Financial Investigation Agency

Annual Report 2009

BRITISH VIRGIN ISLANDS

BRITISH VIRGIN ISLANDS

FINANCIAL INVESTIGATION AGENCY

P.O. Box 4090, Pasea Estate, Road Town, Tortola, British Virgin Islands
Tel: (284) 494-1335 ***Fax:*** (284) 494-1435
Email: fia@bvifia.org

February 23, 2011

The Deputy Governor, Mrs. Inez Archibald
Chairman of the Board, Financial Investigation Agency
Deputy Governor's Office
Road Town, Tortola
British Virgin Islands

Dear Chairman:

Pursuant to section 11 (1) (b) of the ***Financial Investigation Agency Act,*** I am pleased to present you with the sixth annual report for the Financial Investigation Act of the British Virgin Islands. The report contains details of our work during the year, the challenges we faced, and our priority areas going forward into the new year.

We will continue in our efforts to prevent financial crimes from taking a foot hold within the Territory's financial services sector.

Yours sincerely,

Errol George
Director

Director's review

The Agency was formed in 2004 as part of the Territory's international obligations to fight against financial crime, particularly those linked to Money Laundering and the Financing of Terrorist activities. The Agency is a statutory body and its core functions are contained in section 4 of the Financial Investigation Agency Act, 2003.

Since its formation, the Agency has collaborated with its domestic regulatory and law enforcement agencies in an effort to reduce to the extent to which it is possible the use of the many products offered by the various regulated businesses within the Territory from being used by local and internal criminal enterprises to perpetrate financial crime.

During the past year, the Agency received and processed more Suspicious Activities Reports than it has since its formation in 2004. This increase we believe is attributed in part to increased vigilance undertaken by the reporting sector in an effort to fulfill their reporting obligations. We wish to impress upon the industry the need to maintain this vigilance as there will always be criminal elements seeking to exploit weaknesses in the global financial services system.

The Agency has long recognized the important role it plays in assisting international efforts to counter money laundering and the financing of terrorist related activities. To this end, we undertook several inquiries received from our international partner agencies worldwide and responded to over five hundred (500) requests for information on British Virgin Islands registered business companies. We also processed several request for mutual Legal assistance and were able to provide valuable material to the requesting authorities to assist with prosecuting various financial offences in their respective countries.

We also continued our participation in the important work undertaken by regional and international organizations such as the Caribbean Financial Action Task Force (CFATF) and the Egmont Group of Financial Intelligence, and attended several of their meetings which were held throughout the year.

The work undertaken by the Agency over the past year and during the time of its existence is testament to the hard work and dedication of its present staff, the level of cooperation with its partner agencies and its collaboration with the regulated sector. I express to them my gratitude.

In this context, it is also fitting to recognize the important contribution of the Agency's Board and Steering Committee. Without them we would not have been able to achieve the things we did over the past year. I wish to thank them and look forward to their continued support going forward.

Looking ahead we anticipate a great deal of changes in the coming year as we focus on building a stronger Agency. We hope to achieve this by increasing our resources. To this end, we will focus on ensuring that our new office space is prepared in the shortest possible timeframe.

Equally, we will focus on providing our staff with the tools that will be vital if we are improve our level of output in the coming year.

Our goal going forward is to achieve greater success while maintaining the high standards. We will also build on our reputation as we strengthen the expanded role of the Agency as the Territory's designated Financial Intelligence Unit.

Errol George
Director

Reader's guide

This annual report which covers the period January 1st to December 31st 2009 is meant to inform the Cabinet, House of Assembly, key stakeholders, and the general public about the performance of the Financial Investigation Agency against the priorities which were set coming into the year 2009.

It also serves to highlight the important role the Agency plays in helping the Territory to fulfill its international obligations while adhering to global Anti-money laundering and Counter Financing of Terrorism standards which are set by regional and international organizations such as the Caribbean Financial Action Task Force (CFATF), the Financial Action Task Force (FATF), the Egmont Group of Financial Intelligence Units, and other organisations which continue to play a major role in the international efforts to counter the devastating effects these and other related crimes could have on the global economy should they be allowed to take root.

Introduction

The introductory section includes a review by the Director, which summarises the major achievements and the work undertaken by the Agency during the year. It also gives a summary of the plans and priorities areas going forward into the year 2010.

Overview

The overview provides information about the role and function of the Agency, the organisational structure, and the main highlights for the reporting period.

Performance reporting (Statistical data)

This section features various charts and graphs reflecting input, output, and trends of the Agency during the year.

Appendixes

The appendixes provide information about money laundering typologies using a number of cases referred to the Agency by regulated institutions during the year under review.

The appendixes also include money laundering and terrorist financing indicators specific to the various products and services offered within the Territory's Financial Services Sector.

Financial accountability

This section features the financial statement reflecting the Agencies financial performance during the year. This is in keeping with section 14 (1) of the Financial Investigation Agency Act, 2003 (FIAA).

Other features

A glossary of terms/acronyms has also been included to assist readers.

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 financial 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, it 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 the strategies aimed at countering 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 the sector regarding their reporting obligations under the Proceeds of Criminal Conduct Act, 1997.
- Recognising 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 dedicate a great deal of its financial resources to ensure that staff members receive the necessary training to equip them with the knowledge and skills to perform effectively in their roles.

Governance

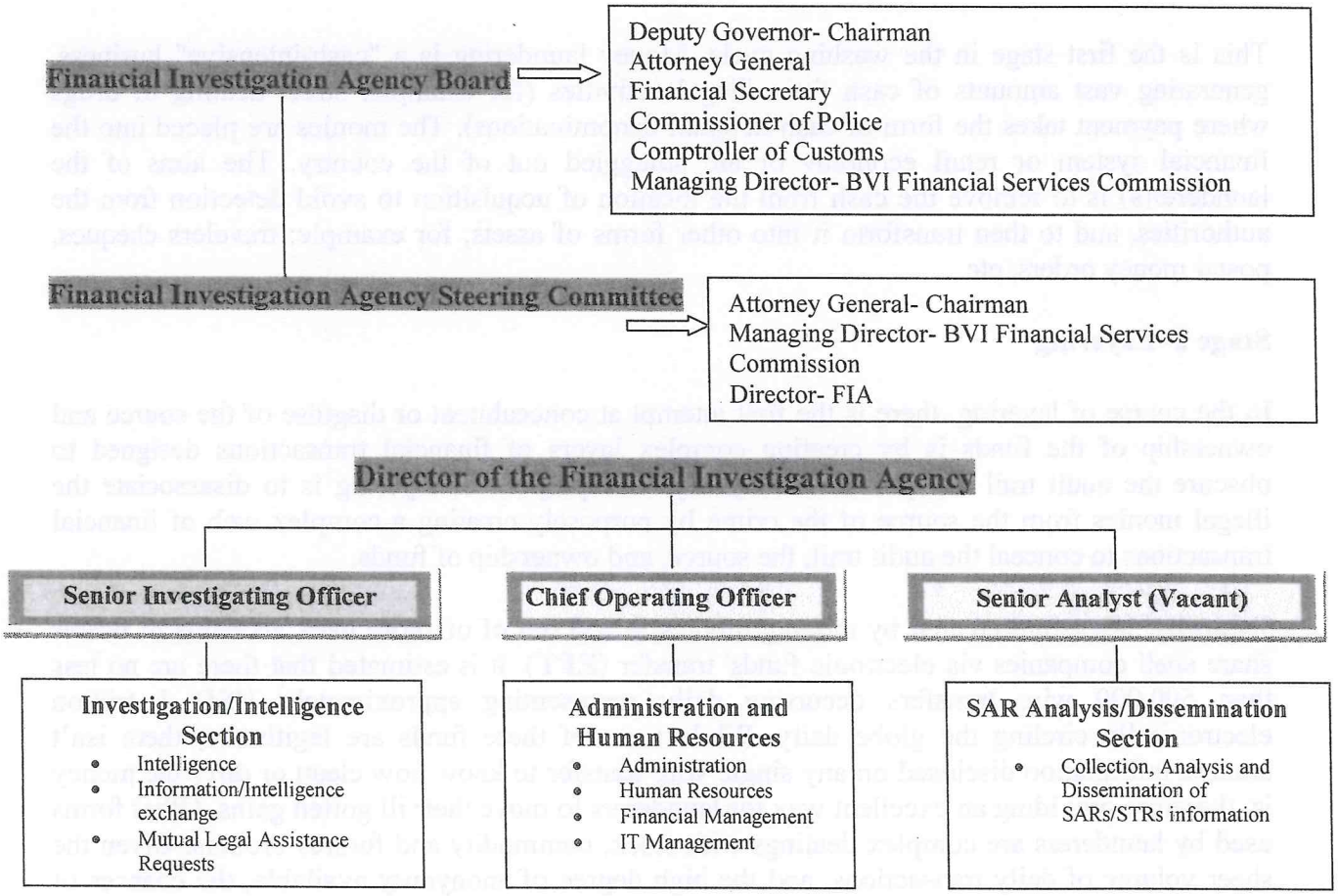
Section 3 (1) (b) of the FIA Act creates a policy making Board which is charged with oversight of the Agency. The Members of the board include the following:

- Deputy Governor (Chairman)
- Attorney General
- Financial Secretary
- Managing Director/CEO Financial Services Commission
- Comptroller of Customs
- Commissioner of Police

Section 3 (1) (3) of the FIAA provides for a Steering Committee, which is charged with the responsibility of guiding the course of investigations linked to SARs. This Committee comprises of the following:

- The Honourable Attorney General (Chairman)
- Managing Director/CEO of the Financial Services Commission
- Director, FIA

Figure-1 FIA Structure



Our legal framework

The Agency's functions are supported by the following pieces of legislation:

The Financial Investigation Act 2003 (as amended)
The Proceed of Criminal Conduct Act, 1997 (as amended)
The Drugs Trafficking Offences Act, 1992 (as amended)
The Anti-money Laundering Regulations, 2008
The Anti-money Laundering and Terrorist Financing Code of Practice, 2008
The Proliferation Financing (Prohibition) Act, 2009

The BVIs AML/CFT Regime

Money Laundering defined

Money Laundering is defined as "the process by which criminal disguise the true origin of their wealth which is derived from criminal activity."

Stages of the Money laundering process

Stage 1- Placement

This is the first stage in the washing cycle. Money laundering is a "cash-intensive" business, generating vast amounts of cash from illegal activities (for example, street dealing of drugs where payment takes the form of cash in small denominations). The monies are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderer(s) is to remove the cash from the location of acquisition to avoid detection from the authorities, and to then transform it into other forms of assets; for example: travelers cheques, postal money orders, etc.

Stage 2- Layering

In the course of layering, there is the first attempt at concealment or disguise of the source and ownership of the funds is by creating complex layers of financial transactions designed to obscure the audit trail and provide anonymity. The purpose of layering is to disassociate the illegal monies from the source of the crime by purposely creating a complex web of financial transactions to conceal the audit trail, the source, and ownership of funds.

Typically, layers are created by moving monies in and out of offshore bank accounts of bearer share shell companies via electronic funds' transfer (**EFT**). It is estimated that there are no less than 500,000 wire transfers occurring daily representing approximately USD 1 trillion electronically circling the globe daily. While most of these funds are legitimate, there isn't enough information disclosed on any single wire transfer to know how clean or dirty the money is, therefore providing an excellent way for launderers to move their ill gotten gains. Other forms used by launderers are complex dealings with stock, commodity and futures brokers. Given the sheer volume of daily transactions, and the high degree of anonymity available, the chances of transactions being traced is low.

Stage 3- Integration

The integration stage is the final stage in the process. This is the stage where the money is integrated into the legitimate economic and financial system and is assimilated 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 what is legal and what is not.

Methods popular to money launderers at this stage of the game are:

(i) the establishment of anonymous companies in countries where the right to secrecy is guaranteed. They are then able to grant themselves loans out of the laundered money in the course of a future legal transaction. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.

(ii) the sending of false export-import invoices overvaluing goods allows the launderer to move money from one company and country to another with the invoices serving to verify the origin of the monies placed with financial institutions.

(iii) a simpler method is to transfer the money (via EFT) to a legitimate bank from an offshore bank owned by the launderers.

Criminalization of Money Laundering in the BVIs

Money laundering was criminalized under the Proceeds of Criminal Conduct Act, 1997 (POCCA) and the Drug Trafficking Offences Act, 1992 (DTOA). ML offences include receiving, possessing, concealing, disposing of, importing or exporting, proceeds of criminal conduct. The physical and material elements of the ML offence include all aspects of the relevant Conventions with the exception of certain controlled drugs as required by the Vienna Convention.

The offence of ML extends to any type of property and applies to persons who commit the predicate offence. Criminal liability extends to legal persons and proof of knowledge can be drawn from objective circumstances. The low number of ML prosecutions suggests a limited implementation of the legal framework.

Criminalization of Terrorist Financing

Terrorist financing is criminalized in accordance with the TF Convention in the Terrorism (United Nations Measures) (Overseas Territories) Order 2001(U.K. S.I. 2001 No. 3366) (TUNMOTO), the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002, (U.K.S.I No. 2002 No. 1822) (ATFOMOTO) and the Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 (ATUNMOTO). These were extended to the British Virgin Islands by the United Kingdom Government.

The components of the terrorist financing offence capture funding for individual terrorists or terrorist organizations. Funds are defined in accordance with the provisions of TF Convention. A range of secondary offences are covered, terrorist financing offences are predicate offences for ML and objective factual circumstances may be used to prove intent. Both natural and legal persons are subject to criminal sanctions.

There is no evidence to substantiate the existence of terrorists or terrorist related activities occurring in the Territory of the British Virgin Islands and to-date the FIA received no SARs relating to possible cases of terrorist financing.

Provision is made for confiscation, freezing and seizing of the proceeds of crime under the POCCA, the DTOA, the ATFOMOTO and the TUNMOTO. Confiscation of instrumentalities used in or intended for use in the commission of ML or other predicate offences is allowed.

Financing the Proliferation of the Weapons of Mass Destruction

Financing the Proliferation of weapons of Mass Destruction is criminalized under the Proliferation Financing (Prohibition) Act, 2009. The enact empowers the FIA to take action against persons and activities that may have some connection to terrorist financing, money laundering, and the development of weapons of mass destruction and other related matters. This includes giving directions to any particular person or description or class of persons or all persons operating in the financial sector if certain conditions are met. These conditions include

- Where the UN Security Council or the FTAF have issued advisories that certain measures should be adopted in relation to as specific country on account of the risks that of terrorist financing or money laundering activities are being carried on in that country, whether by the government of the country or by persons resident in that country.

- When the FIA reasonably believes that there is a risk that terrorist financing or money laundering activities are taking place in such a country or by the government of the country or persons resident therein which poses a significant threat to the interest of the Territory;

- Where the FIA reasonably believes that the development or production of weapons of mass destruction in that country or anything that facilitates such development or production poses a significant risk to the interest of the Territory.

Introduction

Tremendous changes are now being witnessed as financial institutions in the many financial sectors across the globe redesign and implement AML/CFT policies in the wake of the 2007 financial meltdown.

It has been established that unsound financial systems are clearly safe havens for criminal activities. When financial systems are not transparent, regulations are not well established, and monitoring is lax, then opportunities for criminal activities, especially ML/TF thrive.

The British Virgin Islands takes seriously its obligations to do what is necessary to prevent financial crimes from taking root in its financial services sector, which is a key pillar of its economic sector and growth. Among the many steps taken by the Territory to fulfill these

obligations over the last decade was the introduction of new laws and regulations aimed at strengthening its AML/CFT framework.

During the late 1980's moving into the 1990's, many countries saw the need to create specialized government agencies referred to as Financial Intelligence Units or (FIUs). These units now exist in almost every country where AML/CFT laws exists, and are key components in global fight against ML and TF. FIUs provides a vital link between the financial services sector and law enforcement agencies by helping to identify suspicious financial transactions that could be linked to money laundering or the financing of terrorist activities.

FIUs are defined as "a central, national agencies responsible for receiving, and, as permitted, requesting, analyzing and disseminating to competent authorities, disclosures of financial information concerning suspected proceeds of crime and potential financing of terrorism, or required by national legislation or regulation in order to combat money laundering and the financing of terrorism".

The ability of FIUs to transform financial data into financial intelligence which is useful in helping to detect financial crimes means they play a pivotal role in the global fight against money laundering, terrorist financing, and other types of financial crime. FIUs also provide an avenue through which financial information can be shared on a domestic and international level.

The Financial Investigation Agency is the Financial Intelligence Unit of the British Virgin Islands. The Agency receives Suspicious Activity Reports from regulated institutions within the Territory's financial services sector. The Agency also receives information from various other sources.

Information coming into the Agency, including information provided in Suspicious Activity Reports is analysed in an effort to identify current or emerging money laundering patterns. This type of information is useful as it can determine whether a change in strategy is needed to counter new and emerging threats.

As predicted, there was an increase in the number of SARs filed in 2009 when compared to the number of reports filed during the previous year. A total of 227 reports were filed in 2009 representing a 50% increase over the previous year.

Suspicious Activities reporting

Suspicious Activity Reports (SARs) are filed by financial institutions subject to Money Laundering and Terrorist Financing reporting requirements. These reports are submitted to the Reporting Authority of the British Virgin Islands. SARs play vital role in assisting law enforcement to initiate and supplement money laundering or terrorist financing investigations and other criminal cases. The information submitted in SARs is also useful in helping the Financial Investigation Agency to identify new methods, trends and patterns associated with financial crimes.

Who reports suspicious activity

SARs can start with anyone at a bank, from a teller to a back office clerk to a manager. They are generally trained to be alert for suspicious activity, such as people trying to wire money out of the country without producing the required identification, or a customer who suddenly starts depositing large sums of cash which is considered to be above what is normally deposited. It is a requirement for financial institutions to provide employees with the necessary training to identify suspicious activities. Once an employee identifies a suspicious activity, he or she is usually required to bring that suspicion to the attention of the appropriate person(s) who would then make the decision whether to file a report or not.

Institutions that are legally required to file SARs

The law requires many different types of businesses or institutions who deal directly with financial transactions to file SARs. There is a general SAR form which was designed to accommodate the different types of businesses or institutions. These businesses and institutions include banks or deposit taking depository institutions, Trusts and Company Services Providers (TCSPs), money services businesses (MSBs), legal practitioners, real estate companies, automotive dealers, jewelry stores, and non-profit organisations.

When is a SAR filed?

A Suspicious Activity Report is filed when there is reasonable ground to suspect that a particular activity or financial transaction is linked to money laundering, terrorist financing or other criminal activity.

Structure of SAR reports

SARs normally include detailed information about financial transactions or activities that are suspicious in nature. In addition to what was stated earlier, SARs also assist relevant law enforcement agencies to identify persons, groups and organisations either involved or suspected to be involved in criminal activities including fraud, terrorist financing, money laundering, and other serious crimes.

Keeping SARs confidential

Disclosure of SAR information without authorisation is a criminal offense contrary to the proceeds of Criminal Conduct Act, 1997. In other words, an 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 not anyone else, including the customer who is under suspicion. The fact that a SAR has been filed is required to be kept confidential.

An individual or organisation is precluded from discovering the existence of a SAR filed that includes their name. 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 and/or attorneys or other trained professionals prior to filing.

Filing SARs with the Reporting Authority

SARs can be sent to the Reporting Authority either electronically to reportingauthority@bvifia.org or in hard copy format. Our vision is to develop a more comprehensive electronic-reporting system via our secure website.

Penalties for non-compliance or failure to report suspicious activity

Financial institutions and their employees face civil and criminal penalties for failing to report Suspicious Financial Activity including fines, imprisonment or both.

The Agency received a total of 227 SARs during the year under review compared to 151 reports received the previous year which represents a 50.3% increase. Of these, one hundred and twenty (120) were recorded as proactive reports, while the remaining 31 were recorded as reactive. These figures are in comparison with 110 reactive reports received in 2007.

Chart 1- Shows a monthly break down of SARs filed for 2009

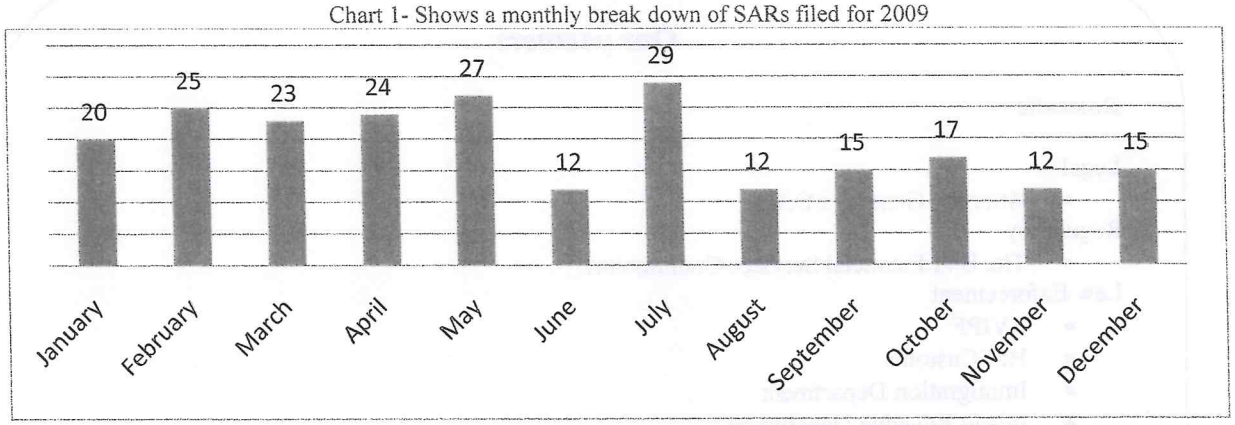


Chart 2: Shows the number of SARs received between the periods 2006-2009

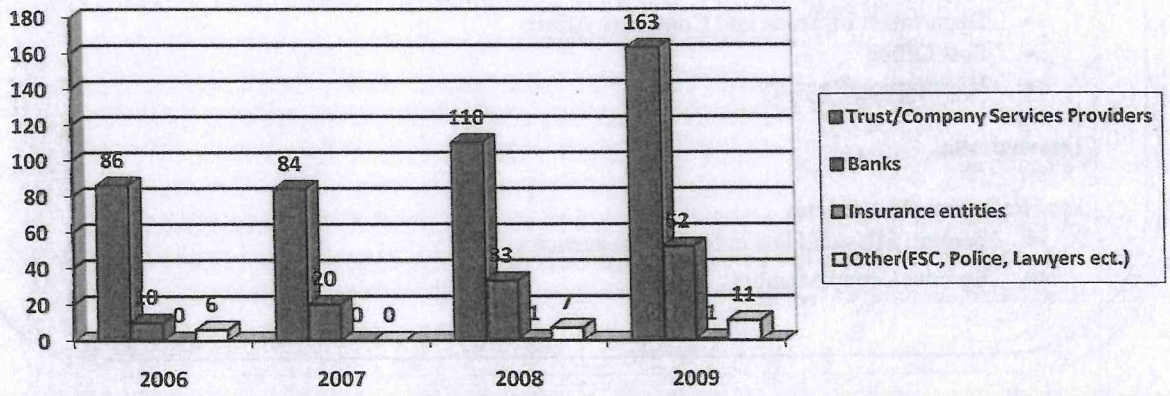


Table 1: Shows a breakdown of how the SARs/STRs received were disposed of during the reporting year 2008

Category	2006	2007	2008	2009
SARs Received	102	104	153	227
SARs/STRs Analyzed	102	75	104	227
SARs/STRs Disseminated Domestic Law Enforcement	2	Nil	6	2
SARs/STRs Disseminated to international Law Enforcement Agencies and FIUs	Nil	Nil	12	15

As previously mentioned, there was an increase in the number of SARs filed by reporting institutions during the year. See factors listed on pages 7 and 8.

Our partners

Domestic

Legal
- Attorney General's Office

Regulatory
- The BVI Financial Services Commission

Law Enforcement
- RVIPF
- HM Customs
- Immigration Department
- Inland Revenue Department
- Office of the DPP

Other Agencies
- Airport Authority
- Department of Trade and Consumer Affairs
- Post Office
- VI Shipping Registry

International

Law Enforcement Agencies
- Foreign FIUs and law enforcement agencies
- Egmont Group Members

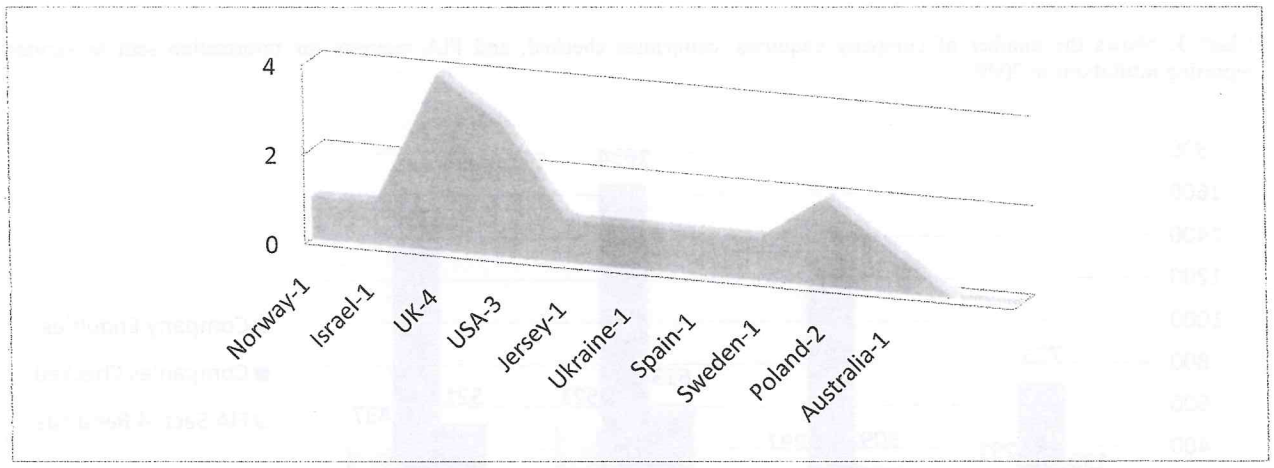
Mutual Legal Assistance

Mutual legal assistance is a vital tool that aids in the successful prosecution of criminals who perpetrate criminal activities that extends beyond the borders of individual countries. The Territory's mutual legal assistance regime is a vital avenue through which valuable information, intelligence, and evidence is shared with foreign countries to assist the global efforts to fight against serious and organised crimes. Mutual legal assistance matters can take place between competent authorities or through direct exchange of information for intelligence purposes such as what occurs between regulatory and law enforcement agencies. Judicial requests are usually processed in accordance with the provisions of the Mutual Legal Assistance Treaty (United States) Act, 1990 or the Criminal Justice International Cooperation Act, 1993.

Table 2: Shows a breakdown of Mutual Legal Assistance requests received between 2005-2009

Mutual Legal Assistance Requests	2006	2007	2008	2009
	25	36	22	16

Chart 2: Shows country by country break down of Mutual Legal Assistance Requests received in 2009



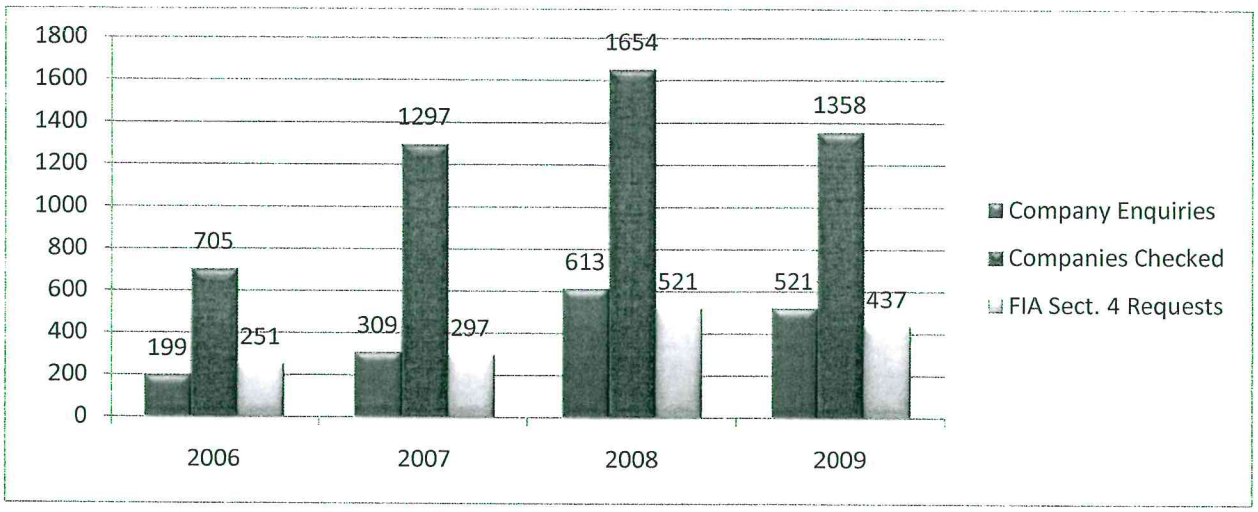
During the year under review, the Agency conducted inquiries linked to sixteen (16) mutual legal assistance requests received from foreign countries. These requests originated from ten (10) different countries including Norway, Israel, the United Kingdom, United States of America, Jersey, Ukraine, Spain, Sweden, Poland, and Australia. Much like the previous year, these requests were mainly linked to the investigation and prosecution of fraud and money laundering related offences. As is customary, these requests involved British Virgin Islands registered business companies alleged to have been used to facilitate the above mentioned criminal offences.

Information sharing

The British Virgin Islands remains the largest corporate domicile for the incorporation and registration of corporate entities, larger than any other financial services jurisdiction. Whereas, most of these companies are used for the purpose of facilitating legitimate trade on a global scale, some continue to be used for illegal purposes. There are instances, albeit very few, where these companies may themselves fall prey to fraudulent criminal acts. Apart from investigating the activities in both circumstances, the Agency often provides information or details on these companies. Such information is either provided spontaneously or upon requests by foreign authorities. The majority of these requests originate from foreign financial intelligence units, which are members of the Egmont Group.

The number of requests for information or company inquiries conducted on business companies registered in the British Virgin Islands has always remained relatively high and therefore will always be considered an important part of the Agency's work. The time it takes to process these requests for information can be critical because it is often the starting point for investigations. Additionally, it can prove useful in assisting requesting authorities to trace and identify assets that may be linked to the crimes being investigated. The next step in the process occurs when a requesting authority is seeking material to be used as evidence in a court of law. These steps are covered under the mutual legal assistance process which was previously discussed.

Chart 3: Shows the number of company enquiries, companies checked, and FIA requests for information sent to various reporting institutions in 2009

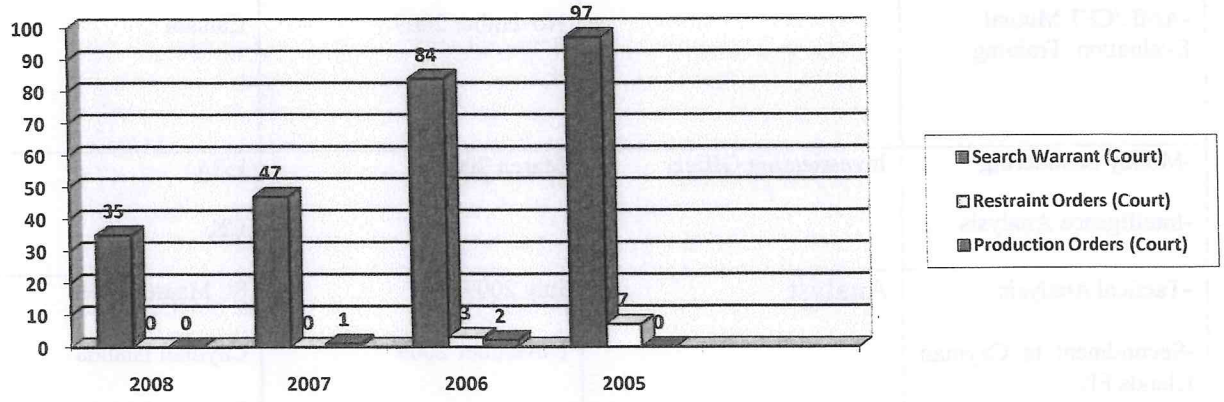


The number of company enquiries, companies checked and FIA requests for information sent to reporting entities during the reporting year was lower when compared to the previous year. This coincides with a decrease in the number of requests for information sent to the Agency by our local and domestic partner agencies.

Table 3: Shows a country by country breakdown of requests for information received from local and domestic partner agencies in 2009

Country	No. of Requests	Country	No. of Requests	Country	No. of Requests
Argentina	4	Australia	4	Anguilla	2
Armenia	1				
BVI FSC	86	RVIPF	202	Belgium	16
Greece	1	Bosnia and Herzegovina	1	Singapore	1
Bulgaria	13	Brazil	4	Cayman Islands	1
Costa Rica	2	Colombia	1	Senegal	1
Cyprus	8	Croatia	9	Sri Lanka	1
Denmark	2	France	6	Germany	1
Japan	4	Hungary	3	India	1
Ireland	1	Italy	4	Iceland	1
Lithuania	3	Luxembourg	3	Liechtenstein	1
Malta	3	Mauritius	2	Montenegro	9
Nigeria	9	Macedonia	1	Moldova	5
Netherlands	5	Peru	2	Poland	4
Portugal	4	Romania	8	Russia	11
South Africa	1	Spain	1	Serbia	1
Turkey	1	USA	17	USVI	2
Switzerland	2	Turkey	1	Taiwan	1
Uzbekistan	1	Kazakhstan	9	Israel	2
UK	25	St. Vincent	4		
Total	**519**				

Chart 4: Shows the number of Search Warrants, Restraint Orders and Production Orders served between 2005 and 2009



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 Courte. 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 taking place within or outside the British Virgin Islands.

Training Activities

The issues relating to money laundering and terrorist financing are many and they are constantly changing. During the year, members of staff attended numerous training programmes and activities. These programmes and training activities were in keeping with the Agency's commitment to enhancing the staffs knowledge and experience in Anti-Money Laundering issues. A list of these programmes and training activities are contained in the following table.

Table 4: represents list of training courses and seminars attended by members of staff during the year 2009

Training Course/Seminar	By whom Attended	Date Attended	Country
-Money Laundering -FATF/CFATF Joint Typologies Meeting -Money Laundering and Terrorist Financing	Director	March 2009 November 2009 May 2009	USA Grand Cayman Qatar
-Money Laundering -Money Laundering and Terrorist Financing -AML/CFT Mutual Evaluation Training	Senior Investigating Officer	April 2009 June 2009 November 2009	USA Qatar Canada
-Money Laundering -Intelligence Analysis	Investigating Officer	March 2009	USA UK
-Tactical Analysis -Secondment to Cayman Islands FIU - FATF/CFATF Joint Typologies Meeting	Analyst	July 2009 November 2009 November 2009	St. Maarten, NA Cayman Islands Cayman Islands

Challenges

The challenges experienced during the year, though not insurmountable were many and included some from the previous year. These include:

- The lack of adequate and affordable office space which prevented us from proceeding with our planned expansion. Developing and expanding the Agency's resources is of particular importance given the increased workload. Further, the increased role the Agency is expected to play in its supervision of the Territory's Designated Non-Financial Businesses and Professions (DNFBPs), and Non-Profit Organisations will call for ever greater resources.

  DNFBPs consist of Real Estate Agents, Jewelry Stores, Auto Dealerships, Lawyers, and Accountants. Non-Profit Organisations include charitable organisations. These businesses and professions all falls within the scope of the FATF 40 plus 9 Recommendations aimed at countering money laundering and the financing of terrorist activities.

Going Forward

The complexity associated with identifying the new techniques and methodologies used by money launderers and terrorist financiers challenges us to build on our strengths and strengthen the Agency's internal capacity. This include adequate training of staff, enhancing operational processes and procedures by adopting best practices to ensure that we become more efficient in what we do and the way we do it, and developing our technology infrastructure.

The following areas were identified as key areas to be developed in the coming year. These areas will be reflected in the Agency's Work Plan for 2010.

IT Security Measures

Since the information we handle include information on individuals and business activities, and this information is quite sensitive, the Agency will continue developing a more modern Information Technology System. This project which started back in 2008 sought to identify modern and affordable information storage software to assist with the secure storage of information coming into the Agency.

Streamlining the Agency's operational procedures

In the coming year the Agency will seek to streamline its operational procedures by introducing an operational procedures manual. This manual will contain information relative to our core functions and will serve as a guide to the Agency's staff to ensure that correct procedures are followed in a manner that will help to safeguard the integrity of the information handled within the Agency.

Ensuring continuity following a disaster

Another priority area in the coming year is the development of a comprehensive Disaster Recovery Plan ("the Plan") for the Agency. The purpose of the plan is to organise and consolidate an approach to manage recovery activities following an unforeseen or unplanned incident or business interruption. This would reduce the impact resulting in a shortened period of business interruption. The Plan will be drafted in accordance with the Disaster Management Act (Ref: Part IV-14c).

Raising AML/CFT awareness among industry practitioners and the general public

Raising AML/CFT awareness within the Territory will continue to be one of the Agency's main focus heading into the coming year. This will include attending and participating in various fora organized by the Financial Services Commission, meeting one on one with reporting institutions to educate them on the role of the Agency and their reporting and under obligations under the POCCA and other important pieces of domestic AML/CFT legislation. Our aim is to improve the quality of reporting and the quality of the information provided by these institutions in their SARs.

Supervision of DNFBPs

Among the Industry practitioners are Designated Non-Financial Businesses and Professions which make-up a relatively large part of the Territory's economy and financial services sector. These business and professionals are currently regulated under the Territory's AML/CFT Framework, and responsibilities for their supervision currently rest with the FIA. However, there are still a number of issues regarding their supervision which the Agency in close collaboration with other key stakeholders will aim to address in the coming year 2010.

Building on our achievements to increase intelligence output

It is long recognized that one of the keys to combating the scourge of financial crimes is the exchange of information and intelligence between partner agencies. In previous years, the Agency placed great emphasis on improving the quality of intelligence disseminated to our local and international partner agencies. Going forward, the Agency will strive to further develop its output of valuable financial intelligence as a means of playing an even greater role in the global AML/CFT efforts.

Strengthening our relationship with international partners

The Agency will continue in its efforts to forge stronger ties with its international counterparts through the sharing of financial information and intelligence with Financial Intelligence Units of the Egmont Group.

Conclusion

Though the coming could be just as challenging as this year, the Agency will continue to work to meet and overcome its challenges.

The Agency will do so by delivering on its core functions to the best of its ability. This will serve as a positive indication to the international law enforcement community that the FIA is at the forefront in the fight against money laundering, the financing of terrorist activities and other related crimes.

The commitment of trained officers from the Police and Customs, alongside a dedicated and well trained support staff indicates the value placed in protecting the local, and to a large extent the global financial services system through the effective implementation of global measures aimed at combat money laundering and the financing of terrorism in accordance to the CFATF/FATF 40 plus 9 recommendations.

Appendix 1- Examples of Suspicious activities reported to the FIA in SARs

Cash and check deposits followed by immediate withdrawals

Substantial amount of money was deposited to Customer A's savings account over a nine month period. The deposits consisted of both cash and checks and coincided with an unusual number of withdrawals from the said account. The sudden increase in activities on the account was deemed to be outside of what was considered normal based on customer's profile.

Failure of a Customer to provide CDD information

Customer B goes into a financial institution with a large sum of cash for the purpose of opening a new account. Customer was asked to provide copies of valid ID and to verify the source of the cash prior to opening the account after and as a result became highly annoyed and indicated that he no longer wished to open the account.

Use of Corporate Vehicle to facilitate Bribery and Money Laundering

A Politically Exposed Person (PEP) from Country A established an offshore entity in the British Virgin Islands through an intermediary in Country B. It was later discovered that the PEP used his position to secure lucrative state contracts for a close associate who owned a construction business in the said Country A. The PEP used the offshore entity to launder the proceeds of Bribes which were paid to him to secure the Government contracts on behalf of his associate.

Use of Money Services Business to facilitate cross-border movement of cash

Mr. B who is suspected to be involving in the sale of illegal drugs regularly sent funds from the British Virgin Islands to the same individual who resides in Country A. The funds are sent via a local Money Services Business. Country A is known for its production and sale of illegal drugs. Enquires revealed that the individual in Country A is a known drug dealer and hence it is suspected that the money sent by Mr. B. may have been sent to purchase illegal drugs.

Use of the internet to facilitate Financial Fraud

An unknown number of individuals established an internet website to facilitate investment in an unregulated offshore entity. The online website advertised a prospectus which guaranteed potential investors an above average return on their investments. It was later determined to be an online investment fraud resulting in substantial loses.

Money transfers to high risk jurisdictions

Customer A is the holder of a bank account in the British Virgin Islands and frequently sends money in the form of bank drafts which are drawn on an account in a bank in a jurisdiction which is considered high risk from a terrorist financing perspective.

Use of corporate vehicles to commit breach of UN Sanctions imposed against a particular state government

Company A, an offshore entity in the British Virgin Islands has a purchase agreement with Company B which is a licensed manufacturer of weapons components. It was suspected that Company A upon purchasing the weapons from Company B resells them to Country C, which is subject to a UN Arms embargo.

Appendix 2- Examples of Money Laundering and Terrorist Financing Indicators

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 terrorist acts and groups.

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 estates, 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 3- Work Plan for 2010 (See the following pages numbered 1-8)

Appendix 4- Financials Reports 2009 (see the following pages numbered 1-12)

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
INTERPOL-	International Criminal Police Organisation
LOR-	Letter of Request
POCCA-	Proceeds of Criminal Conduct Act
MLA	Mutual Legal Assistance
SAR-	Suspicious Activity Report
STR-	Suspicious Transaction Report

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 estates, 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.

Appendix 3- Work Plan for 2010 (See the following pages numbered 1-8)

BRITISH VIRGIN ISLANDS

Financial Investigation Agency 2010 Work Plan

Introduction

The Financial Investigation Agency's (FIA) 2010 Work Plan outlines the major objectives and associated tasks set for the upcoming year. It is consistent with the objectives that will be detailed in the Agency's overall Strategic Plan for 2010-2013, which is in the final stages of completion. The work plan is supported by the Agency's Budget Estimates which highlights the resources needed to accomplish these objectives and facilitate the overall growth of the Agency.

It remains the current policy that the Territory should continue to play its role in the shaping and establishment of international standards of regulation, supervision and enforcement, especially in matters concerning or relating to its financial services industry.

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, it 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 the strategies aimed at countering 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 support to local financial institutions and trust and company services providers.

Recognising that the success of the Agency in properly carrying out its core functions largely depends on the degree of knowledge and competencies of persons

BRITISH VIRGIN ISLANDS

- Develop competency models, which will be integrated in all areas of human resources, while seeking to identify the particular learning needs of the Agency.

Performance targets

- Director and Chief Operating Officer will closely scrutanise applicants and prepare a list of potential candidates who appear to meet the necessary criteria.

- Work closely with training institutions and develop an overall training plan including a comprehensive list of relevant training courses, seminars and programmes in areas identified as key to ongoing employee development.

- Provide the necessary financial support to assist staff members in acquiring suitable professional qualifications in the areas of AML/CFT compliance.

- Develop a long term training plan with the assistance of the Egmont Group Training Working Group to address the long term training needs of the FIA.

Objective # 2

Expand the FIA's technical resources and streamline internal work flows and processes with a vision of improving the overall level of service we deliver to our local and international counterparts.

Tasks

- Develop an operational procedures manual to serve as a procedural guide for the FIA's staff. This manual will ensure that our procedures are consistent, efficient and effective. This manual will provide FIA employees with the proper guidance needed to fulfill the goals and objectives as set out in the FIA's Strategic Plan. The manual is currently in the initial drafting stages.

- Upgrade our information storage systems and our internal and external security systems with an aim to identify any potential weaknesses that may

- Prepare and circulate as necessary, written and electronic information such as public warning and advisories about money laundering, terrorist financing, and general financial crimes.

Performance targets

- Liaise with and assist the Financial Services Commission to plan training events. Additionally, assist in the preparation of training material and ensure their effective delivery.

- Liaise with the Financial Services Commission in the preparation of educational material for circulation to the general public.

Objective # 4

To increase the FIA's financial reserves as a practical way of preparing for the potential financial burden of investigating major financial crimes. In recent years we have seen how costly it can become to effectively investigate major financial crimes. It is imperative that the Agency remain forward thinking and grow its capacity to finance major investigations.

Tasks

- Further develop and implement investment policy designed to safeguard and grow reserve accounts.

- Seek additional funding sources including a formal request to share in the proceeds of the recent IPOC case.

Performance targets

- Indentify sound investments that will provide maximum returns while preserving the integrity of the FIA's financial assets.

BRITISH VIRGIN ISLANDS

- Secure off-premise accommodations to house Emergency Operations Center which can serve as a temporary office facility with full access to relevant data and equipment. This will reduce business interruption in the event of a natural disaster, manmade or other unplanned incident.

Performance target

- A comprehensive Business Recovery Plan submitted to the FIA Board for approval.

Objective # 7

Building a stronger relationship with our international counterparts

Tasks

- Contribute to the work of regional and international organizations such as the Caribbean Financial Action Task Force (CFATF), the Financial Action Task Force (FATF), and Egmont Group of Financial Intelligence Units.

- Seek to foster closer cooperation with specific members of the Egmont Group.

- Assist Financial Intelligence Units in CFATF member countries to gain membership in the Egmont Group.

Performance targets

- Regional and international conferences, workshops and training activities will be attended and the opportunities to participate in, and benefit from these activities will be documented.

- Seek to enhance the level of information sharing with key Egmont Member FIU's through formal information sharing mechanisms such as Memorandum of Understandings.

Appendix 4- Financials Reports 2009 (see the following pages numbered 1-12)