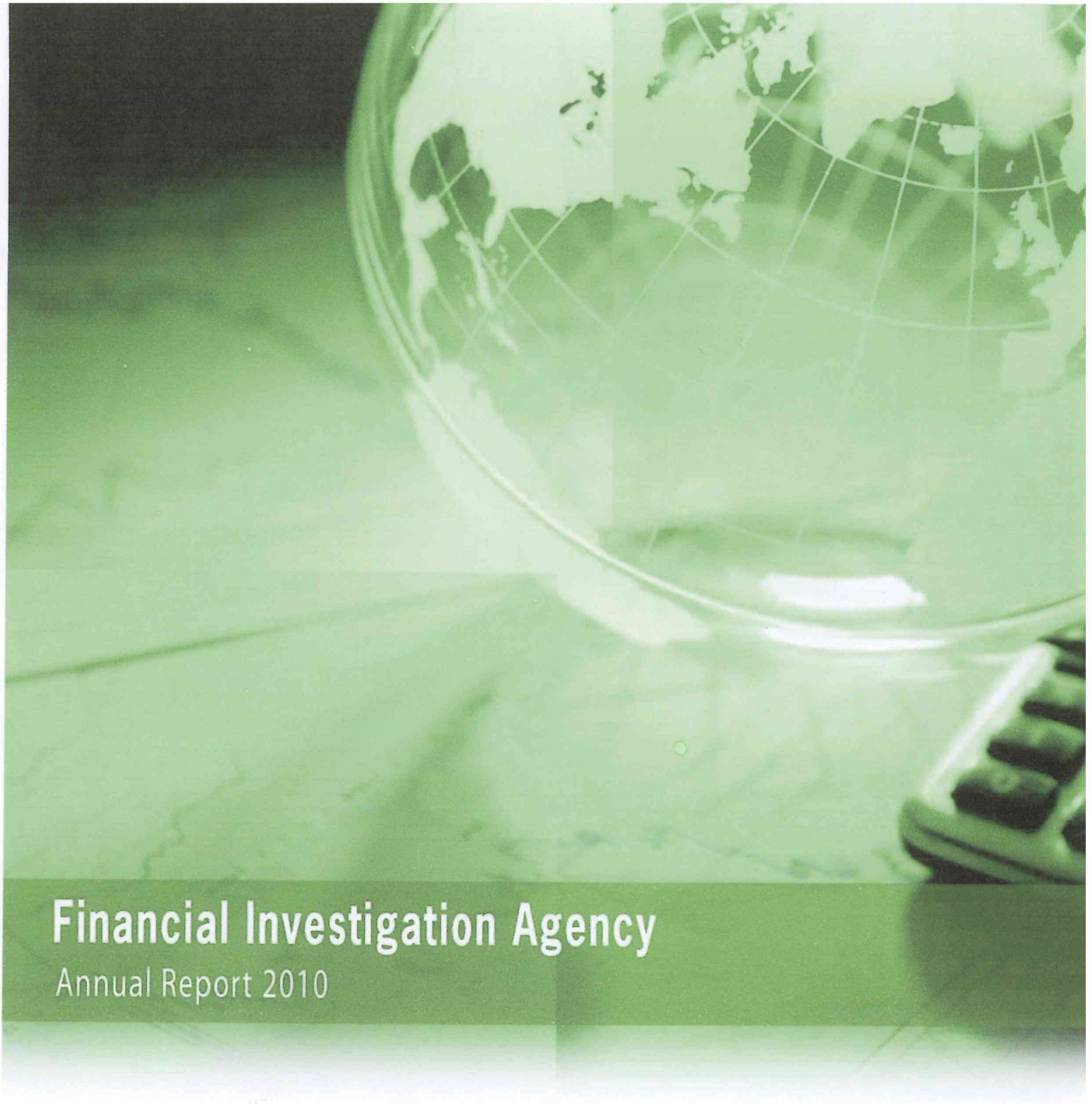


Financial Investigation Agency

Annual Report 2010

BRITISH VIRGIN ISLANDS

September 15, 2011

Deputy Governor Mrs. Inez Archibald
Chairman
Financial Investigation Agency Board
Deputy Governor's Office
Central Administration Complex
Road Town, Tortola, BVI

Dear Chairman:

Pursuant to section 11 (1) of the *Financial Investigation Act*, I am pleased to present you with the 7th Annual Report for the Financial Investigation Agency of the British Virgin Islands (FIA). This report provides details of our operations and our achievements for the reporting year 2010.

We will remain steadfast in our commitment to work closely with our local and international counterparts in an effort to counter the threats posed by money laundering, terrorist financing, and other transnational crimes. This will be achieved mainly by providing high quality information/intelligence in a timely manner.

Yours sincerely,

Errol George
Director

Message from the Director

Since becoming Director, my primary focus has been on building the Agency's capacity and improving its efficiency to better serve those that depend on us for high quality financial information and intelligence. In this regard, greater emphasis was placed on increasing the number of intelligence disclosures to our counterparts and improving our response time to requests for information and intelligence from both our local and international counterparts.

In addition to increasing our level of intelligence disclosures, we also worked hard to improve our response time to mutual legal assistance requests. I am also happy to report that we were able to build our resources by taking on three (3) additional members of staff with a further increase planned in the coming year. This increase in our human resources is in preparation for taking on the additional responsibilities of supervising DNFBPs and NPOs sometime during the next twelve to eighteen months.

During the year we experienced a slight decline in the number of Suspicious Transaction Reports which fell to one hundred and ninety-one (191) when compared to two hundred and twenty-seven (227) received the previous year representing a 15.7% decrease. The majority of these reports were money laundering, fraud, and compliance related. There has been a noticeable increase in fraud related offences since the general down turn in the global economy.

There was also a very small increase in the number of Mutual Legal Assistance Requests, the majority of which originated from the UK like the previous year. Likewise, there was an increase in the number of company enquiries conducted during the year which rose to six hundred and ninety (690) up from five hundred and twenty-one (521) received the previous year representing a 32.4% increase. The majority of these enquiries originated from the Russian Federation via the Egmont Secure Web (ESW).

Our liaison with our local and international counterparts continued during the year in an effort to facilitate an increase in the level of information and intelligence sharing. During the year we started the process of compiling a list of Egmont Group FIUs in preparation for the commencement of negotiations aimed at formalizing the exchange of financial

information/intelligence through the signing of MOUs. This will be one of our main priorities heading into the coming year 2011.

As is customary, the FIA attended and participated in several Egmont Group meetings as well as Caribbean Financial Action Task Force meetings that took place through the year.

In our effort to ensure the staff received ongoing training several members of staff attended a number of AML/CFT training seminars and courses throughout the year. These seminars and courses were in keeping with our aim to enhance their knowledge and expertise.

Though we expect some challenges in the coming year, I anticipate the additional resources we took on this year together with what we hope to take on in the coming year will put us firmly in a position to meet and overcome these challenges.

Errol George
Director

2010 at a glance

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

Receipt and collection of information

- Number of Suspicious Activity Reports (SARs) received = 191

Analysis and dissemination

- Number of Suspicious Transaction Reports (SARs) processed = 191
- Number of Suspicious Activity Reports cleared = 106
- Number of Suspicious Activity Reports carried over into 2010 = 85
- Number of reports disclosed to the Royal Virgin Islands Police Force Financial Crimes Investigation Unit = 6
- Number of disseminations to foreign FIU's = 58

Working with domestic regulator and law enforcement authorities

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

Financial Services Commission= 81
BVI Customs= 3
RVIPF= 327

International collaboration to combat ML/TF

- Number of Letter of Requests for Mutual Legal Assistance received = 17
- Number of Letter of Requests for Mutual Legal Assistance processed= 15
- Number of FIU/Law Enforcement Requests for information received = 690
- Number of foreign FIU/Law Enforcement Requests for information processed = 493
- Number of FIA requests sent to foreign FIUs= 26
- Number of request refused= 1 (absence of an MOU)

Our continued growth

- The Agency moved into new office accommodations in June of 2010
- The Agency took onboard two (2) additional members of staff during the third quarter of 2010 to assist us in meeting the demands of a growing workload
- Commissioned our new IT System including phased construction of a customized database to facilitate the greater storage and integrity of sensitive data held by the Agency

Increasing AML/CFT awareness

Local and international training seminars

- The FIA participated in six (6) in-house training seminars organized by reporting entities within the local financial services sector.
- FIA 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 conferences organized by the Egmont Group of Financial Intelligence Units and the Caribbean Financial Action Task Force (CFATF).

The FIA at the Glance

Our Vision

To provide an affective, professional, and transparent, internal 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, 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 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 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.

Our Core Functions (What we do)

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.

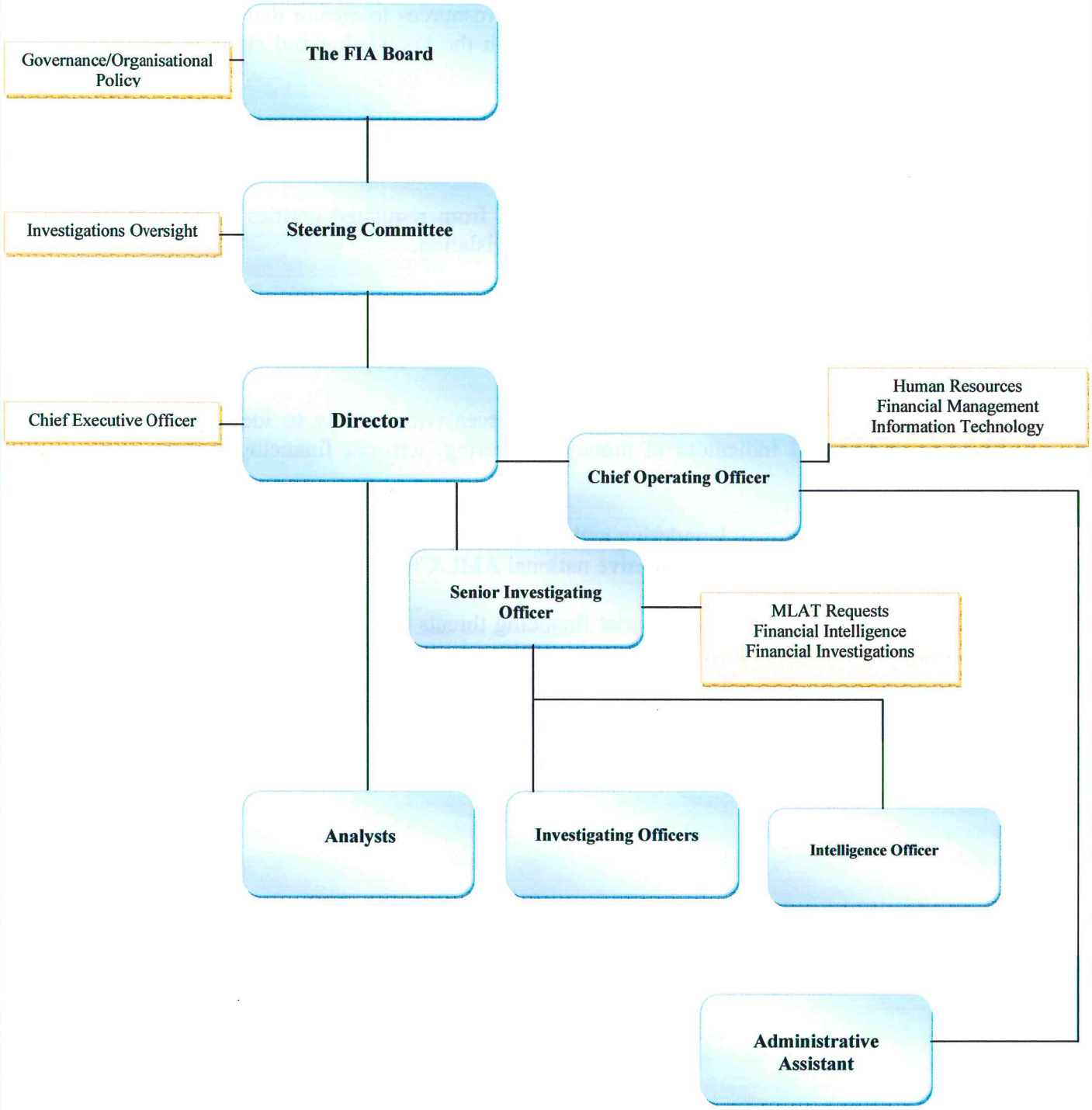
Analyze information obtained from various sources with a view to identify new and emerging trends and indicators in money laundering, terrorist financing and types of financial crime.

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



Meet the FIA Team

From Left to Right: Sandra Blaize-McCall (Analysts), Delia Jon-Baptiste (Analyst), Julien Johnson (Chief Operating Officer, Mia Wattley-Forbes (Intelligence Officer), Alcedo Fahie (Senior Investigating Officer) Chyrisia Millington (Administrative Assistant), Errol George (Director), and Claude Williams (Investigating Officer)

Introduction

Overall, there were very little differences between the current reporting year and the **previous year 2009 with** respect to the Agency's overall responsibilities. The total **number of suspicious activity reports (SARs)** received during the year was slightly lower than last year. As is customary, Trusts and Company Services Providers (TCSP) accounted for the majority of SARs filed, followed by Banks, and the local financial services regulator, the FSC.

The year also saw an increase in the Agency's output when compared to any other year since the Agency's formation in 2004. This was in spite of the fact that the number of Suspicious Activity Reports (SARs) received for the year fell slightly below what was received the previous year 2009.

During the year, we continued our efforts to build closer and more meaningful relationships with our domestic and foreign partner agencies. As part of this process, several regional and international meetings were attended by members of staff. The aims and objectives of these meetings with our counterparts were to discuss matters of mutual concerns as we pool our resources to fight against the scourge of money laundering, terrorist financing and other financial crimes.

Our outreach efforts included assisting the FIUs of the Republic of Trinidad and Tobago, Montserrat, and Guyana to gain membership in the Egmont Group of Financial Intelligence Units. As a result of these efforts which started almost two years ago, I am very pleased to report that we are now one step closer to seeing the FIU of Trinidad and Tobago join the rank of several of the region's Financial Intelligence Units, which are already Egmont members. This we hope will be finalized in the coming year when the Group meets at its annual plenary scheduled to take place in the Republic of Armenia in July of this year 2010.

Some may ask why it is so important for Financial Intelligence Units in the Caribbean hemisphere to become members of Egmont, and why it is so important to take part in the work of the Egmont Group. To answer this, one only need recognise the value of the role played by financial intelligence units in the global fight against ML, TF and other financial crimes. More so, the important contribution the Egmont Group make to the international discourse on AML/CFT issues. These issues are driven by key international bodies such as the Financial Action Task Force, the G20 grouping of developed countries, the Caribbean Financial Action Task Force, and the Organisation for Economic Cooperation and Development (OECD)M, only to name a few.

This is one of the key reasons why the Agency's ongoing participation in these regional and international fora will always be regarded as a propriety area.

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 agencies 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 Territory without producing the required identification, or a customer who suddenly starts depositing large sums of cash which is considered to be above his or her normally deposits. It is a statutory 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 various types of reporting institutions. These institutions include banks or deposit taking institutions, Trusts and Company Services Providers (TCSPs), Money Services Businesses (MSBs), Lawyers, Real Estate Agents, Auto Motive Dealers, Jewelry Stores, Accountants, and Non-Profit (NPOs) or Civic 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 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 191 SARs during the current reporting year, 2010 when compared to 227 reports received the previous year, 2009. This represents a 16% decrease. Of these, 154 were recorded as proactive reports, while the remaining 37 were recorded as reactive. Reactive reports are reports that are usually filed in response to the Agency's request for information in accordance with the powers granted to the Agency under the provisions of the FIA Act, 2003.

Chart 1- Shows a monthly break down of SARs filed for 2010

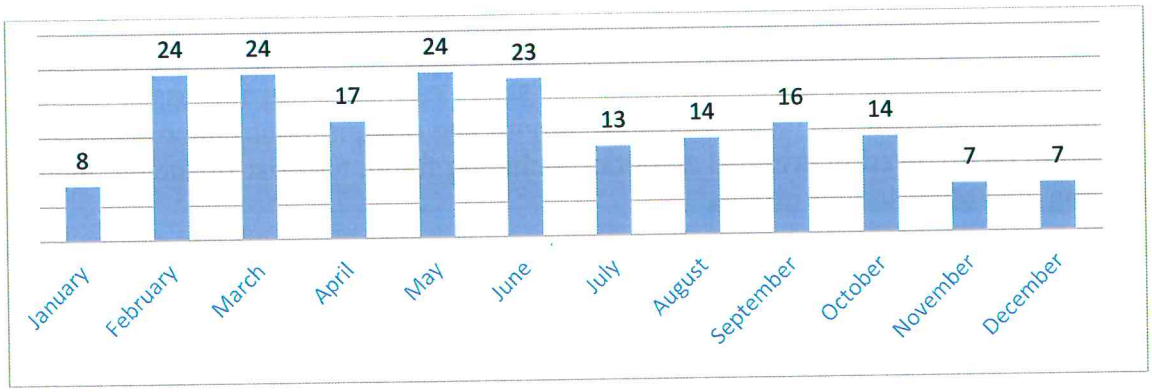


Table 1: Breakdown indicating grounds for suspicion for SARs filed during the year 2010

Grounds for suspicion	Number
Mutual Fund Fraud	38
Mortgage Fraud	1
Wire Fraud	1
Insider Trading	1
General Fraud	8
Money Laundering	41
Terrorist Financing	1
Human Trafficking	1
Drug Trafficking	1
Bribery and Corruption (PEPs)	3
Sanctions Listing	2
Compliance related issues	56
Regulatory Action (Advisory Warning)	6
FIA Requests for Information prompting filing of Reactive/Defensive Reporting by Regulated Sector	31

Chart 2: Shows the number of SARs received between the periods 2007-2010

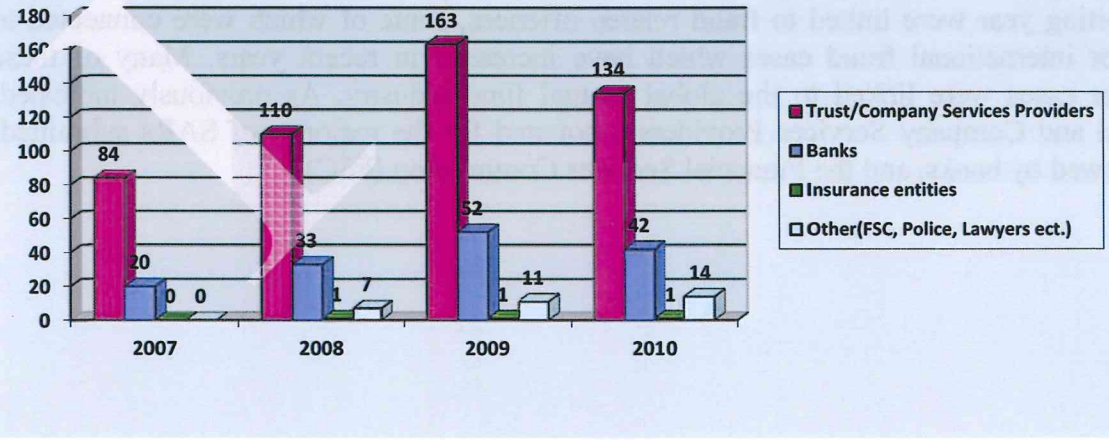


Table 2: Shows a breakdown of how the SARs/STRs received were disposed of during the reporting year 2010

Category	2007	2008	2009	2010
SARs Received	104	153	227	191
SARs/STRs Analyzed	75	[illegible]	[illegible]	[illegible]
SARs/STRs Disseminated Domestic Law Enforcement	Nil	6	2	12
SARs/STRs Disseminated to international Law Enforcement Agencies and FIUs	Nil	12	15	54

As previously mentioned, there was a 16% decrease in the number of SARs filed by reporting institutions during the reporting year relative to the 220 reports submitted during the previous year. Though the number of reports is lower than 2009, the figure is above the average of the previous three years. The reasons behind the fluctuation in SARs from year to year are many. On one hand, it could be merely statistical in nature as there is almost certain to be changes in the reporting pattern. There is also the likelihood that some cases could trigger a number of SARs involving the same subject. This is very likely given the interconnectivity of the local financial services industry.

The reasons for filing these reports are very similar when compared to the previous reporting years. The majority of the 154 proactive reports submitted during the current reporting year were linked to fraud related offences, some of which were connected to major international fraud cases which have increased in recent years. Many of these major cases were linked to the global mutual fund industry. As previously indicated, Trust and Company Services Providers accounted for the majority of SARs submitted, followed by banks, and the Financial Services Commission (FSC).

Chart 3: The pie chart above represents a breakdown of SARs filed by institutions during 2010

Mutual Legal Assistance

Mutual legal assistance is a vital tool that aids in the prosecution of criminals who perpetrate criminal activities that extends 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 continued to share information and evidence with foreign countries to assist in the prosecution of financial and other types of crimes.

Table 3 shows a breakdown of Mutual Legal Assistance Requests received between 2007-2010

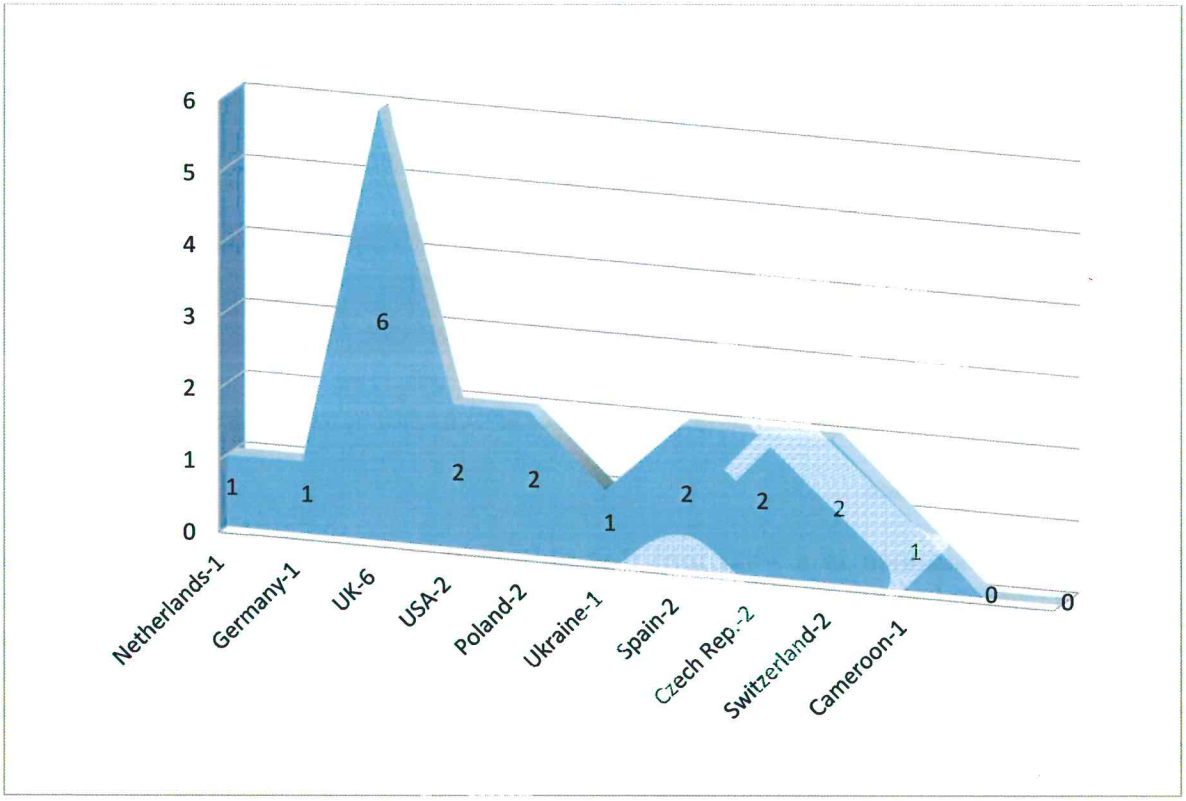
MLA Requests	2007	2008	2009	2010
	36	22	16	17
	36	22	16	17

Table 4: Shows the a breakdown of Mutual Legal Assistance Requests received in 2010 catagorised by offences

Fraud	Bribery and Corruption	Money Laundering	Theft or Embezzlement	Illegal Smuggling of Goods	Drug Trafficking
12	5	11	4	1	1

Note: Letters of Request for Mutual Legal Assistance may often include more than one predicate offence

Chart 4: Country by country break down of Mutual Legal Assistance Requests processed in 2010



The Agency received twenty (20) mutual legal assistance requests from foreign countries during the reporting period. Of those, seventeen (17) were processed during the reporting period. The requests originated from ten (10) different countries as indicated in the above chart. The majority of these requests originated from the United Kingdom. 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 allegedly linked to criminal activities in foreign jurisdictions.

Our International Obligations

The Egmont Group of FIUs

Tackling money laundering and terrorist financing is no easy task. It is one that requires a great deal of dedicated effort by a vast network of local and international law enforcement agencies. Financial Intelligence Units are at the forefront of this effort.

These units provide valuable information/intelligence which allows police and prosecutorial authorities to build cases against persons involved in criminal activities.

The Egmont Group of Financial Intelligence Units was formed in 1994 to promote the free exchange of financial information among its member FIUs. The group provides avenues through which issues surrounding the operations of FIUs can be discussed. Issues include training of FIU personnel, information exchange, FIU cooperation with other law enforcement bodies, and information storage and security only to name a few.

Egmont Group members are expected to respect and adhere to the Egmont Principles of Information Exchange. Information exchange among Egmont members can be done freely or though bilateral arrangements such as Memorandum of Understandings (MOUs).

The British Virgin Islands Reporting Authority, the Territory's first designated FIU became a member of the Egmont Group in 1999. Since then, the FIA has actively participated in the work of Egmont as members of the Outreach Working Group. Representatives from the Agency attend the annual Plenary Meetings, as well as Working Group meetings. In addition to attending the 2010 Plenary Meeting held in Cartagena, Colombia in July of the reporting year, we also attended the Working Group meeting held in Kuala Lumpur, Malaysia.

Information exchange

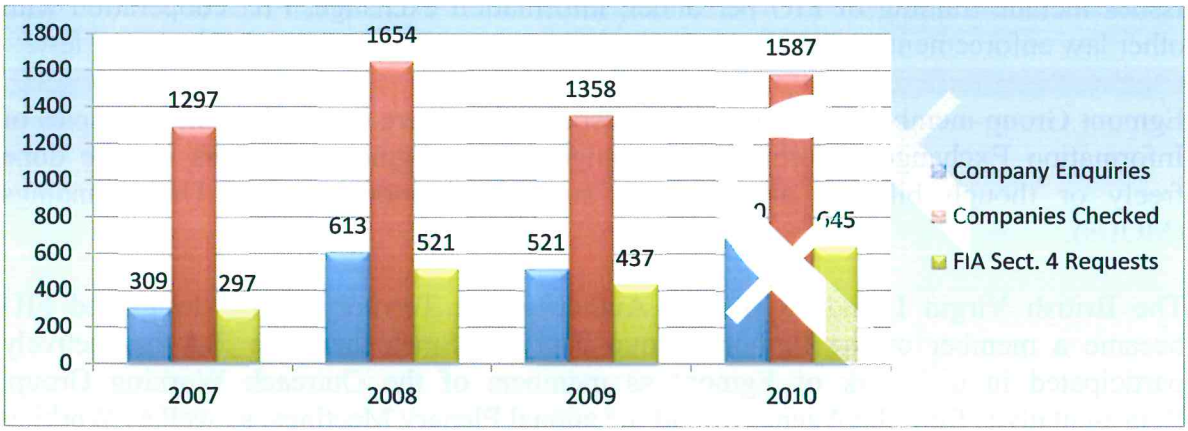
The British Virgin Islands remains the largest corporate domicile for the incorporation and registration of corporate entities referred to as BVI Business Companies. The number of BVI Business Companies currently on the Company's Register is larger than any other financial services jurisdiction. Whereas, most of these companies are used for the purpose of facilitating legitimate trade on a global scale, some continue to be used for illegitimate purposes.

The FIA requests information from its foreign counterparts when disclosures are linked to other jurisdictions. Likewise, requests for information are sent to the FIA by foreign counterparts when disclosures receives in those jurisdictions points to or a linked to entities registered in the BVI. These requests originate from our Egmont Group counterparts.

The FIA is receives and processes one of the highest numbers of request for information when compared with its counterparts in the Egmont Group. The number of these requests remains relatively high. The time it takes to process these requests for information is considered critical due to the fact that requests for information are usually the starting point for investigations, in some case major investigations which could have a reputational risk on the territory and its financial services sector. Additionally, it can

prove useful in assisting requesting authorities to trace and identify assets that may be linked to the crimes being investigated. Data on requests for information can be seen below.

Chart 5: Shows the number of company enquiries, companies checked, and FIA requests for information sent to various reporting institutions between 2007 and 2010



The number of company enquiries, companies checked and FIA requests for information sent to reporting entities during the reporting year was higher than the previous year. This coincides with a increase in the number of requests for information sent to the agency by our local and domestic partner agencies.

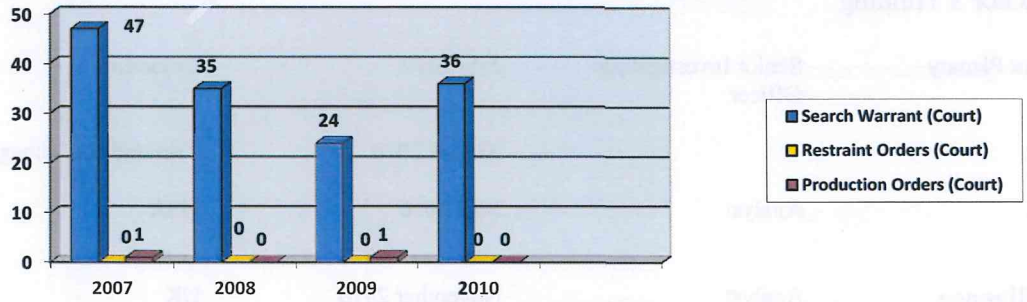
Enhancing in' .national cooperation

Section ' 2) (h) of the FIA Act which guides our operations authorities us to enter into under.. ' with foreign financial investigation agencies for the purpose of sharing informatio. 'ed to financial crimes. However, the said Act gives us authority to share information ' any foreign financial investigation agencies outside of having any formal arrangem ts. However, such is not the case for some of our foreign counter'arts whose domestic legislation requires that they have formal bilateral arrangements before sharing any information with foreign counterparts. During the coming year, the FIA will strive to build on its level of cooperation with its foreign counterparts by commencing them (MOUs). We anticipate having these negotiations completed in time for the 2011 Egmont Plenary meeting scheduled to be held in Yerevan, Armenia.

Table 5: Shows a country by country breakdown of requests for information received from local and domestic partner agencies in 2010

Country	No. of Requests	Country	No. of Requests	Country	No. of Requests
Argentina	1	Australia	2	Anguilla	1
Armenia	2	Isle of man	2	Budapest	2
BVI FSC *	92	RVIPF *	86 (o/b/o Interpol)	Belgium	28
Greece	2	Norway	2	Singapore	1
Bulgaria	13	Brazil	7	Gibraltar	2
Slovakia	2	Dom. Rep.	1	Hong Kong	5
Cyprus	3	Croatia	7	HM Customs	3
Denmark	3	France	19	Germany	12
Lebanon	1	Hungary	4	India	8
Ireland	7	Ukraine	48	Canada	1
Lithuania	5	Luxembourg	2	UK	61
Malta	2	Venezuela	1	Montenegro	14
Seychelles	3	Mexico	2	Moldova	4
Netherlands	3	Albania	1	Poland	2
Portugal	4	Romania	5	Russia	123
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		
Philippines	1	Trinidad and Tobago	1	Panama	1
South Africa	1	Kazakhstan	7	USVI	1
Belarus	[illegible]	Malta	2	Serbia	2
St. Vincent	4	Taiwan	1	Israel	2
Czech Repub[illegible]	2	Latvia	3	Serbia	2
Jersey	[illegible]2	USA	15	Spain	14
Ireland					
TOTAL	6[illegible]				

Chart 4: Shows the number of Search Warrants, Restraint Orders and Production Orders served between 2007 and 2010



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 offences taking place either within or outside the British Virgin Islands.

Training Activities

The FIA recognizes the valuable contribution made by its employees, knowing that what we do calls for a great deal of personal and professional integrity, knowledge, intellect, and commitment. In our efforts to ensure our staff received the necessary training to enhance their skills and expertise on an ongoing basis, the Agency continued to provide training opportunities to its staff regardless of their particular area of expertise. During the year members of staff attended numerous training activities which were in keeping with the Agency's commitment to enhancing the staffs knowledge and experience in AML/CFT issues. These training activities are contained in the following table.

Table 6: represents list of training courses and seminars attended by members of staff during the year 2010

Training Course/Seminar	By whom Attended	Date Attended	Country
-AML	Director	May 2010	USA
-Managing an FIU -Egmont Plenary	Director	July 2010	Columbia
-Workshop on Corruption and Bribery	Director	October	UK
-AML/CFT Mutual Evaluator's Training	Director	November 2010	USA (IMF HQ)
Egmont Plenary	Senior Investigating Officer	July 2010	Colombia
-AML		August 2010	Trinidad and Tobago
-AML	Analyst	May 2010	USA
-Intelligence	Analyst	November 2010	UK

Analysis -Intelligence Analysis	Intelligence Officer	November 2010	UK

Challenges

The challenges we faced during the year were primarily due to two main areas of concern.

1) Our need for additional resources to enable us to take on the additional responsibility of supervising the Territory's Designated Non-Financial Businesses and Professionals (DNFBPs), and Non-Profit Organisations (NPO) sector in accordance with Section 9 (2) of the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008.

While the DNFBP sector is more easily defined given that they are smaller in number, the NPO sector is larger and more diverse. However, certain aspects of the sector can be more vulnerable to terrorist financing than others. For example, NPOs which engage in public fundraising where the funds are intended for beneficiaries abroad, particularly where those beneficiaries are located in high risk jurisdictions.

The NPO sector is a vital and integral part of the Territory's economy and they make a valuable contribution to the community by providing a large spectrum of public services. These services range from providing educational opportunities, offering social services such as free testing for non-communicable diseases, facilitating sports, and advancing environmental, cultural or civic causes, only to name a few.

International standards dictates that these businesses and professions should all be subjected to AML/CFT supervision in accordance with the FATF 40 plus 9 Recommendations aimed at countering money laundering and the financing of terrorist activities.

2) The completion of the first phase of our database brought with it some challenges. Though what we were able to achieve so far was a remarkable achievement, the new database project remains a work in progress. During the year we commenced the process of loading our data which consisted of hard copy files onto our new

electronic storage system. These files consisted of relatively old data which existed since 2004 when the Agency first became operational.

Though the reaming part of this project will continue to be quite challenging given the resource needs we anticipate having it completed within the shortest possible timeframe following the beginning of the coming year 2011.

Looking Ahead (our priorities for 2011)

Staff training

Financial Intelligence Units must keep pace with the ever increasing challenges posed by criminal enterprises. Criminals continue to challenge our resolve as they seek new and more innovative ways to ensure that their clandestine activities go undetected. Recognizing that having a fully trained staff is vital in carrying out our mandates, the FIA will continue to make proactive efforts to identify and provide the most appropriate training necessary to its staff in order to upgrade their skills.

Improving our IT infrastructure

The Agency will continue to develop its IT infrastructure in the coming year. This will include additional upgrades to our information storage systems as well as investing in financial analysis software to assist in the analysis of Suspicious Transaction Reports filed by reporting institutions. We will also look closely at developing a secure online reporting system to facilitate electronic reporting of SARs.

Raising awareness of regulated entities

The success of the FIA and the preservation of the Territory's financial services sector largely depend on the ability of each reporting entity to prevent abuse of our financial services industry. To do this, it is important that they have the necessary knowledge to be able to identify suspicious activities.

As a result, raising AML/CFT awareness within the Territory will continue to be one of the Agency's key priorities going forward. This will include attending and participating in various fora such as the meet the regulators forum which is usually organized by the Financial Services Commission on a quarterly basis, as well as occasional one-on-one discussions with industry professionals where issues such as SARs reporting and feedback will be discussed. The overall aim of these discussions will be to improve the quality of reporting and information provided by these institutions in their SARs.

Additionally, the Agency has seen an increase in the number of Advance Fees or 419 type frauds during the reporting year. As a result, the Agency will commence work

during the early part of the coming year to put together a pamphlet that will contain useful information on the various scams being circulated via the world wide web ect. On completion, these pamphlets will be circulated among the various business places Territory wide in an effort to sensitize persons about the various scams that are in circulation.

Supervision of DNFBPs and NPOs

Apart from raising awareness within the general financial services sector, the Agency will commence laying the foundation to take on the AML/CFT supervision of the Designated Non-Financial Businesses and Professions and Non-Profit Organizations (NPOs). Though the risk for abuse within this sector may be low when compared to financial institutions, it still remains vulnerable to abuse. As a result, our plan for the coming year will include working closely with the Joint Anti-Money Laundering and Terrorist Financing Advisory Committee (JALTFAC) and other key stake holders to build a comprehensive framework to supervise these entities.

Some of the consideration that will be looked at regarding the supervision of these entities will include creating a separate Compliance Unit within the existing structure of the Agency. This new unit will be responsible for undertaking the AML/CFT supervision of these entities. The responsibilities of this unit will include conducting target onsite examinations/inspections of the supervised entities to ensure (1) that they have the necessary policies and procedures in place to identify and manage the AML/CFT risks inherent with their business activities, and (2) to ensure that their AML policies are being used for the purpose for which they are intended.

Building our relationship with international partners

As indicated earlier, the Agency will work hard to build stronger relationships with its Egmont Group counterparts. To this end we will commence simultaneous negotiations with several of the Egmont Group FIU which expressed an interest in entering into formal information sharing arrangements with the Agency. These negotiations will be done with the view to having them finalize in time for the 2011 Egmont Group Plenary which is scheduled to take place in Yerevan, Armenia. These MOUs will facilitate the bilateral sharing of financial information and intelligence linked to money laundering and [illegible] encies resolve in playing a greater role in the fight against transnational crimes.

Conclusion

A general observation, given the global nature of money laundering and terrorist financing, is that geographic borders have become increasingly irrelevant. Money launderers and terrorist financiers will continue to search and create more innovative

ways to conduct their activities. This include moving their activities to jurisdictions with few or weak AML/CFT countermeasures. The ease of which money can be moved across the globe electronically is instantaneous and this will continue to give rise to particular concern for the authorities.

Additionally, the lethargic state of the global economy could result in an increase in the level of transnational criminal activities worldwide all of which has the potential to create wealth using the money laundering processes. These activities include (drug trafficking, arms trafficking, trafficking in nuclear arms material, frauds, human trafficking, bribery and corruption of public officials (PEPs), and major investment type frauds. The fact that none of these activities are confined by borders will continue to makes each and every country vulnerable. The threats posed by these activities are significant and left unchecked can do considerable damage to our local economy.

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

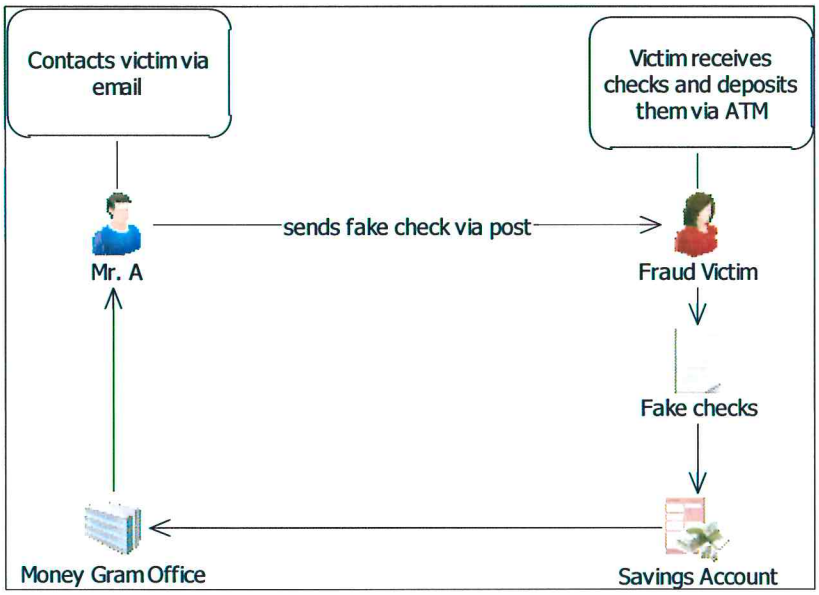
Fake check scam

Case # 1

The Agency received an SAR filed by a local bank concerning one of their customers. The customer indicated that she had received an email from Mr. A, who is believed to be of West African origin residing in the UK purported to be a United States businessman offering opportunities to individuals who prefer to stay at home and work. He subsequently sent her a number of money orders via post and asks her to cash them upon receipt, take a portion as a deposit for work to be done, and return a portion to him in cash via a local Money Gram or Western Union office.

The customer stated that upon receipt of the fake checks she took them to her bank and deposited where she deposited them to her account using the ATM machine and immediately withdrew the money, and send a portion to Mr. A via the local Money Gram office. The fake checks for all intent and purposes appeared to have been negotiated through a reputable banking institution in the USA. The local bank later notified the customer that the checks were fraudulent. The customer suffered a lost after the bank debited her account to recover the amounts of the fake checks.

Outcome: Matter was referred to the local Police for further action and investigations

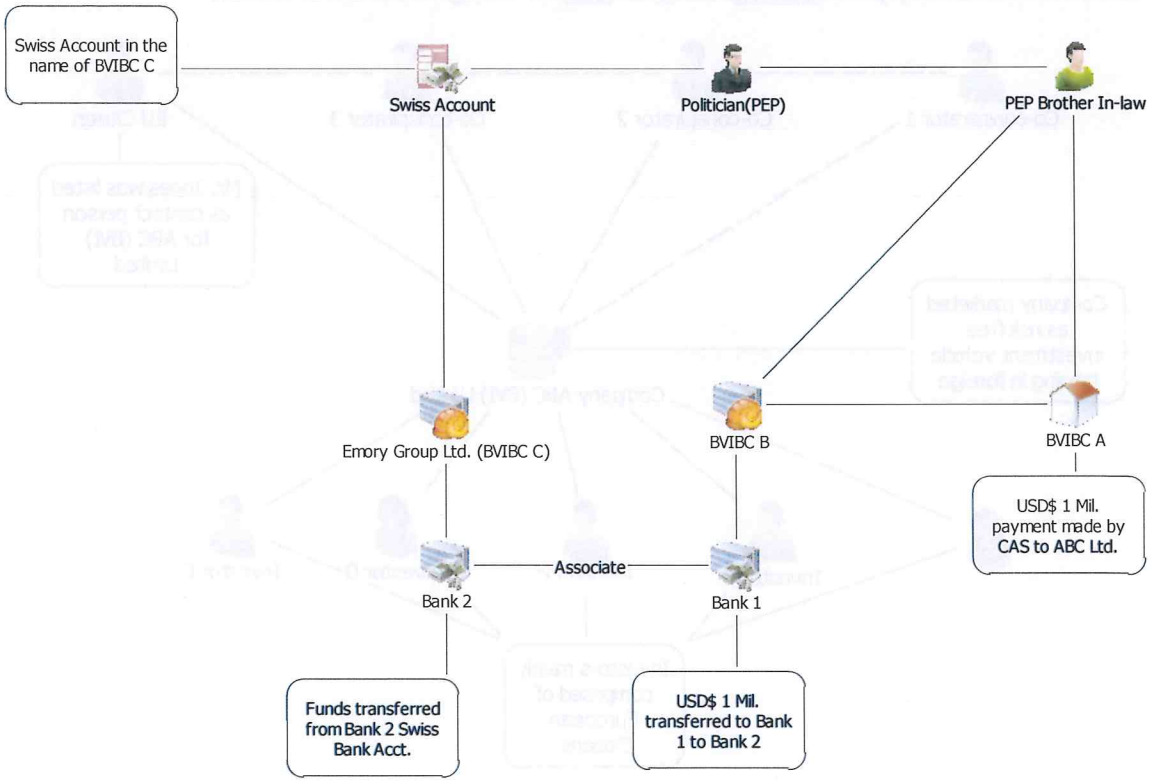


Use of Corporate Vehicle to launder proceeds of Corruption

Case # 2

The Agency received an SAR concerning Mr. B, a Politically Exposed Person (PEP) from Argentina. Mr. B established an offshore entity (BVIBC C) in the British Virgin Islands. It was later discovered that he used his position to secure several lucrative state contracts for his brother in-law who owned a construction business registered which was also registered in the BVI in the name of BVIBC A. In return, the PEP received multiple payments as kickbacks for using his influential position to secure the contract on his brother in-law's behalf. These payments were made to BVIBC C, an entity owned by the PEP from BVIBC B, owned by the PEP's brother-in-law. The PEP then laundered the money through a bank account he opened in another foreign jurisdiction. The account was opened in the name of name of Company D, an entity registered in the BVI.

Outcome: Information in the form of a disclosure was sent to the FIU in the PEPs home country.

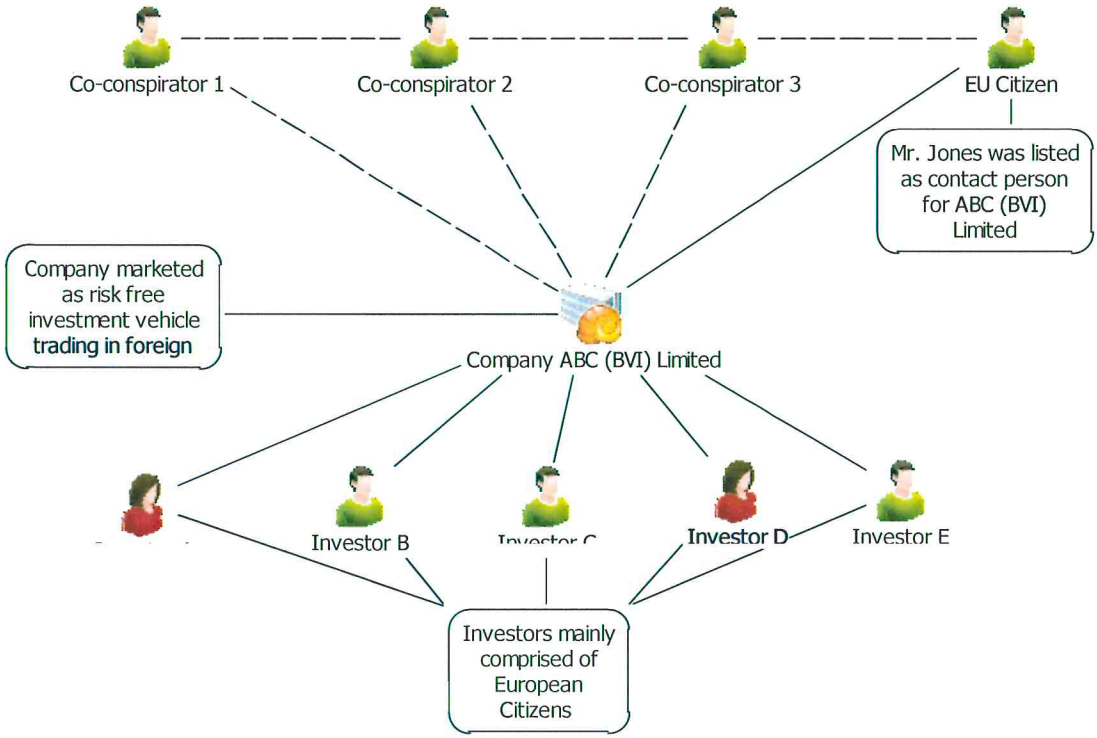


Case # 3

Use of fraudulent BVI Business Company to perpetrate fraud via the internet

The Agency received several complaints from a numbers of investors concerning an Austrian citizen. The said individual along with several unknown accomplices established an internet website promoting a fraudulent entity purporting to be licensed and regulated by the BVI Financial Services Commission. The entity which listed a physical address in the BVI was marketed as an investment vehicle used to invest in currency among other things. The venture was advertised as one with minimal risk offering investors varying rates of return on their investment depending on the terms of their investments. The investment scheme appeared to have targeted mainly Europeans as potential investors.

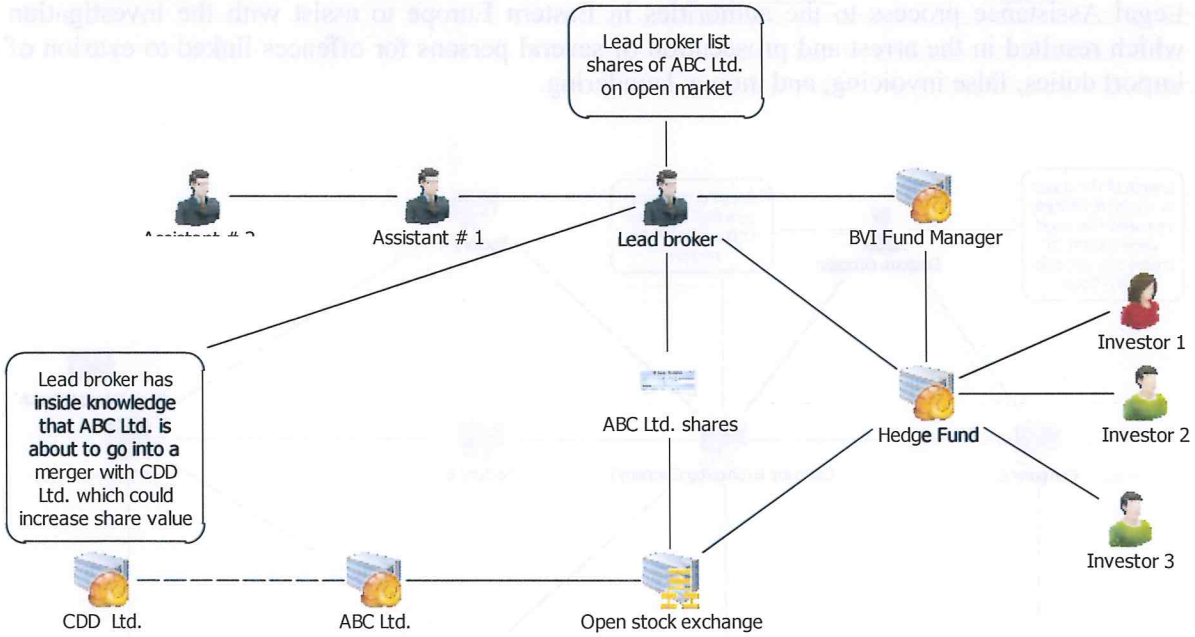
Outcome: Enquiries revealed that the entity was not a BVI regulated entity as purported to be on the internet website. Information in the form of a disclosure was sent to the FIU in the home country of the subject who was listed on the website as main contact, though we had reasons to suspect that the individual was using a factitious name.



Case Study 4 – Fraud/Insider Trading

A United States Citizen who was the founder and Hedge Fund manager for a corporate entity registered in the BVI was charged criminally following allegations of insider trading. The allegations were brought by the United States Security and Exchange Commission (SEC). Though the company registered in the BVI was not implicated in any wrong doing the principal behind the entity was. As a result, a Suspicious Activity Report was submitted to the Agency.

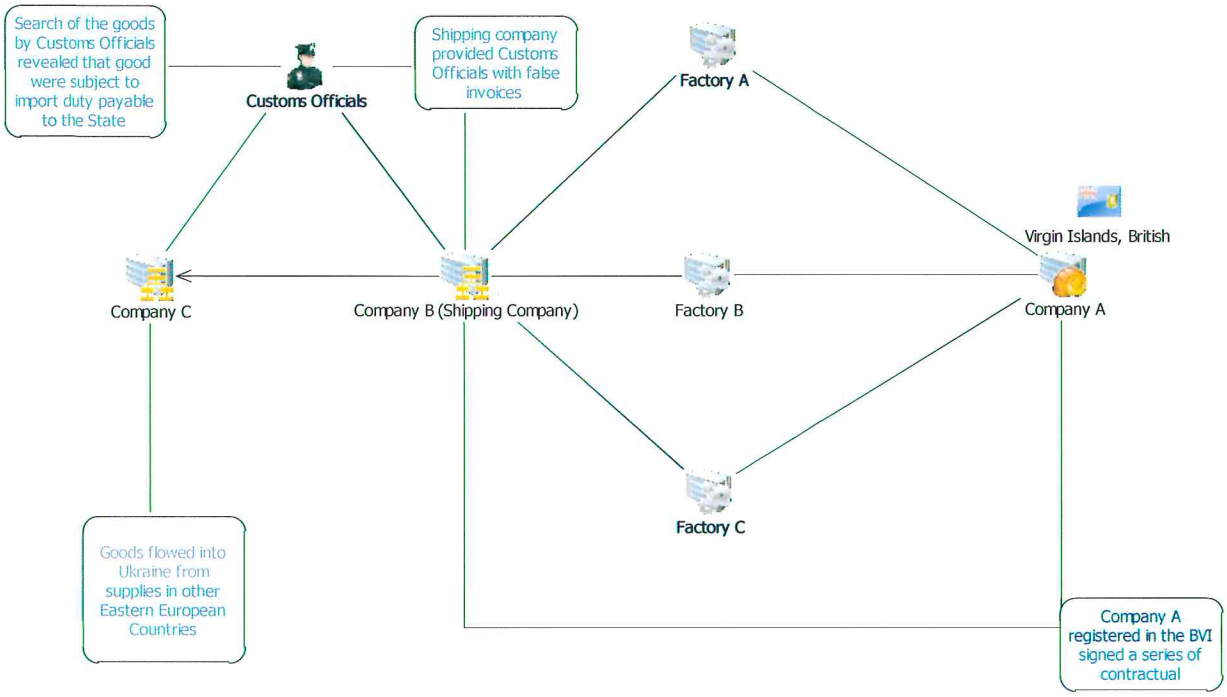
Outcome: Lead broker was indicted by a federal grand jury in the US for insider trading and is awaiting trial.



Case Study 5 Fraud-False Invoicing

Company A, a BVI Business Company signed a series of agreements with a shipping company registered in one of three European countries including Russia from which a number of different pieces of shop equipment were to be purchased and shipped to another Eastern European country. This equipment included refrigerators, show windows, standing racks, and other pieces of furnishers. These items were shipped from various factories in several other European countries. Upon the arrival of the first shipment of goods which arrived in the country of destination, Customs Officials during a routine examination of the goods discovered that the invoices presented by the shipping company did not match the actual equipment. The goods were subsequently seized and an investigation launched.

Outcome: Valuable information and evidence was provided by the FIA via the BVI mutual Legal Assistance process to the authorities in Eastern Europe to assist with the investigation which resulted in the arrest and prosecution of several persons for offences linked to evasion of import duties, false invoicing, and money laundering.



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 4- Financials Reports 2010 (**see the following pages numbered 1-11**)