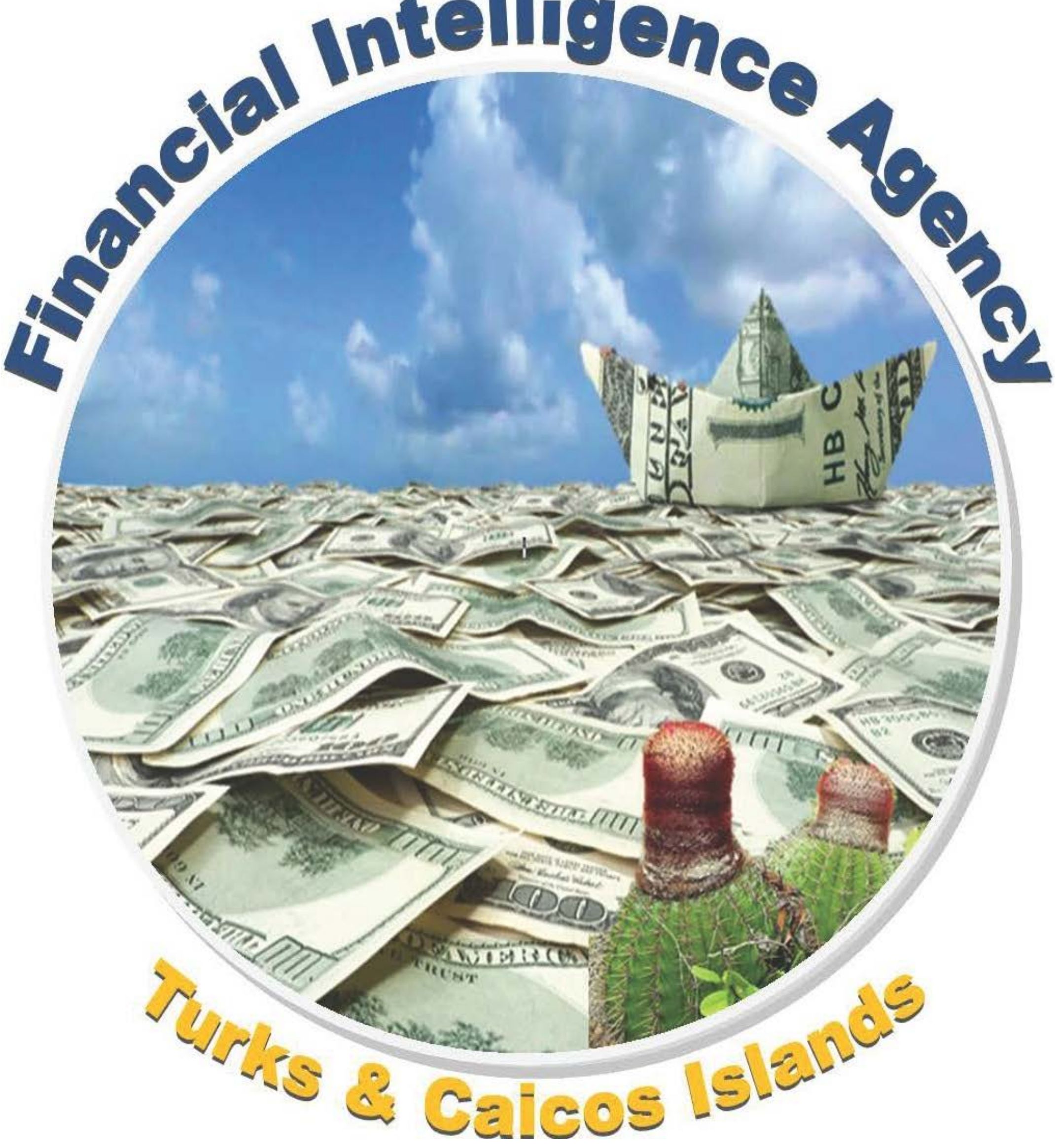

2014 Annual Report

FINANCIAL INTELLIGENCE AGENCY
TURKS AND CAICOS ISLANDS
203 Cabot House, Graceway Plaza
Leeward Highway
Providenciales
Turks and Caicos Islands
Tel: 649 941 7691
Fax: 649 941 7470
Email: fcutcipd@tciway.tc

April 2015

His Excellency the Governor
Mr. Peter Beckingham
Waterloo
Grand Turk
Turks and Caicos Islands

Your Excellency.

I hereby submit the report of the activities of the Financial Intelligence Agency for the period January 1st to December 31st 2014.

This annual report is submitted in accordance with Section 114 of the Proceeds of Crime Ordinance 2007, CAP 3.15.

Dwayne Baker, CAMS
Director
Financial Intelligence Agency
203 Graceway Plaza, Cabot House
Leeward Highway
Providenciales
Turks & Caicos Islands

Attch: FIA Annual Report 2014

Contents

Director's Report

In 2014 the Turks and Caicos Islands saw the passage of key pieces of legislation which have an impact on the Financial Intelligence Unit which since the passage of the FIA Ordinance 2014 is now called the Financial Intelligence Agency of the Turks and Caicos Islands FIA-TCI. The FIA Ordinance is described as "An ordinance to establish the Financial Intelligence Agency as an independent agency to receive reports of suspicious transactions from financial institutions and other persons; to gather, store, analyse and disseminate information to law enforcement authorities and relevant bodies; and for connected purposes.[1]" The FIA Ordinance establishes an independent statutory body to fulfil the responsibilities as described above. Having been proclaimed in October 2014 this signalled a six month period which was allotted for the transition of the Agency from the Royal Turks and Caicos Islands Police Force. Another key piece of legislation passed and enacted was the Prevention of Terrorism Ordinance 2014 - "An ordinance to implement the United Nations convention respecting the suppression of the financing of terrorism; to provide measures to prevent and combat acts of terrorism; and for connected purposes."[2] There were also amendments to the Proceeds of Crime Ordinance. These legislative instruments seek to address deficiencies which were highlighted in the third round of The Financial Action Task Force FATF Mutual Evaluations and seek to remedy some of the lingering issues affecting the Turks and Caicos Islands advancement from the third round and achieving overall compliance with the FATF 40 recommendations. It should be noted here that the Turks and Caicos Islands is in the process of conducting a National Risk Assessment which will seek to identify challenges faced in the Anti-Money Laundering/ Prevention of Terrorist Financing AML/PTF[3] regime using a risk based approach. This exercise is being conducted in preparation for the fourth round of mutual evaluations which will seek to measure and assess the effectiveness of the TCIs AML/PTF systems. The FIA

[1] Short title FIA Ordinance 2014

[2] Short Title Prevention of Terrorism Ordinance 2014

[3] AML/PTF has the same meaning as AML/CFT under the legislation of the TCI and Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010

has extended considerable efforts in this exercise along with other agencies, notwithstanding resource and technical constraints.

The FIA maintained its presence in various International forums through its annual participation in the Egmont Group of Financial Intelligence Units and Caribbean Financial Action Task Force plenaries. Active participation by the FIA and other stakeholders is evidenced by participation in the work of these bodies. The TCI is presently a Co-chair of the CFATF Risks Trends and Methods Group CRTMG which seeks to conduct regionally focused studies on various AML/PTF issues and prepares reports for broad distribution on its findings.

Looking ahead 2015 is expected to be one of new beginnings and further rationalisation of our work, activities and systems with the establishment of the Financial Intelligence Agency. I hope that you find this report informative and look forward to being of continued service nationally and within the wider AML/PTF community.

Dwayne Baker, CAMS
Director
FIA-TCI

Abbreviations

AML/ CFT	Anti-Money Laundering/ Combating the Financing of Terrorism
AML/PTF	Anti-Money Laundering/ Prevention of Terrorist Financing
CFATF	Caribbean Financial Action Task Force
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
FSC	Financial Services Commission
KYC	Know Your Customer
LEA	Law Enforcement Agency
LLEA	Local Law Enforcement Agency
ML/FT	Money Laundering/ Financing of Terrorism
NRFB	Non regulated Financial Business
POCO	Proceeds of Crime Ordinance 2007 (and its amendments)
POTO	Prevention of Terrorism Ordinance 2014
RTCIPF	Royal Turks and Caicos Islands Police Force
SAR/STR	Suspicious Activity Report/ Suspicious Transaction Report

Suspicious Activity/ Transaction Reports

In 2014, the period under review, the Financial Intelligence Agency FIA received 47 Suspicious Activity/ Suspicious Transaction Reports SARs/STRs. This figure reflects a 7.8% decrease in the number of SARs/STRs submitted when compared to 2013. While there was a decrease in the overall total for 2014, SARs/STRs hereafter 'reports' from the banking sector increased by 2 or 8%. For the last three years 2012, 2013 and 2014 majority of reports submitted have come from the banking sector.

Reports from Trust companies and Money Transmitters increased by 2 each representing a percentage increase of 100% over the previous year.

There were 3 reports filed by Company Services Providers in 2014 which represents a decrease of 75% when compared to the 12 reports submitted in 2013. There was a slight decrease of 14.3% of reports submitted by attorneys at law/ law firms.

Inclusive of the 47 reports received, there were two reports in the category of 'other' which fall outside of the categories of entities required to report as prescribed by the provisions under the Proceeds of Crime Ordinance POCO and the Regulations.[4]

A further break down of the 47 reports received for the period shows that financial businesses submitted 32 reports and Non Regulated Financial Businesses NFRBs[5] or Designated Non-Financial Businesses and Professions (DNFBPs) submitted 13 reports.

Within the grouping of financial businesses, the banking sector contributed 81% of the reports submitted while within the DNFBPs grouping, attorneys/law firms contributed 46% of the submitted reports within that category.

Table 1
SARs/STRs Received 2012-2014

Reporting Entities and Others	2014	2013	2012
Commercial Banks	26	25	11
Insurance Companies	2	3	2
MSBs	4	2	2
Mutual Funds	0	0	0
Investment Dealers	0	0	0
Attorneys-at-law	6	7	6
Trust Companies	4	2	2
Company Management	3	12	0
Accountants	0	0	0
Real Estate	0	0	0
Casinos	0	0	0
High Value Dealer	0	0	0
Other	2	0	0
TOTAL	47	51	23

Table 1- Source: FIA-TCI

[4]The POCO CAP 3.15, Anti-Money Laundering and Prevention of Terrorist Financing Regulations.

[5] NRFB is the term used in TCI regulations.

Table 1. SARs/STRs were received from various financial businesses and Non Regulated Financial Businesses.

Figure 1. below shows a comparison of the number of reports submitted by the reporting entities by category for the three year period 2012 to 2014.

Reports submitted by commercial banks represent the majority of reports received over the three year period.

SARs/STRs by entity 2012-2014

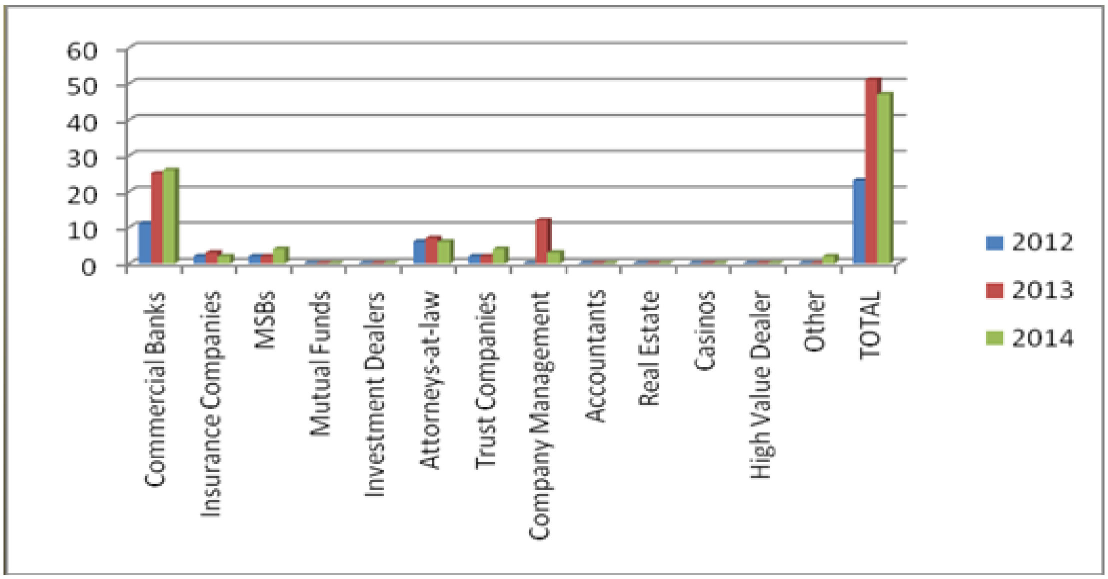

Figure 1-Source: FIA-TCI

Figure 2 shows the contrast between the number of reports submitted by financial institutions and NRFBs for the period 2012, 2013 and 2014. In 2013, there was a sharp increase of 100% in the number of reports submitted by the financial institutions in contrast to the previous year.

That increase was attributed mostly to the increase of submissions from commercial banks. NRFBs also recorded a sharp increase of 162% with company service providers contributing mostly to that rise.

During 2014 the FIA recognized an increase of 1 report or 7% from financial institutions while there was a noticeably sharp decrease of 38% in the number of reports made by NRFBs.

50% of the reports submitted by NRFBs came from attorneys-at-law while company service providers and trust companies accounted for 33% and 17% respectively. No reports have been made by other reporting entities within this grouping. This has been the case for the last three years.

Reports by financial institutions and NRFBs (DNFBPs)

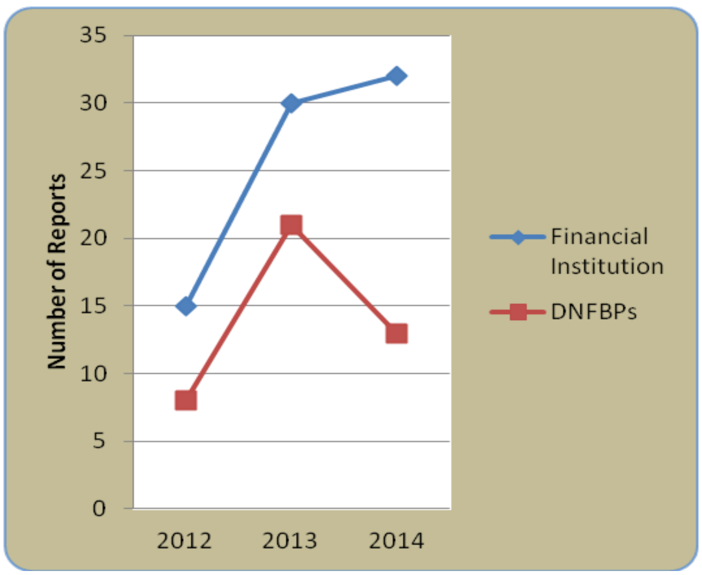

Figure 2- Source: FIA-TCI

Reports filed by NRFB (DNFBPs) for 2014

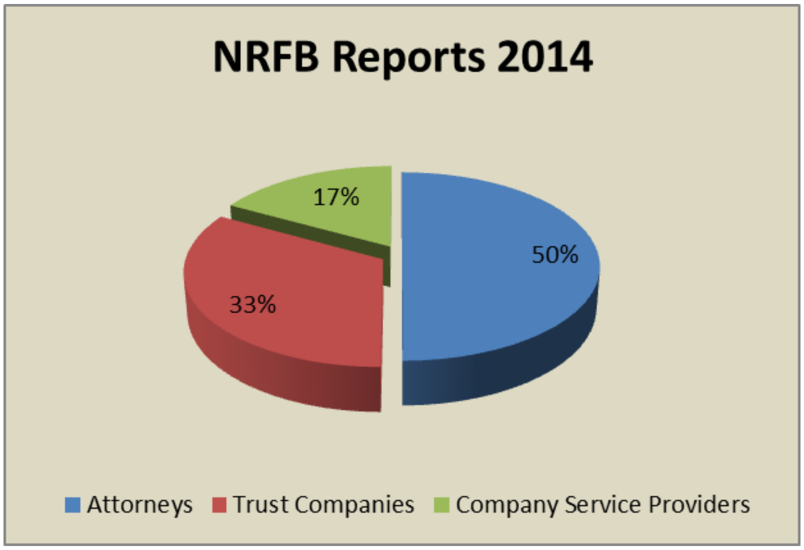

Figure 3- Source: FIA-TCI

Of the reports received by the financial institutions for this period under review, commercial banks accounted for 81% of the reports submitted. Money Service Businesses and Insurance Companies accounted for the remainder of reports filed with 13% and 6% respectively.

Figure 4: Reports made by Financial Institutions for 2014.

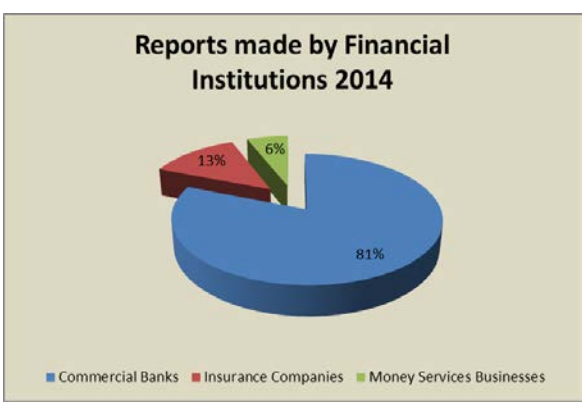

Figure 4-Source: FIA-TCI

Value of transactions Reported as Suspicious

The total value[6] of funds reported as suspicious for the period under review was USD18, 362,181.44 while in 2013 the figure was USD15, 610,731.00. The total for 2014 consisted of 16 reports with monetary values while those for 2013 consisted of 24 reports. All reports with monetary values within both periods were in US currency with the exception of

[6]Total value of transactions filed was not reflected in previous reports by the FIA. The total for 2014 represents 53% of the reports received while the total for 2013 represented 45%.

one report that referenced Canadian dollars[7]

The difference in value for 2013 and 2014 was USD2, 751,450.44, an increase of 18%. This increase was due to a higher dollar value attached to a few of the SARs/STRs. The amounts referenced do not include attempted transactions. Attempted transactions[8] reported as SARs/STRs in 2014 accounted for 11 of the 47 reports filed with a total value of USD50, 450,345.89. One attempted transaction accounted for more than 80% of this figure and represented business that was declined based on adverse information obtained by the reporting entity following their customer due diligence.

The FIA recognizes the valuable efforts of reporting entities in understanding and mitigating the risk associated with the handling and assessing of some transactions and their role in the protection of their respective entities, clients and customers and the country as a whole to the attending risks. Conversely, some lapses were identified on the part of a few of the reporting entities in their failure to carry out proper due diligence and assessment particularly in relation to requests for wire transfers purported to have come from their clients/ customers.

TOTAL VALUE OF TRANSACTIONS REPORTED AS SUSPICIOUS

Actual Transactions	2014	2013	2012
Total Value(USD Million)	18.3	15.6	0.240
No. of Transactions	16	24	5
Attempted Transactions			
Total Value (USD Million)	50.4	0.505	0
No. of Transactions	11	4	0

Table 2- Source: FIA-TCI

Analysis of Financial Transactions[9] by Instruments used

Analysis of reports received for the reviewed period indicated that for the number of actual and attempted financial transactions reported as suspicious, wire transfers were the most utilized and accounted for 12 of the 27 combined reports with monetary values. Overall, 6 of the wire transfer transactions reported as suspicious came about through fraudulent dispositions via email. Three (3) of these frauds were attempts while the other three (3) were successfully carried out with funds transferred overseas to the

[7]USD7014.00 represents the converted amount from Canadian dollars. The Conversion rate at the time was USD. 0.91 to 1 Canadian Dollar.

[8] Attempted transactions include reports relating to a number of scams - overpayment scam, attempted wire fraud, debt collection schemes and business denied due to adverse reports on beneficial owners.

[9]Transactions refer to those reported as being suspicious whether attempted or actually occurred.

value of USD166, 145.00. However, of the total transferred USD160, 695.00 was recovered by recall of the funds from the recipient banks when the entity realised that the fraud had been committed. It was also shown that suspicious transactions where fraudulent cheques[10] were utilized accounted for 7 of the reported cases. Other transactions involving remittances and cash accounted for the remainder of these types of reports.

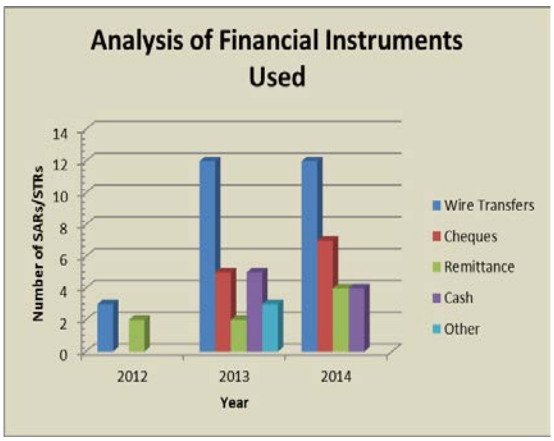

Figure 5- Source: FIA-TCI

Analysis of Reports by Customer Type

Of the 47 SARs/STRs received for 2014, 29 or 62% were reported on natural persons, some of whom had links to one or more legal persons[11]. 18 or 38 % were reported on businesses and corporate entities **See Figure6**

Further analysis of the reports submitted on natural persons[12] who were customers or clients of the reporting entity indicated that 14 or 48 % were deemed to be suspicious for various reasons with regard to their activities and transactions whether carried out or requested. The remainder of the SARs submitted in respect of natural persons were based on other issues such as adverse media reports or as a result of being victims or targets of attempted frauds. Also, for the reports made on legal persons as customers 8 or 53 % were viewed to be suspicious regarding activities and transactions which that legal person carried out or requested.

Figure 6: Reports by Customer Type

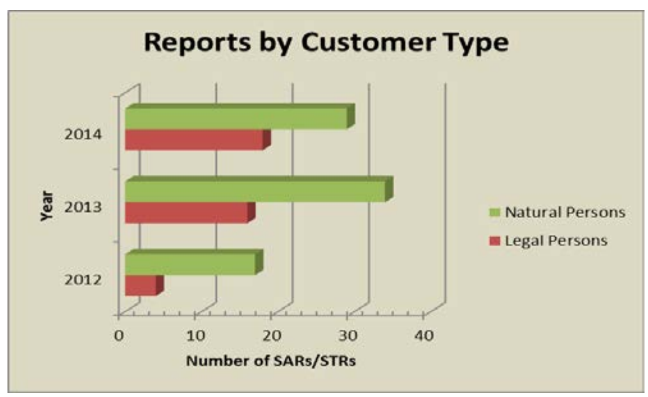

Figure 6 – Source: FIA-TCI

[10] Counterfeit cheques sent by scammers to a number of entities for the purpose of executing their scheme to defraud entities of funds or properties belonging to their clients/customer under the guise of debt collection schemes and overpayment scams.

[11] Legal Person refers to non-human entities. E.g. corporations, partnerships, government agencies.

[12] Natural Person refers to a human being

Reasons for Filing Reports

From all the reports filed with the FIA, it is recognized that suspicious activity and transactions and matters of a fraudulent nature (actual and attempted) accounted for 57% of the overall total. Due Diligence relating to existing customers/clients or potential customers/clients, theft, declined business and others accounted for the remaining 43%. See **Figure 7.**

Types of Activity/Transactions Reported

Some of the submitted reports of suspicious activities are based on factors relating to activities which were inconsistent with the customer profile retained by the reporting entity. In other words, the customer at the stage of establishing a business relationship with the entity may have indicated that the account was for a specific purpose or to receive a specific amount however activities thereafter were found to be inconsistent with their stated profile.

Example:

A customer's account with a bank was credited with USD2.4 million within a month despite their annual expected turnover on the account which was stated to be in the range of USD50, 000 to USD300, 000.

From a transactional view point, some of the suspicious transactions included third party transactions, large cash transfers, structuring of multiple deposits below the bank's reporting threshold and small structured money transfers (remittances) to multiple individuals in different jurisdictions.

Other suspicious reports were based on unusual requests by individuals purporting to act on behalf of legal persons.

Example:

B purporting to be the attorney for company X a company incorporated in country Z, contacted a law firm in country Z to solicit their services to hastily have company X voluntarily struck from the company register even though company X is managed by another firm.

Overall, the reporting entity is not required to determine that a crime has been committed. Once the activity or transaction appears to be irregular, questionable or inconsistent with the customer's known legitimate business indicating possible money laundering or terrorist financing a report that suspicion must be made to the FIA.

Fraud/Attempted Fraud

Persons perpetrating fraud continue to utilize the internet to target a various entities, their customers and individuals, to put into action their craft geared at separating entities and individuals of their funds or other valuables.

From the reports received that were attributed to fraud and attempted fraud, the FIA identified that most were internet derived or initiated. In many instances, at some point there was email correspondence between the reporting entities and fraudsters/criminals purporting to be prospective clients/customers. In other instances information of known customers was used to make requests such as requests for wire transfers or enquiries as to the amount of funds in a client's account. These requests to the entity were made to appear as though they came from the known customer/client of that entity. In some instances where the fraud was detected sending institutions were able to successfully recall the transfer. These frauds was primarily targeted at banks, lawyers/law firms and real estate practitioners and consisted of known schemes such as wire fraud, phishing, over payment scams, debt collection scams and counterfeit cheque fraud.

Another type of fraud reported was cheque kiting for which the FIA received one report. This fraud resulted in losses to the financial institution concerned. In instances where the fraud was quickly detected loss to entities was significantly reduced. While most of the entities were vigilant in identifying the potential frauds, a few fell through the cracks particularly in instances of wire frauds where transfers were executed in line with instructions received via email. Under such circumstances where the actual customer did not make any request for transfers, the indications by customers affected by this fraud were similar in that email compromise or account hacking were reported as the cause.

Reporting entities as a matter of their own internal risk assessments, ongoing Know Your Customer KYC policies and due diligence utilize a number of sources to obtain information on known or prospective clients/customers. Some of these sources are: public records, subscribed information databases, various forms of news media and the internet to name a few. These tools enable entities to make better judgments as to who they take on as new customers and in other cases the extent to which they continue existing business relationships. These various sources of information also assist in assessing and identifying the potential risk of customers who may use their entity as a conduit to launder the proceeds of crime, or facilitate terrorist financing activities.

The internet when used properly can be a useful tool to gather information and in this regard, details of a customer or potential customer's connection to crimes for example arrests, charges, connections to individuals or entities that are the subjects of investigations pertaining to criminal activities particularly money laundering, drug trafficking, fraud, corruption, terrorist financing or regulatory breaches. This information is also useful to the FIA as it can be an effective in determining the extent of a reported subject's business relationship, business interest or possible stake holdings held extraterritorially.

Reasons for Reporting 2014

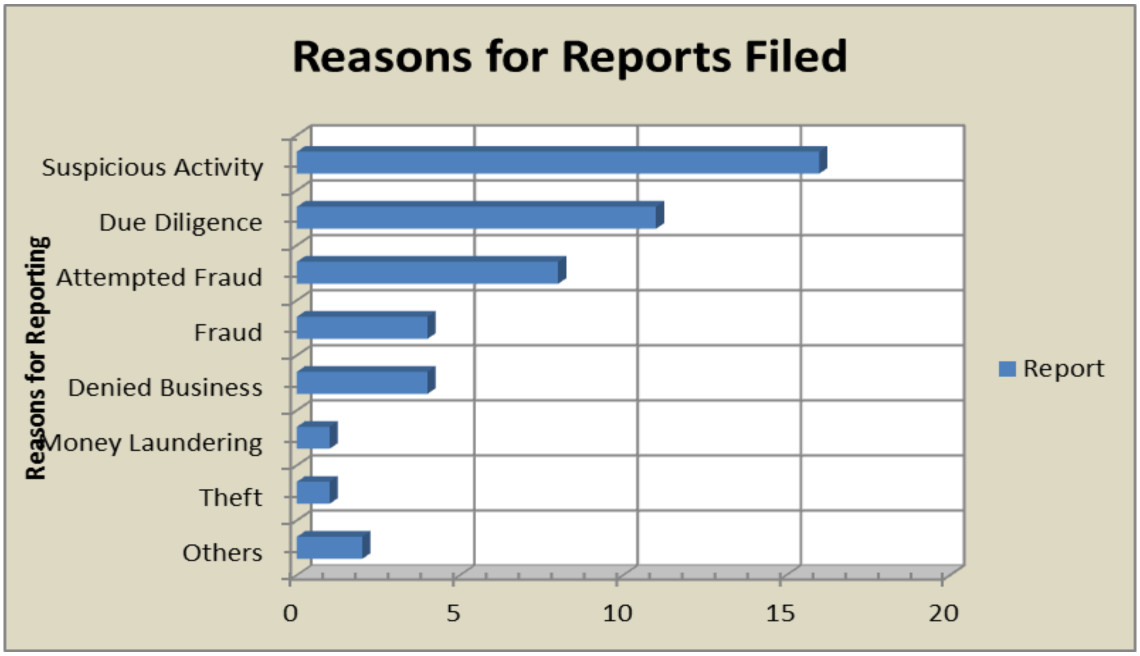

Figure 7- Source: FIA-TCI

Disposition of SARs/STRs

Disseminations of Financial Intelligence

Intelligence reports generated from SARs/STRs are vital in assisting law enforcement and government agencies whether local or International in combating money laundering, financing of terrorism and other serious or related offences. These reports can be the basis of new investigations into suspected criminal activities, or regulatory breaches; help in ongoing investigations or assist in the tracing of proceeds of crimes.

For the period under review, Sixty eight 68[13] reports were analysed from which 31[14] intelligence reports were generated. The 68 reports were inclusive of the 47 reported SARs/STRs filed in 2014 and 21 SARs/STRs carried over from 2013 requiring ongoing analysis. Of the 31 intelligence reports generated 6 were disseminated to the Royal Turks and Caicos Islands Police Force RTCIPF; 1 to the Immigration Department; 1 to the National Insurance Board and 23 to overseas FIUs and Law Enforcement Agencies LEAs.

Of the 23 Intelligence Reports disseminated to overseas counterparts, 7 were sent to the United States, 6 to Canada, 3 to the United Kingdom, 2 to Bermuda and 1 each to Denmark, the United Arab Emirates, South Africa, Hong Kong and St. Kitts and Nevis. **See Figure 8**

Figure 8: Disseminations by Country

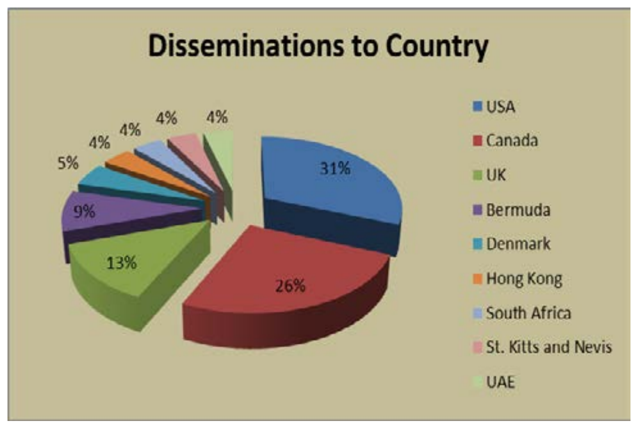

Figure 8-Source: FIA-TCI

Handling of SARs/STRs Received

Of the 68 SARs/STRs reviewed, in-depth analysis was conducted on 45 reports which were later filed for intelligence purposes or required no further action. The remaining 24 reports required ongoing analysis. Table 3 shows the disposition of SARs/STRs received for 2012-2014.

[13] This figure consists of a combination reports for 2014 and previous years representing ongoing analysis.

[14] 25 SARs/STRs contributed to 31 intelligence reports generated. Multiple intelligence reports were created from two or more SARs/STRs.

Table 3: Disposition of SARs/STRs Received

ACTION TAKEN	2014	2013	2012
Number of SARs/STRs received	47	51	23
Ongoing Analysis	12	11	10
SARs/STRs filed as intelligence	35	40	13
SARs/STRs resulting in disseminations	25	9	8

Table 3- Source: FIA-TCI

Requests for production of Information

As part of the FIA's legal responsibility to receive, analyse and disseminate SARs/STRs, requests are routinely made to relevant entities and government agencies for information. These requests are made for the purpose of clarifying or developing the information disclosed within SARs/STRs.

Other functions of the FIA include: liaising with local and International law enforcement agencies with whom periodic assistance may be provided in response to requests for information which is provided on an intelligence basis. Conversely, the FIA makes similar requests to our overseas counterparts for information to enhance the analysis of SAR/STRs and assist in local investigations.

To facilitate requests made by local and International law enforcement, the FIA in most circumstances makes further requests to the relevant entities or government departments/agencies in order to obtain relevant and necessary information to conduct proper analysis and make informed decisions.

In 2014, the FIA made 141 requests for information[15] to various financial institutions and government agencies consisting of 84 requests to financial institutions and 57 to government agencies. Of the 84 request to financial entities, those to commercial banks accounted for 86% followed by company management with 5% and other entities 9%.

Information requested from financial institutions may include but is not limited to account opening information; customer transaction history, bank statements, company documents particularly articles of association and memoranda of understanding to name a few.

[15] A request to entities for information does not include such covered under privileged material or subject to attorney client privilege. The power to request information was found under Section 109 of the Proceeds of Crimes Ordinance; this section has since been repealed and the power is now found under Sec. 28 of the FIA Ordinance 2014.

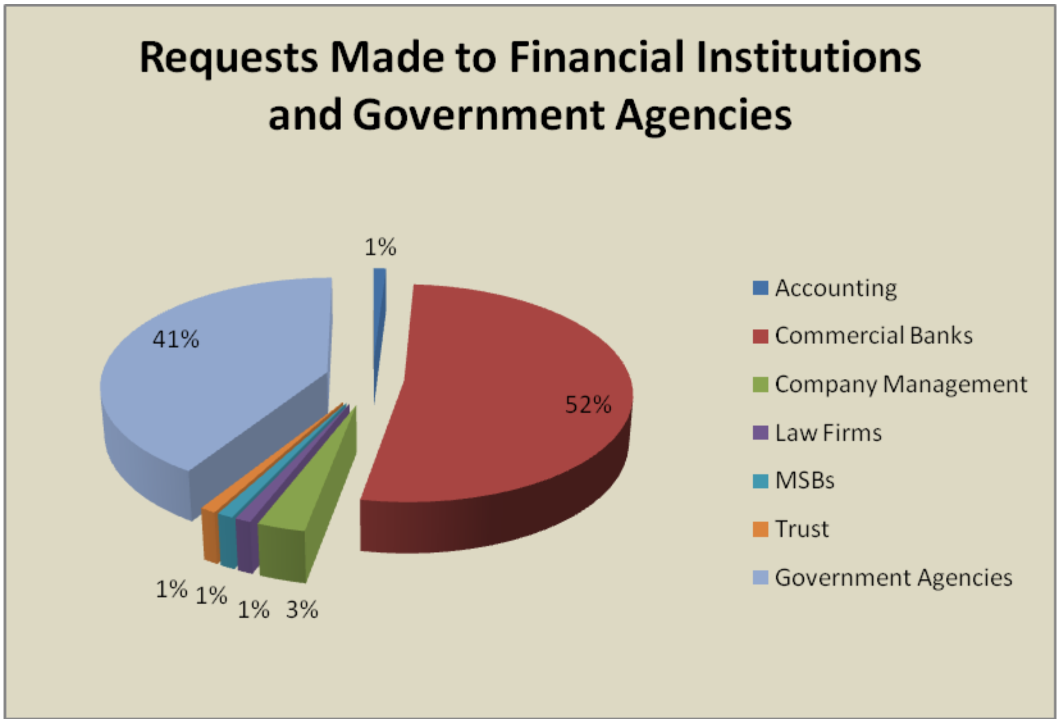

Figure 4-Source: FIA-TCI

Figure 9 shows a breakdown of local requests made by the FIA.

International Co-operation

International Co-operation is important in the fight against money laundering and terrorist financing, but this can only be accomplished when countries establish the appropriate mechanisms to facilitate mutual cooperation.

With countries signing on to treaties, MOUs, and actively participating in groups such as the Financial Action Task Force FATF, Egmont, the Caribbean Financial Action Task Force

CFATF and others, it opens the door for communication and correspondence with each other. This communication includes the voluntary disclosure of information relating to money laundering, terrorist financing, drug trafficking and other crimes; garnering assistance on investigations; restraint and forfeiture of assets; tracing the proceeds of crimes; and sharing knowledge, expertise and training in the conducting of investigations among others. The FIA-TCI is able to facilitate such assistance in these instances is on a FIU to FIU basis through the Egmont Secure network. Others forms of communication may involve direct contact between law enforcement agencies and their counterparts in their respective jurisdictions.

Local and International Requests

In 2014, the FIA made 22 requests for assistance to LLEAs and overseas counterparts and received 27 requests for assistance from local and overseas law enforcement agencies and FIUs. A total of 12 requests came from local enforcement agencies and 15 from overseas counterparts comprising 11 different jurisdictions. Overall, this figure when compared to the 35 requests received in 2013 showed a decrease of 57%. On a similar note regarding the figures for 2013, most of the requests received in 2014 came from the USA with 5, while 10 other jurisdictions made one (1) request each. **See figure 10**

The FIA made 8 outgoing requests for information with 8 different countries, one (1) request less than the total number for 2013.

Table 4

Incoming and Outgoing Requests[16]

2014			
Requests for Assistance	**Local**	**Overseas**	**Total**
Requests sent by the FIA	22	8	30
Responses received	22	7	29
Requests received by the FIA	12	15	27
Responses sent	11	14	25

Table 4- Source: FIA-TCI

[16] The 15 International Request received by the FIA are inclusive of 11 request from Overseas FIUs and 4 from overseas enforcement agencies.

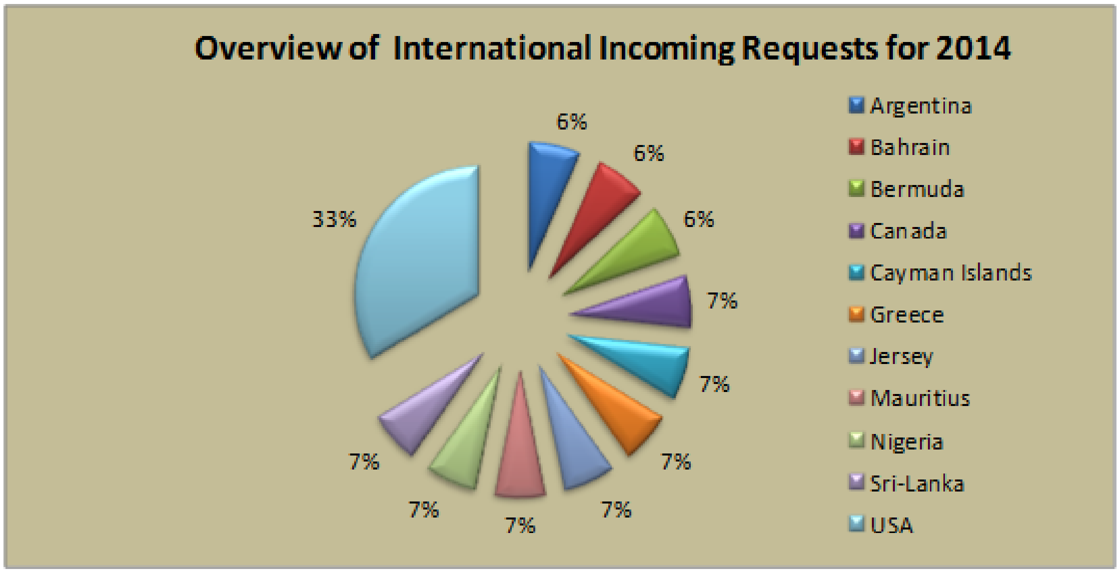

Figure 10-Source: FIA-TCI

Figure 10 showing incoming requests for assistance received by the FIA.

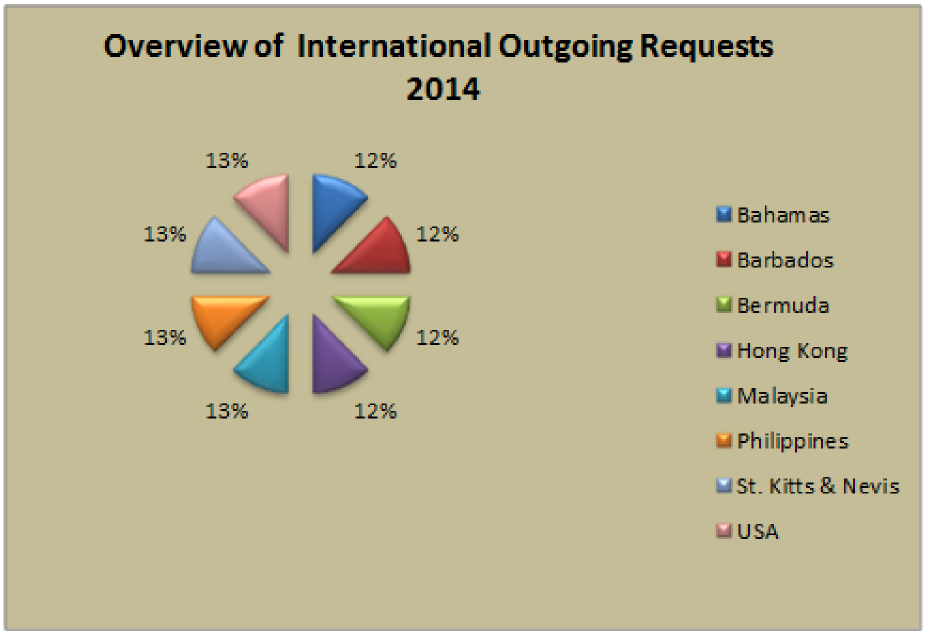

Figure 11-Source: FIA-TCI

Figure 11showing all outgoing requests for assistance by the FIA to other Countries.

Figure 12-Source: FIA-TCI

Figure 12 gives an overview of the number of incoming and outgoing International requests for the period 2012 to 2014.

Trends and Typologies

Continued Trend - Wire fraud

The FIA observed for the review period the continued threat of wire fraud both actual and attempted through email compromise, attempted counterfeit cheque schemes, and debt collection scams. This has caused significant challenges to reporting entities and their customer/clients alike. There have been cases of actual wire frauds akin to the previous year in which a number of funds were wire transferred to a number of countries. Recall of these funds has been varied.

Typology

Email Compromise/ Wire Fraud[17]

An individual purporting to be an account holder with a bank in country (A) sends instructions via email requesting a transfer in the amount of USD5000.00 to an account with a bank in another country. The email also indicated that the client was out of the country and their only available communication was by email. The bank proceeded with the instructions and the amount requested was sent to a bank account held in another country. Shortly after (realizing

[17]The total of USD 166,145.00 was transferred through such fraudulent schemes to a number of jurisdictions including the UK, USA and Malaysia. However, a vast majority of that amount was successfully recalled from the recipient banks as a result of the customers indicating they didn't send any instructions for such transfers.

the success of their fraud) instructions were received for a second transfer by the bank in Country (A). This raised concerns at the bank. The true beneficial owner of the account from which the funds were debited was contacted by the bank and it was confirmed that the customer did not send any instructions for transfers and further stated that there was a compromise of their email. Efforts to recall the funds transferred were futile.

Indicators:

- *Instructions were sent by an individual purporting to be the beneficial owner of the account held with the bank*.
- *The bank was of the view the instructions came from their customer's email account* and unwittingly wired the funds.
- *The email account of the beneficial owner was compromised and apparently the unknown individual (fraudster) mirrored same to effect the fraud.*
- *The funds credited to the account with the recipient bank were immediately withdrawn once the transaction was completed.*

Outreach and Awareness

The FIA continued its outreach in 2014 partnering with the Financial Services Commission (FSC) in these efforts. It is hoped that this aspect of the FIAs operations can be improved with increased capacity in the Agency.

Table 5: Record of Outreach and Awareness Events

Date	Event	Audience	Number of participants	Summary of Event/ Purpose
21/06/14	Bar Association Seminar – Beaches Resort Provo	Attorneys and Law Firms	41 + 4 presenters	Reasons for AML/PFT framework (AG's Office), Myths and Realities of Money Laundering, Obligations and Vulnerabilities of Legal Sector, Writing a Compliance Program (FSC), suspicious Activity Reporting (FIA)
07/10/2014	NCS E-money Services AML/PTF and regulatory Awareness	Money Service Business staff (all levels)	11 + 3 presenters	This was a collaborative effort with the Financial Services Commission. A background on money laundering, description of what ML and terrorist financing is, legal responsibilities and penalties, Suspicious Activity Reporting and preparation of guidance manuals were discussed.

Table 5: Source FIA-TCI

FIA Alerts and Notices

The FIA issues Alerts and Notices to reporting entities as fraudulent schemes arise where they are or may be targeted. These alerts are intended for the protection of the financial system and for all stakeholders to be aware of the threat posed by such schemes should the individuals be successful. The Alert Notices issued by the FIA in 2014 were related to cheque fraud, card cloning and email fraud. Copies of these alerts can be viewed in Appendix A, B and C.

Appendix A

1/2014 12 February 2014

Turks and Caicos Islands Financial Intelligence Unit (TCIFIU)

ALERT – Credit Card Cloning

The TCIFIU has received information indicating that within recent weeks members of an organized criminal gang have been travelling throughout the Caribbean using cloned credit cards to withdraw cash from ATMs. It is believed that the card holders whose cards they cloned are of French origin and the cards purported to have been compromised in Europe.

It is believed that members of the gang are of Eastern European origin and possibly travelling in small groups. The countries visited by the groups so far include, Anguilla, Antigua, Barbados, Puerto Rico, St. Lucia, and Guadeloupe.

Two Mastercards® used by one of the groups have the last digits 6916 and 2958 respectively and were detected in Anguilla in early February 2014.

Our research on cloning revealed the following information:

- Unsuspecting to the customer the information from their credit cards can be copied using a skimmer device when used at restaurants, gas stations, super markets etc by a recruiter of criminal gangs.
- Criminals can install skimming devices over the slot where you insert your card at an ATM machine.
- Hidden cameras may also be used to record your pin at the ATM machine or as you use the keypad terminal to enter your pin at service areas.
- The skimming device can then be attached to a computer and the data is used to create a duplicate of the credit card.
- Another machine can be used to swipe your credit card and the information is then copied from the card's magnetic strip. That information is then transferred to a blank card by swiping that blank card through the machine.

While we are aware that banks routinely network with each other and share information. TCIFIU is sending this alert out of an abundance of caution and in accordance with our obligation to notify entities when we have been alerted to certain trends especially where specific entities are targeted.

Appendix B

2/2014 28 April 2014

Turks and Caicos Islands Financial Intelligence Unit (TCIFIU)

ALERT – Email Fraud

The Financial Intelligence Unit and local law enforcement continue to receive reports of the accounts of customers and clients of various entities being hacked, and those email accounts used to send instructions to said entities in order to execute some form of transaction purported as coming from their known customer/client.

It is important that institutions receiving such requests via email enact necessary safeguards to reduce the instances of such fraud. This could include but is not limited to follow up phone calls to the client, requesting verification via an alternate email address and carefully matching email addresses against those on record. For instance, example@fraudmail.com vs exampl@fraudmail.com. Some fraudsters rely on simple changes or alternations in the spelling of an email address to test an entity's systems.

While entities may have the minimum contact information required on file with regard to each customer, it is important to have other lines of contact to which the relevant entities can correspond with their customers to verify that they are the originators of requests sent via email, especially those involving the transfer of funds.

To date a considerable amount of money has been wire transferred from a number of client/ customers' accounts to accounts in other countries. In most of these cases, once the funds reach the destination, it is withdrawn, comingled with other funds or go through a complex cycle of wire transfers thus making the job of tracing the funds very difficult.

End

Appendix C

3/2014 01 May 2014

Turks and Caicos Islands Financial Intelligence Unit (TCIFIU)

ALERT – Cheque Fraud

Financial Institutions and entities handling financial transactions are asked to be on alert for cheques being sent by post or physically delivered to their entities in the following format (see next page). A number of local institutions have received these cheques. These cheques have been identified as fraudulent. Correspondence received from the following email address - hartwelljonnrodney@yahoo.com should also be flagged as suspicious. The FIU has notified its international counterparts of this fraud so as to assist in curtailing this activity and to ultimately identify the perpetrators. A sample of the cheques received by local institutions in the mail can be viewed below (see next page).

This notice is intended for the recipients to whom the TCIFIU has disseminated it only. Any request for further dissemination should be made directly to the FIU.