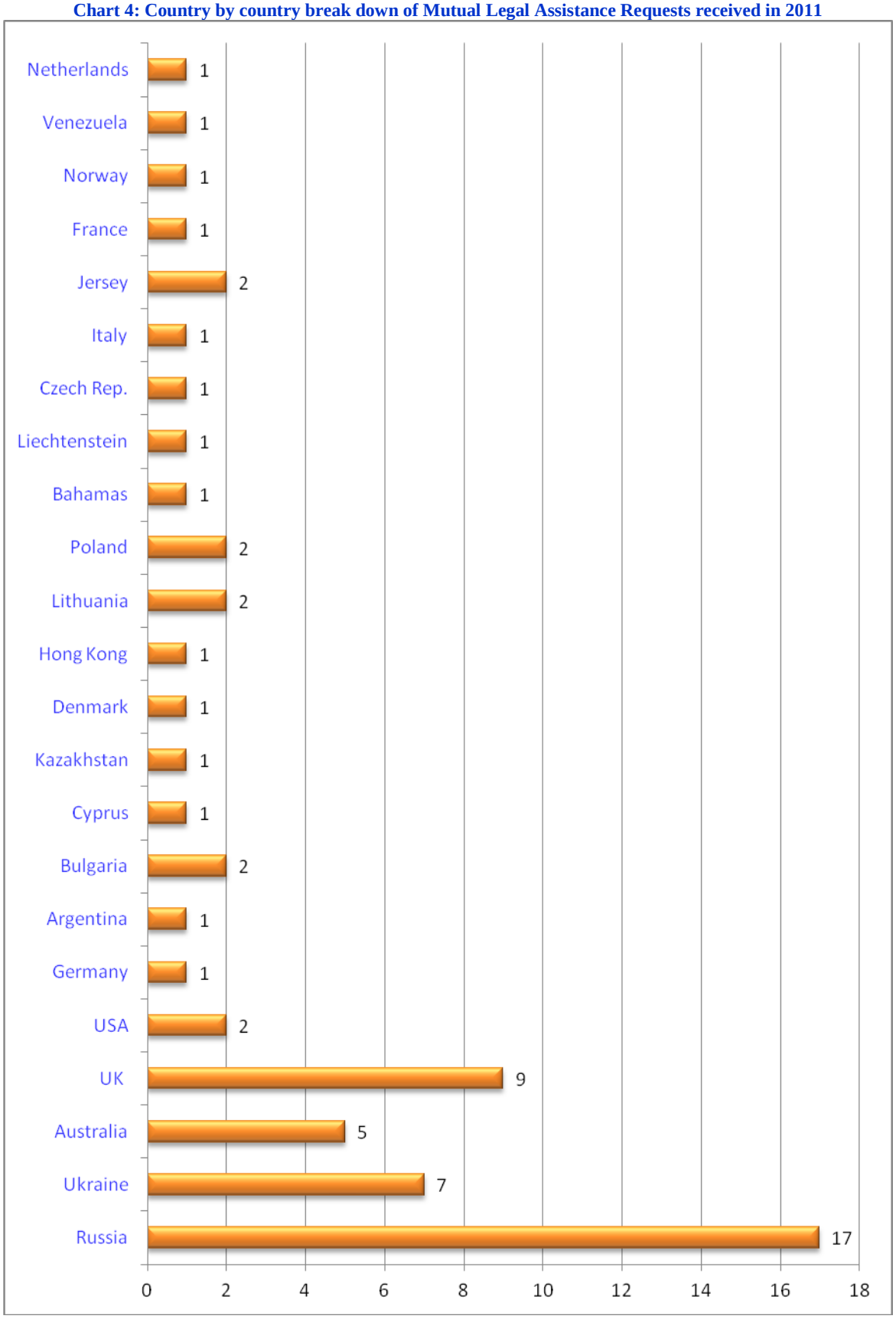
MLA Requests	2008	2009	2010	2011
	22	16	17	62

Table 4: Shows the a breakdown of Mutual Legal Assistance Requests received in 2011 categorized by types of offences

Fraud	Corruption	Money Laundering	Theft or Embezzlement	Illegal Smuggling of Goods	Drug Trafficking
35	5	19	7	4	1

Note: The majority of Mutual Legal Assistance Requests includes more than one offence

Chart 4: Country by country break down of Mutual Legal Assistance Requests received in 2011



Information Exchange

Exchange of information is relevant to an FIU's analytical functions. The Agency has developed clear processes and procedures to facilitate the exchange of information with its counterparts and always adheres to the Egmont Principles of Information Exchange. One of the fundamental principles of information exchange is the ability to exchange information/intelligence in a secure and timely manner. Confidentiality is of the utmost importance due to the sensitive nature of the information being handled, notably information contained in suspicious activity reports and other information that is relevant to law enforcement investigations. The majority of information exchange takes places between the Agency and its Egmont Group partners.

The Egmont Group

The Egmont Group is an international body made up of member financial intelligence units (FIUs), which are central, national agencies responsible for receiving, analyzing, and disseminating to, and as permitted, requesting from, the competent authority disclosures of financial information. FIUs play a key role in the global fight against money laundering, the financing of terrorism, and other financial crime by transforming financial transaction data into financial intelligence.

The Egmont Group was established in 1995 by fifteen (15) FIUs. It was established as an informal network for sharing information about money laundering. Since then, the Egmont Group has grown markedly and has evolved from an informal network into a formal, self-sustaining, internationally recognized entity consisting of one hundred and thirty-one members. The group's permanent Secretariat is located in Toronto, Canada. The Egmont Group's evolution has strengthened information exchanges and international cooperation to combat anti-money laundering and the financing of terrorism.

The BVI's then Financial Intelligence Unit became a member of the Egmont Group in 1998. The Agency now participates in the Outreach Working Group which is one of the five working groups that make up the Egmont Group. The Outreach Working Group seeks to expand membership in the Egmont Group by identifying candidates and FIU sponsors to work with them to ensure compliance with international standards. The Working Group also coordinates with other international organizations to promote outreach in those areas of the world which need increased attention and resources. In line with the strategic and operational significance of the sub-Saharan African region, the Outreach Working Group is currently working with regional and international partner

organizations to provide outreach, training, and development assistance to FIUs in that region.

The Legal Working Group aims to protect the FIU-specific character of the Egmont Group and to enhance the mutual cooperation and information exchange between FIUs. The Legal Working Group reviews the candidacy of potential members and handles all legal aspects and matters of principle within Egmont, including member compliance with Egmont Group standards.

The Operational Working Group seeks to bring FIUs together to work on cases and strategic projects. Current initiatives include an FIU information exchange project, a concept paper on the impact of the financial crisis on financial crime being developed in conjunction with the Wolfsberg Group of financial institutions, and a terrorist financing paper containing sanitized cases with red flags and indicators.

The Information Technology Working Group examines new software applications that might facilitate analytical work and focuses on such issues as data standards and security. The Group also works to enhance the capabilities of the Egmont Secure Web, the secure internet system used for FIU-to-FIU information exchange.

The Training Working Group identifies training needs and opportunities for FIU personnel and conducts training seminars for Egmont members and non-members. Training programs focus on areas of particular interest to Egmont members, including tactical analysis, mutual evaluation, and the recent strategic analysis course.

During the reporting year the agency recorded seven hundred and two (702) requests for information. Of these four hundred and twelve (412) resulted in the exchange of information with our foreign counterparts. The difference was shared with other international law enforcement agencies, the Financial Services Commission (FSC), HM Customs, and the Royal Virgin Islands Police Force (RVIPF).

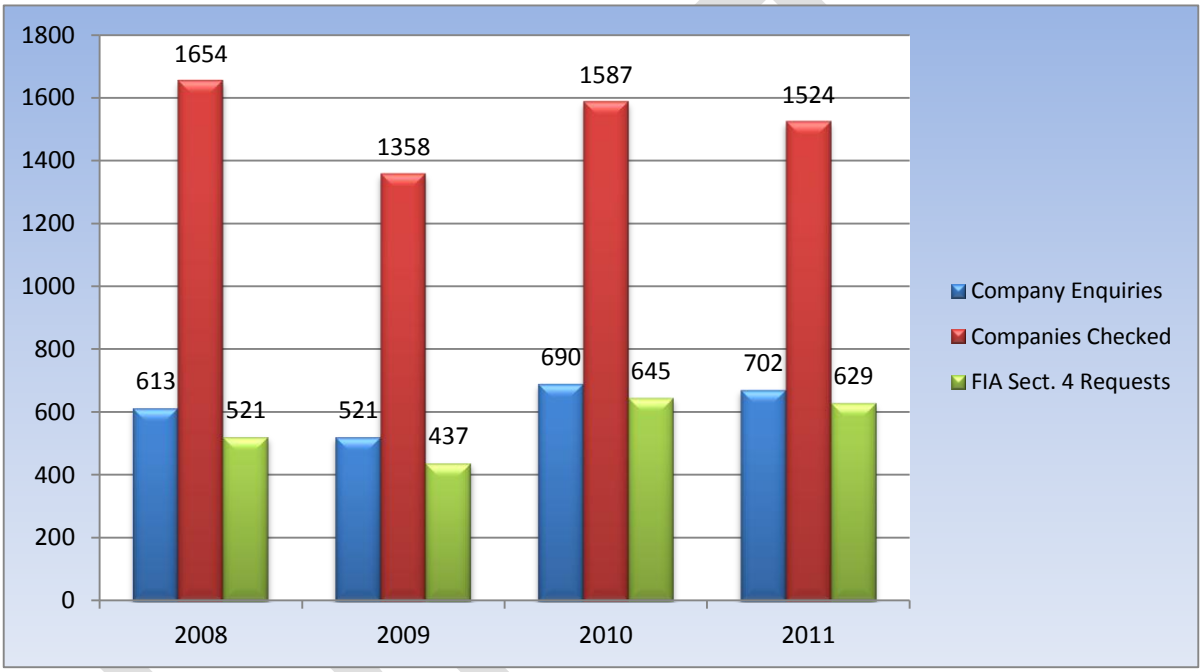
As previously indicated, the number of requests for information received during the current reporting year increased by a very small margin of 1.73% relative to the previous year. As a consequence, the FIA continues to process one of the highest numbers of requests for information when compared with its Egmont Group counterparts. The Agency sent only sixteen (16) requests to its foreign counterparts.

As a result, the Agency endeavors to increase the number of requests for information to its foreign counterparts. What this means is that the Agency will endeavor to process and

analyze SARs and other types of disclosures reported to the Agency in the shortest possible timeframe given that timely requests and dissemination of information is an essential requirement of an FIU.

Information sharing on a reciprocal basis is a necessary tool used by FIUs to support the work of law enforcement agencies in their fight to counter money laundering and terrorist financing. The statistics on requests for information received during the year in review can be seen in the following chart.

Chart 5: Shows the number of company enquiries, companies checked, and FIA requests for information sent to various reporting institutions between 2008 and 2011



Though the number of company enquiries increased slightly during the reporting year, there was a slight decline in the number of company checks and requests for information decreased when compared to the previous year. There was also a noticeable decline in the number of requests for information received from our domestic partner agencies, particularly the number of requests received from the FSC and RVIPF whereas the number of requests received from HM Customs remained relatively unchanged.

Enhancing International Cooperation

Section 4 (2) (h) of the FIA Act which guides our operations authorises the Agency to enter into arrangements with foreign financial investigation agencies for the purpose of sharing information linked to financial crimes. The Agency can share information with any foreign financial investigation agency outside of having any formal arrangements.

This means that the Agency can share information on the basis of reciprocity. However, such is not the case for some of our foreign counterparts whose domestic legislation makes it mandatory for them to have formal bilateral arrangements before they can share any information with foreign counterparts.

During the coming year, the Agency will continue building stronger relationships by negotiating and signing additional MOUs with its Egmont partners. These agreements would add to the growing number of MOUs that that are now in place. To date, the Agency has negotiated and entered into MOUs with the FIUs of Canada, Poland, the Russia Federation, the Republic of Moldova, Macedonia, Romania, Montenegro, and Australia. These MOUs were signed at the Egmont Group 19th Plenary meeting in Armenia in July of 2011.

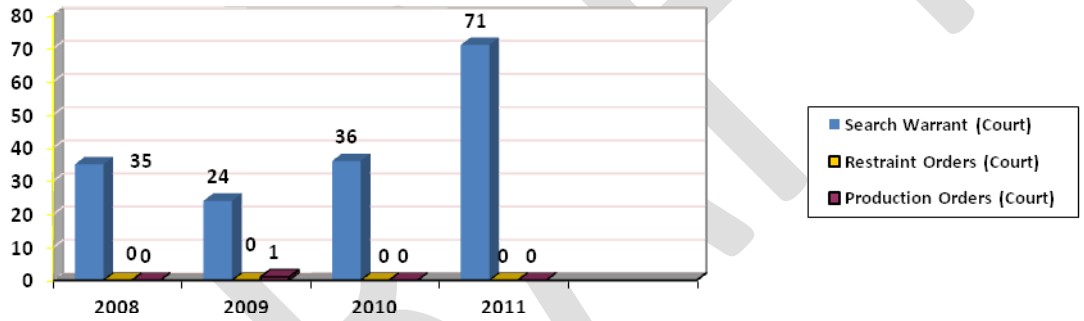
Table 5: Breakdown of requests for information received from domestic and foreign partners in 2011

Country	No. of Requests	Country	No. of Requests	Country	No. of Requests
BVI FSC *	60	RVIPF *	176 (obo Interpol)	HM Customs*	4
Hungary	1	Armenia	2	USVI	1
Australia	1	Norway	5	Slovakia	1
Bulgaria	3	Brazil	3	Hong Kong	3
Cyprus	4	Croatia	7	Belgium	19
Lebanon	3	France	17	Germany	7
Argentina	6	Anguilla	1	India	9
Lithuania	4	Ukraine	29	Hungary	1
Seychelles	2	Luxembourg	3	UK	13
Malta	4	Venezuela	3	Montenegro	16
Netherlands	1	Taiwan	1	Moldova	7
Portugal	3	Romania	5	Poland	2
South Africa	2	Spain	9	Russia	21
Turkey	1	USA	22	Serbia	1
Panama	5	Kazakhstan	2	Israel	1
South Africa	1	Mauritius	2	Liechtenstein	5
Belarus	5	Malta	4	Serbia	2
St. Vincent	4	Taiwan	1	Spain	22
Czech Rep.	22	Latvia	22	USA	22
Jersey	13	Bahrain	1	Cayman Is.	5
Indonesia	5	South Korea	2	Japan	1
Saudi Arabia	1	UAE	2	Jordan	2
Barbados	6	Peru	2	Turkmenistan	2
UN	2	Curacao	2	Singapore	2
San Marino	2	Georgia	8	Egypt	3
St. Kitts	2	Finland	1	Grenada	1
Italy	4				
TOTAL	**702**				

Search Warrants/Restraint Orders/Production Orders

Search warrants, restraint orders, and productions orders are usually generated as part of the mutual legal assistance process. These orders are obtained from the Magistrate Court or the High Court. Search warrants and production orders are used to lawfully seize documents and other useful material from persons and entities in whose possession such material is held. Restraint orders are used to prevent the disposal or removal of proceeds or suspected proceeds of criminal activities. Material is often used as evidence to assist with the investigations and prosecution of criminal offences taking place either within or outside the British Virgin Islands. While no restraint or production orders were recorded during the year under review, there was a 97.2% increase in the number of search warrants recorded relative to the previous year. This increase coincides with the unprecedented increase in the number of Mutual Legal Assistance Requests recorded and executed during the reporting year.

Chart 4: Shows the number of Search Warrants, Restraint Orders and Production Orders served between 2008 and 2011



Training Activities (Seminars and Workshops)

The Agency recognises that the promotion of compliance with the territory's ML and TF reporting regime through close interaction with reporting institutions is necessary. Apart from assisting financial institutions to be able to better identify suspicious or unusual financial activity, it helps them to improve the quality of their reporting. During the year, the Agency was able to meet with industry members on at least two occasions to discuss various AML/CFT related matters focusing on issues such as the role and powers of the Agency as the Territory's designated Reporting Authority and Financial Intelligence Unit, money laundering and terrorist financing indicators and SAR/STR reporting.

The Agency also believes in building organizational capability so that it would be better equipped to face the ever increasing challenges brought about by the changes and complexity of financial crimes. This is why training remains one of our top priorities. Training is vital to building competency. The following table contains data on training/outreach activities undertaken by the agency between 2008 and 2011.

Table 6- Training/Outreach Activities between 2008 and 2011

Training/Outreach	2008	2009	2010	2011
Domestic Outreach	3	2	1	2
International Training	7	4	7	10

Strengthening our IT infrastructure

The Agency continued its focus on strengthening its information technology capabilities during the year under review. During the year significant progress was made as we moved closer to completing the upgrades to our electronic information storage system. However, there is still some work to be done which we hope to complete during the coming year. Our desired outcome is to substantially enhance the efficiency and effectiveness of the Agency's data management capabilities.

Challenges

The challenges we faced during the year were primarily linked to two (2) main areas of concern.

1) The need to build capacity in order to be able to supervise and monitor the local Non-Profit sector and the Designated Non-Financial Businesses and Professionals (DNFBPs) operating in the territory.

While the Agency made some progress in this regard, there is still a great deal of work to be done before the framework to supervision and monitoring the DNFBP and NPO sectors. This will include the need for larger office space to accommodate the creation of a compliance unit which will undertake the responsibilities of supervising and monitoring the DNFBPs and NPOs.

2) The overall increase in workflow, particularly due to the unprecedented increase in the number of Mutual Legal Assistance Requests coupled with the high volume of requests for information emanating from our domestic and international partners made it very difficult to fulfill our goal to shorten our overall response time to request for information including requests for mutual legal assistance. This issue will be looked at more closely in the coming year when we undertake a full review of our international processes and procedures. Our aim will be to identify potential weaknesses and take the necessary corrective action.

Looking Ahead (strategic priorities for 2012)

Our focus during the coming year will be on the implementation of our Strategic Priorities outlined in our 2012 Work Plan. Though most of these initiatives would be implemented over the short term; many of them will be implemented on an ongoing basis.

Capacity Building

The FIA firmly believes that capacity building will be key to overcoming future challenges of money laundering and terrorist financing related criminal activities.

As a result, the Agency will focus on building capacity in five (5) main areas during the coming year 2012:

Building our Human Resources

The foundation of the FIA success is a competent staff. To this end, the Agency will dedicate a significant portion of its financial resources in the coming year to further train and develop the competences of each staff member in their individual area of expertise. This will include the recruitment and training of personnel to staff the new compliance unit.

Outreach/Public Awareness

The significance of public participation in the prevention of ML and TF could play an important role in helping to ensure that persons do not unwittingly take part in ML and TF related activities. To this end the Agency will work closely with the FSC and the Police to raise public awareness through education and training seminars. This will be done on an ongoing basis and will involve local print and electronic media.

Strengthening Domestic Partnerships

The Agency has a strong working relationship with the FSC and the Royal Virgin Islands Police Financial Investigations Unit and holds regular meetings to discuss pertinent issues and offer feedback on ongoing enquiries. One of our goals in the coming year is to strengthen this relationship by improving the direct flow of information among our three agencies.

International Cooperation (strengthening our international relationships)

As indicated earlier, the Agency has a close working relationship with its partners in the Egmont Group. During the coming year we will seek to strengthen our cooperation with our Egmont Group partners through direct information sharing agreements (MOUs). This will form an important part of our global outreach strategy aimed at strengthening relationships with our international partners.

Improving our IT Infrastructure

Development of the agency's IT infrastructure will take place on an ongoing basis. This will include the purchase of additional computer hardware to complete our offsite back-up system, and the purchase of additional software to protect the integrity of the sensitive information held in the Agency's database. These additional measures will form part of a comprehensive plan to develop and install a secure online system to facilitate electronic reporting of SARs by financial and other reporting institutions.

Glossary

AGC-	Attorney General Chambers
AML-	Anti-Money Laundering
BVIBC-	British Virgin Islands Business Company
CFATF-	Caribbean Financial Action Task Force
CFT-	Counter Financing of Terrorism
DNFBPs-	Designated Non-Financial Businesses and Professions
DPP-	Director of Public Prosecutions
FATF-	Financial Action Task Force
FIAA-	Financial Investigation Agency Act
FIU-	Financial Intelligence Unit
FSC-	Financial Services Commission
JALTFAC	Joint Anti-Money Laundering and Terrorist Financing Advisory Committee
INTERPOL-	International Criminal Police Organization
LOR-	Letter of Request
POCCA-	Proceeds of Criminal Conduct Act
MLA	Mutual Legal Assistance
SAR-	Suspicious Activity Report
STR-	Suspicious Transaction Report
TCSP-	Trust and Company Services Provider

Appendix 1- ML Typologies

The FATF requires FIUs to periodically publish typologies relating to money laundering and the financing of terrorist activities and more recently emphasis has been placed on corruption of public officials (PEPs) due to the ML risk they pose by virtue of their position The following cases are extracts of SARs and other types of cases handled by the Agency during the reporting year 2011.

Typologies Case examples (2011)

Case # 1

Use of Corporate Structures by a corrupt foreign public official

Mr. W. held the post of Director General in a Government Ministry in an Eastern European country. During his time as Director General he was responsible for overseeing the privatization of a state owned company by a foreign entity from Ireland. Using his position as a state official, he forced the representative of the Irish entity to pay a bribe of USD 1 million prior to the acquisition of shares in the state owned company. The bribes were allegedly funneled through a BVI Business Company.

Outcome: Valuable information and evidence was provided by the FIA via the BVI Mutual Legal Assistance process to the prosecuting authorities in the Eastern European country to assist with the investigation and prosecution of the PEP. No feedback in reference to this matter has been provided to date.

Case # 2

Use of fraudulent bearer negotiable instruments

Ms. E. opened a savings account at A LOCAL bank on April 28, 2011 to accommodate her earnings from her place of employment where she was employed as a scuba diver. On her application she stated that deposits into her account would be somewhere in the range of USD 1500.00 monthly.

On September 14, 2011 she deposited a check in the amount of USD 9,354.21 from a company by the name of Austin Powder Ltd. which was drawn on JP Morgan Chase in Canada. However, the check was subsequently returned to the bank as fraudulent/counterfeit.

When questioned by bank officials Ms. E. stated that she answered a work from home ad in a local newspaper and subsequently received the check which she deposited to her

account. She was later instructed by an unknown gentleman to keep USD 3,354.21 for herself as a deposit and return USD 6,000.00 via Money Gram back to him. The transaction resulted in Ms. E. bank account being overdrawn.

Outcome: The intelligence was shared with local law enforcement authorities

Case # 3

Use of Corporate Vehicles to hide assets purchased with the proceeds of corruption

The Agency received an SAR concerning Mr. Q, a Politically Exposed Person (PEP) from Libya who was subject to international sanctions. The SAR alleged that Mr. Q was the beneficial owner of a BVI registered offshore entity which held a residential property in the UK said to be worth several million pounds. The assets were allegedly purchased with state funds.

FIA analysis confirmed that the BVI registered entity was in fact owned by Mr. Q. as alleged in the SAR. This information was shared with our counterparts in the UK.

Outcome: The property was subsequently seized and returned to the Libyan people.

Money Laundering Indicators

The following are examples of transactions which may give rise to suspicion, which in turn should prompt relevant institutions to consider filing a suspicious or unusual transaction report with the FIA in accordance with the relevant sections of the Proceeds of Criminal Conduct Act, 1997 (as amended) and the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008. A number of these examples or similar examples are included in Schedule 1 (Section 56) of the AML/CFT Code of Practice, 2008.

These indicators/red flags are based on internationally accepted AML/CFT guidelines and publications issued by internationally recognized bodies such as the FATF.

Banks

Deposit Accounts

The following is a list of various transactions and activities that may indicate potential money laundering. While not all-inclusive, the list does reflect ways that launderers have been known to operate, though they may not necessarily be indicative of money laundering if they are proven to be consistent with a customer's legitimate business activities.

1. **Minimal, vague or fictitious information provided**. An individual provides minimal, vague or fictitious information that the bank cannot readily verify.

2. **Lack of references or identification.** An individual attempts to open an account without references or identification, gives sketchy information, or refuses to provide the information needed by the bank.

3. **Non-local address**. The individual does not have a local residential or business address, and there is no apparent legitimate reason for opening an account with the bank.

4. **Customers with multiple accounts.** A customer maintains multiple accounts at a bank or at different banks for no apparent legitimate reason. The accounts may be in the same names or in different names with different signature authorities. Inter-account transfers are evidence of common control.

5. **Frequent deposits or withdrawals with no apparent business source**. The customer frequently deposits or withdraws large amounts of currency with no apparent business source, or the business is of a type not known to generate substantial amounts of currency.

6. **Multiple accounts with numerous deposits under the legally prescribed threshold**. An individual or group opens a number of accounts under one or more names, and makes numerous

cash deposits just below the legally prescribed threshold, or deposits containing bank checks or traveler's checks.

7. **Numerous deposits under institution's prescribed threshold in a short period of time**. A customer makes numerous deposits under prescribed threshold amount in an account in short periods of time, thereby avoiding the requirement to file an SAR. This includes deposits made at an ATM.

8. **Accounts with a high volume of activity and low balances**. Accounts with a high volume of activity, which carry low balances or are frequently overdrawn, may be indicative of money laundering or check kiting.

9. **Large deposits and balances.** A customer makes large deposits and maintains large balances with little or no apparent justification.

10. **Deposits and immediate requests for wire transfers or cash shipments**. A customer makes numerous deposits in an account and almost immediately requests wire transfers or a cash shipment from that account to another account, possibly in another country. These transactions are not consistent with the customer's legitimate business needs. Normally, only a token amount remains in the original account.

11. **Numerous deposits of small incoming wires or monetary instruments, followed by a large outgoing wire**. Numerous small incoming wires and/or multiple monetary instruments are deposited into an account. The customer then requests a large outgoing wire transfer to another institution or country.

12. **Accounts used as a temporary repository for funds.** The customer appears to use an account as a temporary repository for funds that ultimately will be transferred out of the bank, sometimes to foreign-based accounts. There is little account activity.

13. **Disbursement of certificates of deposit by multiple bank checks.** A customer may request disbursement of the proceeds of a certificate of deposit or other investments in multiple bank checks, each under prescribed threshold amount. The customer can then negotiate these checks elsewhere for currency. He/she avoids the transaction reporting requirements and eliminates the paper trail.

14. **Early redemption of certificates of deposits**. A customer may request early redemption of certificates of deposit or other investments within a relatively short period of time from the purchase date of the certificate of deposit or investment. The customer may be willing to lose interest and incur penalties as a result of the early redemption.

15. **Sudden, unexplained increase in account activity or balance**. There may be a sudden, unexplained increase in account activity, both from cash and from non-cash items. An account may be opened with a nominal balance that subsequently increases rapidly and significantly.

Wire Transfers

This document lists various transactions and activities that may indicate potential money laundering. While not all-inclusive, the list does reflect ways that launderers have been known to operate. Transactions or activities listed here may not necessarily be indicative of money laundering if they are consistent with a customer's legitimate business. Also, many of the "indicators" involve more than one type of transaction.

1. **Wire transfer to countries with bank secrecy legislation**. Transfers to well known "bank secrecy jurisdictions."

2. **Incoming/Outgoing wire transfers with instructions to pay upon proper identification**. The instructions to the receiving bank are to "pay upon proper identification." If paid for in cash, the amount may be just under the prescribed threshold amount so no SAR is required. The purchase may be made with numerous official checks or other monetary instruments. The amount of the transfer may be large, or the funds may be sent to a foreign country.

3. **Outgoing wire transfers requested by non-account holders.** If paid in cash, the amount may be just under prescribed threshold amount to avoid a SAR. Alternatively, the transfer may be paid with several official checks or other monetary instruments. The funds may be directed to a foreign country.

4. **Frequent wire transfers with no apparent business reason**. A customer's frequent wire transfer activity is not justified by the nature of their business.

5. **High volume of wire transfers with low account balances.** The customer requests a high volume of incoming and outgoing wire transfers but maintains low or overdrawn account balances.

6. **Incoming and outgoing wires in similar dollar amounts**. There is a pattern of wire customers, on the same day or next day. The customer may receive many small incoming wires, and then order a large outgoing wire transfer to another city or country.

7. **Large wires by customers operating a cash business**. Could involve wire transfers by customers operating a mainly cash business. The customers may be depositing large amounts of currency.

8. **Cash or bearer instruments used to fund wire transfers**. Use of cash or bearer instruments to fund wire transfers may indicate money laundering.

9. **International funds transfer which are not consistent with the customer's business**. International transfers, to or from the accounts of domestic customers, in amounts or with a frequency that is inconsistent with the nature of the customer's known legitimate business activities could indicate money laundering.

10. **Other unusual domestic or international fund transfers.** The customer requests an outgoing wire or is the beneficiary of an incoming wire, and the instructions appear inconsistent with normal wire transfer practices. For example: The customer directs the bank to wire the

funds to a foreign country and advises the bank to expect same day return of funds from sources different than the beneficiary named, thereby changing the source of the funds.

12. **No change in form of currency.** Funds or proceeds of a cash deposit may be wired to another country without changing the form of currency.

13. **Limited use of services.** Frequent large cash deposits are made by a corporate customer, who maintains high balances but does not use the bank's other services.

14. **Inconsistent deposit and withdrawal activity.** Retail businesses may deposit numerous checks, but there will rarely be withdrawals for daily operations.

Insurance and Insurance Products

The following examples may be indicators of a suspicious transaction and give rise to a transaction report.

1. Application for business outside the policyholder's normal pattern of business.

2. Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal activity (e.g. drug trafficking or terrorist activity) or corruption is prevalent.

3. Any want of information or delay in the provision of information to enable verification to be completed.

4. An atypical incidence of pre-payment of insurance premiums.

5. Insurance policies with premiums that exceed the client's apparent means.

6. Insurance policies with values that appear to be inconsistent with the client's insurance needs.

7. Any transaction involving an undisclosed party.

8. Early termination of a product, especially at a loss, or where cash was tendered and/or the refund check is issued to a third party.

9. A transfer of the benefit of a product to an apparently unrelated third party.

10. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).

11. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder.

12. The applicant for insurance business appears to have policies with several institutions.

Designated Non-financial Businesses and Professions (DNFBP's)

Real Estate Agents

The following is an example of how real estate agents can be utilized to assist in a money laundering operations.

1. Engaging in a series of transactions designed to conceal the illicit source of funds; these transactions may be classified as part of the layering stage.

2. Investing in tourism related activities so as to acquire a legitimate appearance and conceal the origin of the tainted money used to acquire or purchase the property.

3. Buying and selling real estate properties using fictitious names.

Dealers in precious stones and metals

The risks of money launderers misusing the dealers in precious stones and metals are largely due to the fact that precious metals, particularly gold, attracts money launderers, as it has a high actual value and can be found in relatively small sizes, thus facilitating its transport, purchase and sale in several regions around the world. The value of gold tends to remain the same regardless of its form, whether it comes in the form of bullions or golden articles. Dealers are often interested in gold more than gems because it can be melted to change its form while preserving its value.

Diamonds can also be traded around the world easily as the small size of diamond stones and their high value facilitate their concealment and transport and make it one of the most gems and jewels with the risk of being misused as a means to launder money. Diamonds have also been used as a means to finance terrorism.

Gold is used in money laundering operations whether it is acquired in an illicit manner (like theft or smuggling) where it constitutes proceeds of a crime and is therefore deemed to be an illicit fund, or is used to launder money through the purchase of gold against Illicit funds.

Lawyers and Accountants

The potential for criminals and would-be criminals to use the services and products offered by these professionals are real and so are the risks. The following are examples of the types of services that may be misused to facilitate money laundering activities.

1. Establishment of companies or other complex legal arrangements (like trusts), as such services may conceal the link between the proceeds of the crimes and the criminals.

2. Buying and selling of real estate, as the transfer of the real estate ownership is used to cover the illicit funds transfer (layering phase of money laundering or the final investment of the proceeds passed through laundering operations (integration stage).

3. Execution of financial operations on behalf of customers, like cash deposit or withdrawal, foreign currency exchange operations, sale and purchase of shares, sending and receiving international money transfers.

4. Filing of fictitious lawsuits to obtain a judgment to legitimize the funds.

BLANK PAGE

Appendix 4- Financials Reports 2011 (pages 1-15)