TURKS AND CAICOS ISLANDS
FINANCIAL INTELLIGENCE UNIT

ANNUAL REPORT 2013

Table of Contents

Abbreviations

AML	Anti Money Laundering
CFATF	Caribbean Financial Action Task Force
CFT	Counter Financing of Terrorism
FATF	Financial Action Task Force
FCU	Financial Crime Unit
FID	Financial Investigations Division
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
MLRA	Money laundering Reporting Authority
POCO	Proceeds of Crime Ordinance
RTCIPF	Royal Turks and Caicos Islands Police Force
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TCIFIU	Turks and Caicos Islands Financial Intelligence Unit
TCI	Turks and Caicos Islands
UN	United Nations

TURKS AND CAICOS ISLANDS
FINANCIAL INTELLIGENCE UNIT
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 15th 2014

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

Your Excellency.

I hereby submit the report of the activities of the Financial Intelligence Unit for the period January 1st to December 31st 2013.

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

Dwayne Baker Insp. (Ag.)
Royal Turks & Caicos Islands Police Force
Officer in Charge Financial Intelligence Unit
203 Graceway Plaza, Cabot House
Leeward Highway
Providenciales
Turks & Caicos Islands

Report of the Officer in Charge

In 2013 the Turks and Caicos Islands Financial Intelligence Unit continued to carry out its mandate in the anti money laundering and the combating of the financing of terrorism effort AML/CFT. Through our constant efforts and within the constraints of our resources we continue to play our part as the repository for the receipt, analysis and dissemination of intelligence, thus ensuring that the Turks and Caicos Islands maintains its good reputation regarding its local and international commitments relating to anti money laundering and combating the financing of terrorism. This is partly evidenced in a number of international cases for which the FIU has played an important role in bringing money launderers to justice.

Due to the nature of our operations is often difficult to share our successes as we work behind the scenes to facilitate and support investigations aimed at bringing to justice those that seek to do our community harm or otherwise cause significant reputational damage.

2013 saw an increase in the number of suspicious activity reports submitted to the FIU. Some of this increase may be attributed to increased awareness and outreach and a better appreciation for the role that all responsible citizens and residents play in preventing and disrupting these types of activities.

The FIU continues to show its commitment to international AML/CFT efforts by actively participating in and attending meetings bodies which we are members of such as the Caribbean Financial Action Task Force CFATF which provides opportunities for regional counterparts to share experiences and knowledge on AML/CFT issues and to report on various members progress towards achieving full compliance with the Financial Action Task Force revised 40 recommendations.

The TCIFIU will continue to execute its responsibilities with professionalism, mindful of the important role we play in this global AML/CFT effort.

Dwayne Baker

Officer in Charge

Suspicious Activity reports 2013

Summary

In 2013, the Turks and Caicos Islands Financial Intelligence Unit received a total of fifty-one 51 Suspicious Activity Reports (SARs) from various reporting entities in the Turks and Caicos Islands. The Majority of these reports were submitted by commercial banks and company services providers with 24 or 47% and 12 or 23.5% respectively from those entities.

By comparison in 2012, the Turks and Caicos Islands Financial Intelligence Unit (TCIFIU) received a total of twenty three (23) Suspicious Activity Reports (SARs) from various reporting entities in the Turks and Caicos Islands. The majority of the reports for this period were submitted by commercial banks and attorneys with 11 or 48% and 6 or 26% respectively.

REPORTING ENTITIES	2013	2012
Attorneys/ Law firms	07	06
Casinos	00	00
Commercial Banks	24	11
Company Services Providers	12	00
Insurance Companies	03	02
Money Transmitters	02	02
Private Banks	01	00
Trust Companies	02	02
Totals	51	23

Table 1: SARs comparison 2013 and 2012

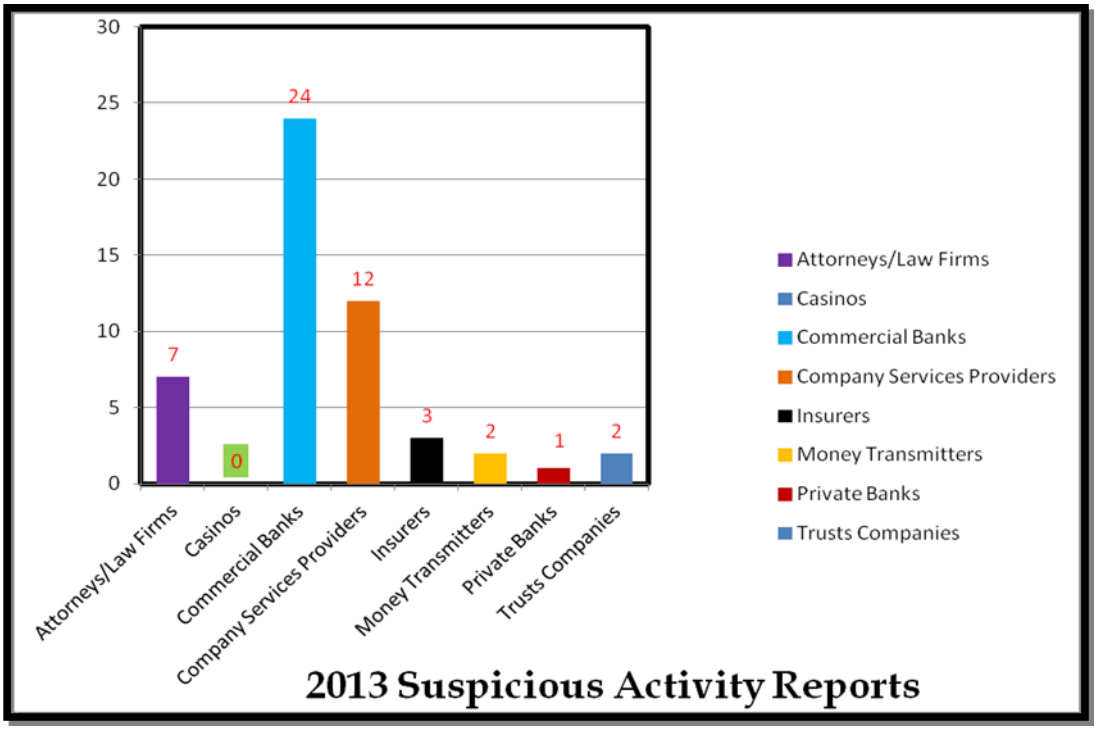

Figure 1 SARs by Sector 2013

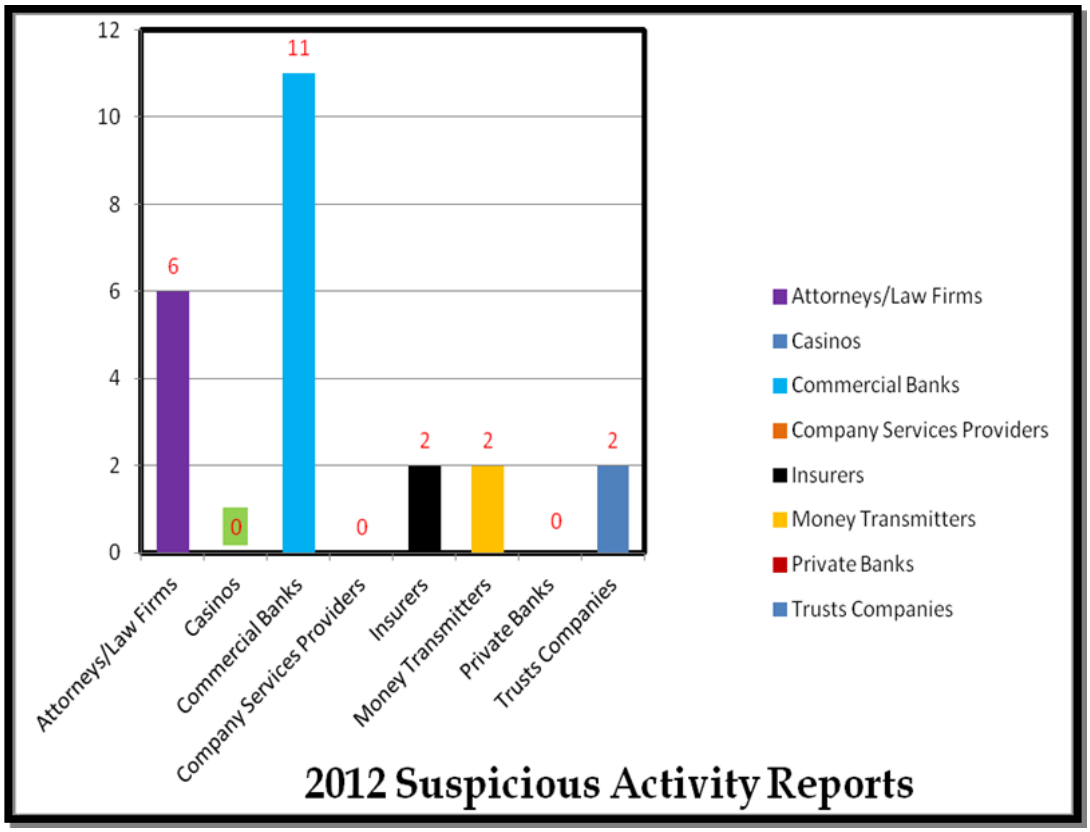

Figure 2 SARS by Sector 2012

Summary continued

The number of SARs submitted for the 2013 review period increased by 28 or 122% when compared to the same period in 2012. In 2013, attorneys/ law firms submitted seven (7) SARs compared to six (6) in 2012.

The number of reports sumbitted by the commercial banks increased from eleven (11) in 2012 to twenty four (24) in 2013, an increase of 118 % from the previous year.

There was a noticable increase of seven (7) reports or an increase of 120 % regarding submissions by company services providers for the period 2013 compared to zero reports in 2012.

Insurance companies submitted three (3) reports for this reviewed period compared to two (2) for 2012. As indicated in our 2012 report, these reports came from the international offices of the insurance agencies rather than from their locally based offices nonetheless these reports still form part of our statistics.

The number of SARs submitted by trust companies and money transmitters remained the same for this review period when compared to 2012. Two reports each were submitted by these entities in 2013 and 2012. One (1) report was submitted by the private banks compared to zero in 2012. There were no submissions from casinos in 2013.

Overview of Suspicious Activity Reports

STRs/SARS	2013	2012
Received	51	23
Investigations by the FIU	08	05
Closed	22	08
Ongoing Analysis	21	15
Spontaneous Dissemination	08	09

Figure 3 SARs 2013 & 2012

- Reports that are under investigation represent those which are ongoing and connected to matters still actively being investigated by the FIU (locally) or in conjunction with counterparts in other jurisdictions.

- Closed reports refer to matters where no further action was deemed necessary after enquiries were exhausted.

- Spontaneous disseminations are those where the information provided within the SARs/STRs was disseminated to other FIUs and law enforcement agencies LEAs as intelligence or to assist with investigations.

- Ongoing Analysis refers to reports for which further information has been requested and responses pending to further enhance the analysis process.

  Reports submitted to the FIU have been based on some of the following indicators:

  - The frequency and size of transactions;
  - The customer has been charged with money laundering related offences, awaiting trial or sentenced;
  - Suspect third party transactions;
  - Compromise of customers' account resulting in wire fraud.

Requests for Information

In most matters reported to the FIU, additional information is needed to enhance the analysis of SARs/ STRs, hence requests for information are made under Section 109(2) (b) of the Proceeds of Crimes Ordinance 2007 Chapter 3.15 which gives the FIU that authority to do so. Most requests for information were met in a timely manner; this demonstrates an understanding of the important role played by the entities especially in facilitating this aspect of their ML/FT responsibilities.

Requests for information are also made to other government agencies which are vitally important in providing the necessary information in order for the FIU to conduct proper and meaningful analysis.

For the reviewed period 154 requests for information were sent to the relevant entities such as banks, law firms, company management providers. 83 requests were made to various government agencies.

Typologies and Trends

In the AML/CFT context, the term "typologies" refers to the various techniques used to launder money or finance terrorism. Criminals are very creative in developing methods to launder money and finance terrorism. Money laundering and terrorism financing typologies in any given location are heavily influenced by the economy, financial markets, and anti-money laundering/counter financing of terrorism regimes. Consequently, methods vary from place to place and over time.[1]

For this period under review, TCIFIU has seen an increase in the amount of reports pertaining to the different schemes and scams used in targeting a number of the reporting entities especially the banks, law firms/attorneys and trust companies and the public at large. Following these reports, the TCIFIU has issued Alerts to the reporting entities and the public to exercise caution and to use express diligence when responding to emails from unknown contacts, unfamiliar and familiar email addresses regarding wire transfers, soliciting of service to collect payments, phishing and other similar schemes. Some of these schemes are perennial.

The following are edited versions of some reported fraud in the TCI which came to the attention of the FIU in 2013. The names of the institutions and individuals have been substituted with other characters to protect their identities.

Typology 1- Phishing

Law firm (A) customer of banking institution (B) received an alert message by email from (D) an unknown person who uses an email address very similar to the authentic email address of (B). (D) sent email alerts as though they were coming from (B) indicating that from a certain date (B) will be introducing new online banking authentication procedures in order to protect the private information of all online banking users.

(A) was only required to confirm their banking details with (B) as they would not be able to have access to the accounts until this had been done. (A) was advised that once the process was completed they would be able to manage their money whenever they want, getting more control of their finances. (A) became suspicious since they do not engage in internet banking. As a result, (A) informed (B) via phone about the emails, (B) informed the customer that it was a scam and that they should disregard such emails.

Key Points:

[1] International Monetary Fund - Anti-Money Laundering/Combating the Financing of Terrorism. http://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

- *It is important for members of the public to be vigilant and make checks with their bank when requested to submit their information from an online source even if the email address is familiar;*

- *Scammers mirrored the email address of the institution to send requests for the banking information of the unsuspecting customers. Should any of these customers respond with their information, the scammers would then use that information to make further requests directly to the bank for funds to be transferred to an account of their choosing.*

Typology 2- Wire Fraud

(X) a law firm, received an email with instructions for a wire transfer of approximately USD90, 000.00 to a third party (beneficiary) (C)**.** This email came from what appeared to be the valid email address of one of their clients who has a trust account with the law firm. (X) proceeded as per the instructions and wired the funds to (C's) account held with a bank in country 2.
Subsequently, (X) received another email with the same instructions for funds to be wired to the same beneficiary however for a larger transfer amount just over of USD100, 000.00. (X) became suspicious of the instructions, and they contacted the client from whose account the request for transfer was sent.

It was discovered that the client's email account was hacked and the requests were fraudulent.
(X) informed their bank and law enforcement of the fraud. Local law enforcement sent a request for assistance to counterparts in country 2.

Law enforcement in country 2 was able to detect and restrain a small amount of the wired funds in (C's) account. The investigation is ongoing.

Key Points:

- *"C" used the email account of X's client to make the request for transfer, and B unknowingly submit to such request believing that it was made by the client.*

- *"C" put their deception to the test and their first attempt proved successful and subsequently made a further attempt.*

- *"X's" member of staff's knowledge of how the client conducted their business prompted them to contact the client.*

Please note the excerpt for typology 2 represents four (4) such reports, in four of these reports the fraudsters/scammers were successful in gaining a total of over USD200, 000.00. These funds were

sent to countries such as Australia, Georgia, Singapore and the USA. Additionally there were some unsuccessful attempts where the entities did their due diligence and contacted their clients to confirm the instructions, thus detecting the attempted fraud. Those attempts had they been successful would have resulted in firms and their clients being defrauded of in excess of USD800, 000.00.

Typology 3

A law firm received an email from (H) of a marketing consultancy firm based in another country. The request was to retain the services of the lawyer to prepare a lawsuit against (J) a local company purportedly for money owing as per work done.

The law firm agreed to take on the client, and sent multiple emails to (H) for the retainer to be signed and fees paid. There was no response from (H) for a prolonged period.
The law firm finally emailed (H) stating that they were no longer interested in doing business with (H). Subsequently, the law firm received in the mail a cheque for USD295, 000.00 from (J), drawn on a bank in country 2 along with a payment plan.

The law firm contacted (J's) office to query the cheque received. The local office of (J) denied knowing (H) or even owing for any consultancy work as purported.
The cheque was confirmed by the bank in country 2 as fraudulent. The lawyer discontinued all correspondence with (H).

Key Points:

- *Non face to face contact can be very problematic without proper verification and references as to the true identity of international clients or customers;*
- *Making references to a known entity may add legitimacy to seemingly legitimate requests or offers until proven otherwise;*
- *Sending a fraudulent cheque and payment plan to gain the lawyer's confidence into believing that they came from a legitimate source is part of the deception*
- *The next possible step would have come in the form of a request for payment of an advance by the scammer.*

International Cooperation

Information sharing serves a critical and significant role in the international community, especially to the global network of financial intelligence units and law enforcement agencies in the fight against money laundering, terrorist financing, drug trafficking and human trafficking among other crimes. Cooperation between FIUs with regard to the exchange of financial intelligence and information is done on a reciprocal basis in accordance with the Egmont Group's best practices for information sharing. Some of the requests for information are facilitated through Egmont while others are channeled to relevant law enforcement agencies.

The table below shows the number of international requests for information received and sent during the period under review from various countries.

JURISDICTION	INCOMING	OUTGOING
Anguilla	01	00
Argentina	01	00
Bahamas	01	00
Canada	07	05
Guernsey	01	00
Indonesia	01	00
Jersey	01	00
Latvia	01	00
Lebanon	01	00
Moldova	07	00
Syria	01	00
UK	02	00
Ukraine	02	00
USA	09	04
Total	35	09

Figure 4 International Requests 2013

Of the 35 request received from our international counterparts, 25 of those have been satisfied while 09 are outstanding due to delays in receiving the requested information locally.

Memoranda of Understanding with FIUs

TCIFIU recognizes MoUs as a vehicle by which exchange of information with regional and international counterparts can be facilitated through terms of agreement stipulated within.

For the past year two MoUs were finalized and signed with the Financial Investigations Division Jamaica and the Financial Intelligence Unit St. Maarten. These MoUs were signed at Freeport Grand Bahama on 19th November 2013 on the occasion of the Caribbean Financial Action Task Force CFATF 38th Plenary.

Staff & Training

Staff

There were no changes in staff numbers in the FIU for the period under review. The Money Laundering Reporting Authority Committee has been working to address issues pertaining to the structure of the FIU and continues its work regarding the Financial Intelligence Agency Bill and the establishment of a detached agency.

Training

Staff benefitted from some training and additional exposure in the AML/ CFT field. One officer attended a cash courier's workshop November 4th – 6th 2013, hosted by the Financial Intelligence Division in Jamaica in collaboration with the United Nations. While a second officer received two weeks Financial Investigations training from November 18th -29th 2014 in Anguilla hosted by the Royal Anguilla Police Force.

Staff also attended a one day seminar on anti-money laundering compliance hosted by audit, tax and advisory firm KPMG.

Outreach and Awareness 2013

In 2013 the TCIFIU increased its outreach and awareness and participated in a number of workshops and seminars targeted at persons and entities in the regulated sectors. These sessions addressed a range of topics such as money laundering, suspicious activity reporting, obligations of reporting entities and requirements under the Proceeds of Crime Ordinance 2007 (and its subsequent amendments).

Date	Event	Audience	Attendees	Summary of Event/ Purpose
25/04/2013	Financial Services Commission AML Conference	Accounting, Banking, Attorneys & Law Firms, Government Agencies, Real Estate, Trust & Company Services Providers	90	International Regulations, POCO requirements, AML Risks and Red flags, Developing an AML policy Manual and training, Compliance Officer appointment Guidelines & STR/SAR reporting
April 2013	Newsprint Editorial in the TCI Sun newspaper and Caribbean News Online Network	National	N/A	Anti-Money Laundering Awareness
May 2013	PTV8- On your Mind talk Show	National	N/A	Speakers from the FSC and the FIU took part in this public awareness exercise. Requirements and responsibilities of individuals and regulated entities relating to money laundering and terrorist financing were discussed.
23/10/2013	KPMG Anti-Money Laundering Compliance in Practice	Accounting, Banking, Attorneys & Law Firms, Government Agencies, Real Estate, Trust & Company Service Providers.	160	AML/CFT awareness, Compliance and Regulations
15/11/2013	Captive Insurance Conference	Insurance Companies, Law Firms	80	Captive Insurance in the Turks and Caicos Islands, Regulations & AML Awareness.
03/05/2013	AML/CFT awareness and SAR/STR reporting	NCS EMoney Services Staff	09	Anti Money Laundering and Suspicious Activity Reporting

Figure 5. Outreach and Awareness 2013

Contact Details

Turks and Caicos Islands
Financial Intelligence Unit
203 Cabot House, Graceway Plaza
Leeward Highway
Providenciales
Turks and Caicos Islands
Tel: 649 941 7691
Fax: 649 941 7470
Email: fcutcipd@tciway.tc
http://www.tcipolice.tc/index.php/financial-intelligence-unit