



Bahamas Association of Compliance Officers

"Committed to Compliance"

MESSAGE FROM THE PRESIDENT

FALL EDITION
September 2008

IN THIS EDITION

MESSAGE FROM THE PRESIDENT

The Executive Committee of BACO meets with the Financial Intelligence Unit (FIU)

SUSPICIOUS TRANSACTIONS REPORTING: BEST PRACTICE IN THE ROLE OF COMPLIANCE

BACO CALENDAR 2008

UPCOMING CONFERENCES 2008



Wow! We have had a great second quarter, with an enthusiastic response from you our members, who have consistently supported our efforts to provide training and re-sources relevant to our industry. I am pleased with the

dedication and commitment demonstrated to date by the executive committee in planning and executing meaningful events.

Here are some of the events completed during the second quarter:

* **Half Day Forum**

In collaboration with the Central Bank of the Bahamas, BACO recently held a half day forum on April 22nd, updating you on matters related to Money Transfer Businesses (MTBs), a risk based approach to KYC and onsite examinations. Governor Wendy Craig has pledged her support to continue such joint efforts.

* **BIFS Annual Week of Seminars, Topic: New Developments in the Compliance Field**

Members of the BACO Executive Committee and Mr. Emmanuel Komolafe represented BACO at the Bahamas Institute of Financial Services (BIFS) annual week of seminars. Using presentations and role plays, the team sought to provide the attendees with updates on relevant topics and issues in the Compliance field.

* **6th Offshore Alert Financial due Diligence Conference**

BACO's founding president, Cheryl Bazard, was one of the panellists for a session on the Bahamas at the 6th Offshore Alert Financial Due Diligence Conference.

- * Execution of an administration agreement with the Bahamas Institute of Financial Services
- * Courtesy Visit with the Chief Executive Officer of the International Compliance Association

ICA is in the initial phase of providing our ICA diploma recipients the opportunity to upgrade to a Bachelor of Science in Compliance, more details to come 1st Quarter 2009

- * Guest Appearance on GEMS talk show with host Michael Pintard

Members of the BACO Executive Committee appeared on the talk show, outlining the history of BACO, with a special call in from our Founding President, and promoting our MLRO Day.

- * **BACO's Annual MLRO All Day Seminar**

Compliance & Money Laundering Reporting: The X Factor in Financial Services and Risk Management. During the lunch session of the programme, Hon. Min. Zhivargo Laing pledged his support and reaffirmed his ministry appropriation of \$25k contribution to BACO for its continuing training activities

The second quarter is now at a close. As we prepare for the third quarter, we are mindful of BACO's objective to provide stimulating and relevant training opportunities' to enrich its membership socially and professionally. For the third quarter we have already planned several exciting events, but just to name two of them: in July BACO will host a special assembly to feature a panel discussion on the riveting topic: Economic Partnership Agreement (EPA), with the lead panellist being the Hon. Min. Zhivargo Laing. Also a special "members only" cocktail event is scheduled to be held at Lucianos, which will provide a good networking forum for members to get to know each other better.

The continued success of our association is largely dependent on the involvement of our members, thus we implore you to get involve and take advantage of the opportunities as offered by your executive committee.

Yours truly,

Fabian Bain
BACO's President

BACO's EXECUTIVE COMMITTEE



President - Fabian Bain
(Banca Del Gottardo)



Executive Vice President - Denora Butler
(Credit Suisse Trust)



Vice President- Marsha Ferguson
(Itau Private Bank)



Treasurer- Pauline Seymour
(Banco Santander)



The Executive Committee of BACO meets with the Financial Intelligence Unit (FIU)

By Valentino Bethel

FIU Representatives present:

Anthony Johnson, Director
Edward Smith, Deputy Director

BACO Executive Committee present:

Denora Butler, Exec. Vice President
Marsha Ferguson, Vice President
Jasmin Strachan, Secretary
Kesna Pinder, Asst. Secretary
Cheryl Fox, Asst. Treasurer
Valentino Bethel, Social & Public Relations Chair
Mario Smith, Education Committee
Joan Rahming, Education Committee

The Executive Committee of The Bahamas Association of Compliance Officers paid a courtesy call to the Financial Intelligence Unit on March 17th, 2008. They had the pleasure to meet with Mr. Anthony Johnson, Director and Mr. Edward Smith, Deputy Director.

Greeting and an introduction of the new Executive Committee were brought by Mrs. Denora Butler, Executive Vice President. Mr. Johnson expressed a warm welcome to the Executive Committee, whilst endorsing the purpose and vision of BACO and encouraging the new committee to remain steadfast to the core principles and cause for which BACO was formed. Director Johnson was also pleased to advise the new committee of the pleasant relationship the FIU has built with BACO over the past few years.

BACO's mandate for 2008 was presented to the FIU. After expressing great enthusiasm, Director Johnson committed the FIU to play a key and strategic role in the upcoming Annual MLRO Day scheduled for June 18th, 2008.

The topic of 'vetting procedures' for Money Laundering Reporting Officers was a burning discussion between BACO & the FIU. Director Johnson reiterated the commitment of the FIU to policing the industry and ensuring that minimum standards are put in place for the designation of MLRO's.

'Legislations and Guidelines' were another hot topic for this meeting. Among those discussed were, The Financial Transactions Reporting Act 2000 (FTRA), The Financial Transactions Reporting Regulations 2001 (FTRR), The Anti-Terrorism Act 2004, the Ministerial report for the Bahamas from CFATF, and the FIU 2005 & 2006 Report.

Deputy Director Smith who also serves on the Egmont Committee was able to advise that the next CFATF meeting will be held in Haiti later this year, and the next mutual evaluation meeting will be held in three years.

SUSPICIOUS TRANSACTIONS REPORTING: BEST PRACTICE IN THE ROLE OF COMPLIANCE

By Andrea Singleton - Saunders



The International Monetary Fund has estimated that the aggregate size of money laundering in the world is between 2-5% of the world's gross domestic product. This would equate to an average of USD 590 billion to USD 1.5 trillion of money laundering on an annual basis. It is clear from these estimates, that money laundering and terrorist financing are issues which can not be ignored and every employee within each financial institution must do their part to ensure that any and all suspicions of money laundering and terrorist financing within their institution are duly reported internally to their respective Money Laundering Reporting Officer, as financial institutions act as "protectors" of The Bahamian financial services industry.

When a Suspicious Transaction Report is made, what should be reported?

When a Suspicious Transaction Report is made, what should be reported?

A suspicious transaction has been defined as a "financial transaction in which there are reasonable grounds to suspect the transactions are related to the proceeds of criminal conduct as defined by the Proceeds of Crime Act, 2000 or any offence under the Proceeds of Crime Act and the Anti-Terrorism Act, 2004 which include the commission of a money laundering offence."

As per the Financial Intelligence Unit's: Suspicious Transactions Guidelines relating to the Prevention of Money Laundering and the Financing of Terrorism for financial institutions in the Commonwealth of The Bahamas, a suspicious transaction would "often be one which is inconsistent with a customer's known legitimate business, activities or lifestyle or with the normal business for that type of financial services product." As a prerequisite to recognizing a suspicious transaction, it is imperative for the financial institution to know the client and the client's usual business activity in order to determine when such client's transac-

tions may be considered unusual.

Clause 58 of the Financial Intelligence Unit's Suspicious Transactions Guidelines states that based on patterns of a customer's legitimate business, a suspicious transaction may fall within on or more of the following categories:

- Any unusual financial activity of the customer in relation to such client's usual activity;
- Any unusual transaction in the course of a usual financial activity;
- Any unusually linked transaction;
- Any unusual use of an intermediary in the course of an usual transaction or financial activity;
- Any unusual method of settlement; and
- Any activity which raises doubt about the client's true identity.

The type of situation that gives rise to suspicion will depend on an analysis of the customer base and the range of products or services offered to the customer. It should be noted that when considering whether a transaction may be considered to be suspicious, there is a need to consider all of the relevant information in relation to the respective person and his/her business. One of the key questions which should be asked when considering whether a transaction may be considered to be suspicious is: "Does it make sense?" If ones answer to this question is no, an internal suspicious transaction report should be duly completed and submitted to the MLRO as soon as possible for the form of suspicion to be further analyzed. Is there too much reporting?

The Financial Intelligence Unit of The Bahamas (the "FIU") has reported that from January 2001 – December 2006, it has received a total number of One thousand One Hundred and Seven (1,107) Suspicious Transactions Reports ("STR's"). The major grounds for the submission of STR's were cash transactions (19%), accounts not in keeping with KYC rules (17%), media/publicity (13%) and internet searches

(9%). Based on these statistics, one may raise the question whether there is too much reporting? I am of the view that there is not enough reporting as:

- The majority of the STR's which were submitted to the FIU between January 2001 – December 2006 were received from banks (92%, being, 1018). Accordingly, other financial institutions and other entities only submitted 8% of the remaining STR's – being 89 reports.

- On average over a period of 5 years, there have been less than 200 STR's submitted to the FIU per year.

- All financial institutions as per the Financial Transactions Reporting Act, 2000 have a mandatory duty to report any transaction where the financial institution knows, suspects or has reasonable grounds to suspect that such transaction involves the proceeds of criminal conduct under the Proceeds of Crime Act (Section 14, FTRA). Such statistics raise the question whether every financial institution is carrying out this duty with the utmost diligence.

- Pursuant to Section 43 of the Proceeds of Crime Act, 2000, all persons who acquire knowledge or suspicion of a person being engaged in money laundering during the course of such person's trade, profession, business or employment have a duty to report such matters to the relevant authorities. In the event a person fails to report the same, such person may be guilty of an offence.

The reporting of suspicious transactions by financial institutions and other entities to the FIU is a bold statement that such entities will not tolerate the use of their entity as a conduit for criminal. Such reporting is also essential for the detection, analysis and prosecution of those involved in money laundering and the financing of terrorism within our country.

Best Practice: Internal procedures: reporting suspicious transactions to MLRO

Each financial institution is required by law to appoint a Money Laundering Reporting Officer ("MLRO"). Such person would be responsible for the independent assessment of all internal suspicious transaction reports and the determination of whether or not a formal STR should be made to the FIU. Best practice for employees to internally report suspicious transactions to the MLRO are as follows:

- Everyone within the institution must know who the MLRO is. It should not be a secret or a guessing game.

- There should be an internal reporting procedure which has been communicated and is accessible by all staff. Such procedure may be within a local compliance policy;

- The reporting lines should be as minimum as possible between the person reporting the suspicion and the MLRO;

- An internal report should include the following information – based on Section 43 of the FIU's, Suspicious Transactions Guidelines:

- o The reporting department/branch;
- o Full details of the customer/client including, name, address, date of birth, occupation or profession and nationality or country of residence;
- o Full details of the reason suspicion has been raised;
- o The date the suspicion was raised by the respective employee;
- o Any connected account which the person who is reporting is cognizant of; and
- o The date and time of the report.

- The MLRO should provide the person who reported the suspicion with a written acknowledgment of receipt of the internal suspicious report;

- The MLRO should inform the person who reported the suspicion of their decision whether or not a report will be made to the FIU;

- The MLRO should maintain a written record of all internal suspicious transactions whether the same are reported or not;

- The MLRO should remind the relevant staff members of their obligation not to do anything which would prejudice inquiries by contacting the customer or a third party related to the customer and disclosing the information to such person as the same is an offence ("tipping off"); and

- The MLRO should also inform the relevant staff members that because an internal suspicious report was submitted their duty to report suspicious transactions does not cease as they are still obligated to report any additional forms of suspicion in relation to the relevant customer or account.

Best Practice: Risk assessment analysis of customers (KYC) and transactions (KYT):

As per international standards which are evident within the Customer Due Diligence for Banks issued by the Basel Committee on Supervision, which provides a forum for regular cooperation on banking supervisory matters for Central Banks on all aspects of

banking supervision, recognized that adequate KYC policies and procedures are important for the safety and soundness of banks. Additionally, the Financial Action Task Force ("FATF"), an inter-governmental body whose purpose is to develop and promote national and international policies to combat money laundering and terrorist financing, as per their revised 40 recommendations on anti-money laundering and combating the financing of terrorism recommended that financial institutions adopt a risk based approach on customer due diligence. The FATF has also drafted "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures, issued June 2007 which provide best practice principles in the implementation of an effective risk based approach.

Locally, the Financial Transactions Reporting Act, 2000 and the Financial Transactions Reporting Regulations, 2001 required that financial institutions developed and implemented a risk based approach when verifying customers. Additionally, the Central Bank of the Bahamas issued a guideline to licensees to assist them to develop a risk based approach.

Taking into account the international and local standards, best practice of a risk based approach for both customers and transactions as per the Central Bank of The Bahamas' Anti-Money Laundering Guidelines should include the following:-

- The differentiation of client relationships by risk categories (low, medium, high) and risk factors (products, client type, country of domicile, complexity of ownership of legal structure, source of business, type of business, type of assets, size and volume of transactions, type of transactions and cash transactions);
- KYC documentation and due diligence information requirements appropriate for each risk category and risk factor;
- A process for the approval of the downgrading/upgrading of risk ratings;
- Ongoing monitoring policies and procedures which assist in the identification of higher risk customers in relation to money laundering or funding of terrorist activity;
- Review of accounts to determine whether a client's risk rating should be adjusted;
- Enhanced due diligence procedures for those clients considered to be higher risk customers, for example PEP's;
- Adequate training of all staff in their legal obligations, internal policies and procedures respecting the reporting of money laundering and the financing of terrorism.

The FATF's Guidance on the Risk Based Approach to combating money laundering and terrorist financing specifies that the most commonly used risk criteria are: country or geographic risk, customer risk and product/services risk. The weight a financial institution would assign to each risk would depend on its specific circumstances. Country or geographic risk may take into account: countries subject to sanctions and embargoes, countries which lack appropriate anti-money laundering and countering the financing of terrorism laws and regulations, countries with designated terrorist organizations operating within them, and countries identified as having significant levels of corruption or other criminal activity. Customer risk would determine which groups of customers pose a higher risk and the potential impact any mitigating factors would have on the assessment. For example, a higher risk customer assessment may include: customers who operate cash businesses such as money services businesses, casinos, betting and other gambling related activities. Product Risk would take into account the potential risk associated with new and existing products an institution offers its customers.

Certain risk variable of a particular customer or transaction may also affect an institutions risk assessment include assessing the following:

- The purpose of an account;
- The level of assets to be deposited by a particular customer or the size of a transaction undertaken;
- The level of regulation a customer is subject;
- The length of the customer relationship; and
- The familiarity with a country's local laws and regulations and the structure and extent of regulatory oversight.

An institutions specific risk based policy should be determined by an assessment of the institutions operation. Such risk based policy would also allow the institution to identify and access the potential of its money laundering risks associated with customers and transactions and allows such institutions to focus more attention on those customers and transactions which present the greatest degree of risk.

The Role of Compliance

As per the Basel Committee on Banking Supervision: Compliance and the Compliance function in banks "Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the board of directors and senior management lead by example. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities."

Pursuant to Regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2001, a financial institution is required to appoint a Compliance Officer. Generally, a Compliance Officer is responsible for managing "compliance risk" which is the "risk of

legal or regulatory sanctions, material financial loss or loss of reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities" (Basel Committee on banking Supervision: Compliance and the compliance function in banks). Specifically, a Compliance Officer would have the following responsibilities within an organization:

- Drafting and implementing internal guidelines within the organization. This responsibility would include ensuring that the origination policies are adhered to by all employees and are in accordance with local legislation, industry standards and best practice. Also such policies should be updated as necessary;
- Ongoing monitoring account transactions and accounts within accounts both manually and electronically in order to detect unusual or suspicious transactions;
- Reviewing proposed new client relationships and all of the relevant documentation (such as I.D., POD, source of wealth and source of funds) to determine whether or not the organization should enter into such relationships. Such review would ensure that the documentation is in line with internal policies and local legislation requirements and ensuring that the information provided is plausible. It is important for no funds are accepted from the proposed client before the account is approved by Compliance;
- Training all staff in respect of anti-money laundering legislation, internal policies, anti-money laundering prevention and countering terrorist financing. In order for the compliance officer to adequately train staff, they themselves must also be trained. In this regard, it is important for compliance professional to obtain regular training on new development within the compliance field, anti-money laundering and countering the financing of terrorism;
- Advising Senior Management and other staff members on various compliance related issues including laws, regulations and new developments which would be applicable to the organization. It is important for the compliance officer to have sufficient experience and knowledge of the industry and the relevant laws and regulations which affect the industry;
- The Compliance Officer's function should be independent of the business of the organization. This would allow him/her to be objective when analyzing compliance related issues. Such person's function should not create a conflict of interest within the organization. For example, as a matter of best practice, the compliance officer should not also be the CEO of the organization as the CEO would be concerned about the overall business and profitability of the organization as opposed to making a decision which takes into account the risk involved. Their objectivity in decision making may be prejudiced; and
- In order for a compliance officer to be effective in their job it is imperative for such person to have access to all of the information they require about the clients, the business and the organization as a whole.

It is important for there to be a compliance culture within the organization in which Senior Management and the remainder of the employees are cognizant of their respective responsibilities within the organization to mitigate risk within the organization.

UPCOMING CONFERENCES

- Euromoney Training – Managing and Measuring Operational Risk
July 7-10, 2008 and November 17-20, 2008
New York City
<http://www.euromoneytraining.com/Americas>
- IIA – International Internal Auditors
2008 Governance, Risk, & Compliance Conference
August 18-20, 2008
Palm Beach, FL
http://www.theiia.org/training/conf/index.cfm?e_code=EVT579
- ACAMS 7th Annual International Money Laundering Conference & Exhibition
September 8 - 10, 2008
Las Vegas, NV
<http://www.acams.org/conferences/annual08/default.aspx>

New challenges

Generally, as expressed within the FATF's Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, "Money Launderers and terrorist organisations have considerable knowledge of the financial sector and take extreme measures to hide their financial activities and make them indistinguishable from legitimate transactions." As this continues to be a general challenge, more specifically, the following new challenges present themselves:-

- Terrorism – Since the inception of the Anti-Terrorism Act in 2004, only 2 STR's were filed with the FIU in 2006 in relation to terrorism as per the FIU's Annual Report 2006. It is important for financial institutions and other entities to be able to detect terrorist financing. The challenge arises as terrorist organizations may receive support and funding from legitimate sources for illegal purpose which may not be as easy to detect as a traditional money laundering case which involves the proceeds of criminal conduct.
- Compliance and Tax issues – For those institutions with Qualified Intermediary status, compliance must ensure that the client's within their institution are QI compliant. This may create a challenge as it is important that a client is correctly placed within the right category. Additionally, the Tax Information Exchange Act ("TIEA") may also increase the role of Compliance within institutions in the event information on a client is requested from an institution in accordance with the TIEA; and
- Money Services Business: the service it provides of allowing persons to transfer funds across the world may be used by money launderers and terrorist financiers. The regulations and issues which money services business present would be addressed by Hubert Edwards.

Compliance will continue to be faced with new challenges as institutions business and products expand but the key in dealing with the challenges and mitigating the risk it presents involve identifying and assessing the risk, developing and implementing appropriate policies and procedures, training the relevant employees who would be affected by the policy and ensuring the policy is adhered to and adequate by conducting independent reviews of the same on a periodic basis.

Conclusion

In conclusion, in order for our fight against money laundering and the financing of terrorism to be effective and to adequately protect our second industry, institutions must ensure that their policies and procedures include suspicious transactions reporting procedures and documented risk assessment policies of customers and transactions. We must always bear in mind that as gatekeepers of the financial industry of The Bahamas, we must ensure that we act in a manner which upholds our jurisdiction as a major participant in the global fight against money laundering and countering terrorist financing.

- AICP – Association of Insurance Compliance Professionals
Annual Conference 2008
October 5 - October 8, 2008
Atlanta, Georgia
<http://www.aicp.net/annualconference/future.cfm>
- IT Governance, Risk and Compliance Conference
October 8 – October 10, 2008
Orlando, Florida, USA
<http://www.isaca.org/Template.cfm?Section=Conferences&Template=/Conference/ConferenceDescByReqClass.cfm&ConferenceID=187>
- 18th Annual Anti-Money Laundering Audit and Compliance Forum
November 10-12, 2008
Marriott Marquis, NYC
<http://www.iirusa.com/AMLAC/welcome.xml>