The Commonwealth of The Bahamas

Financial Intelligence Unit
Annual Report 2016
Government of The Commonwealth of The Bahamas

June 29, 2017

The Hon. Peter Turnquest, M.P.
Minister of Finance
Ministry of Finance
Cecil Wallace Whitfield Centre
Cable Beach
Nassau, The Bahamas

Dear Minister,

I am honoured to submit the Annual Report which outlines the work of the Financial Intelligence Unit for the period January 1st to December 31st, 2016.

The Annual Report is submitted in accordance with section 10 of the Financial Intelligence Unit Act (FIUA), Chapter 367, Statute Law of The Bahamas.

Yours sincerely,

Reuben S. Smith, QPM; RVM
Director
Vision Statement:

"Our vision is for The Commonwealth of The Bahamas to have a robust, dynamic and exemplary financial service industry, free from the scourge of money laundering, terrorist financing, frauds and other criminal conduct."

Mission Statement:

"To proactively network with local law enforcement, regulators and international counterparts to effectively assist in detecting, assessing and eradicating all threats of money laundering and financing of terrorism to the global economy."
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Message from the Director</td>
<td>5-6</td>
</tr>
<tr>
<td>2. Management Team &amp; Organisation Chart</td>
<td>7</td>
</tr>
<tr>
<td>3. Introduction</td>
<td>8</td>
</tr>
<tr>
<td>4. Functions of The Financial Intelligence Unit</td>
<td>9</td>
</tr>
<tr>
<td>5. Money Laundering/Financing of Terrorism, FATF definition of De-Risking</td>
<td>10-11</td>
</tr>
<tr>
<td>6. Improving the quality of Suspicious Transaction Reports/Public Notice/Cyber Crime/Firearms Trafficking/Grand &amp; Petty Corruption/Fraud etc.</td>
<td>12-20</td>
</tr>
<tr>
<td>7. Training</td>
<td>21-22</td>
</tr>
<tr>
<td>9. Overseas Training and Seminars attended by staff members of the FIU</td>
<td>24-25</td>
</tr>
<tr>
<td>10. Annual Statistics of The FIU</td>
<td>26</td>
</tr>
<tr>
<td>10.1 Reporting Period</td>
<td>26</td>
</tr>
<tr>
<td>10.2 General Findings</td>
<td>26</td>
</tr>
<tr>
<td>10.3 Detailed Statistics</td>
<td>27</td>
</tr>
<tr>
<td>10.3.1 FIU Overview 2015</td>
<td>27</td>
</tr>
<tr>
<td>10.3.2 Monthly Statistics of Incoming Reports</td>
<td>28</td>
</tr>
<tr>
<td>10.3.3 Comparative Suspicious Transactions Reporting</td>
<td>29</td>
</tr>
<tr>
<td>10.3.4 Disclosing Institutions</td>
<td>30</td>
</tr>
<tr>
<td>10.3.5 Grounds for Suspicious Transaction Reports</td>
<td>31</td>
</tr>
<tr>
<td>10.3.6 Type of Currency</td>
<td>32</td>
</tr>
<tr>
<td>10.3.7 Nature of Offences – Disclosing Institutions’ Suspicion</td>
<td>33</td>
</tr>
<tr>
<td>10.3.8 Nature of Offences – Financial Intelligence Unit’s Suspicion</td>
<td>34</td>
</tr>
<tr>
<td>10.3.9 Nationality of Contract Partners</td>
<td>35</td>
</tr>
<tr>
<td>10.3.10 Domicile of Contract Partners</td>
<td>36</td>
</tr>
<tr>
<td>10.3.11 Nationality of Beneficial Owners</td>
<td>37</td>
</tr>
<tr>
<td>10.3.12 Domicile of Beneficial Owners</td>
<td>38</td>
</tr>
<tr>
<td>10.3.13 Suspicious Transaction Report - Trends</td>
<td>39</td>
</tr>
<tr>
<td>10.3.14 Investigative Bodies Involved</td>
<td>40</td>
</tr>
<tr>
<td>10.3.15 Requests for Information Received</td>
<td>41</td>
</tr>
<tr>
<td>10.3.16 Status of Requests for Information Received</td>
<td>42</td>
</tr>
<tr>
<td>10.3.17 Requests for Information Sent to</td>
<td>43</td>
</tr>
<tr>
<td>10.3.18 Status of Requests for Information Sent</td>
<td>44</td>
</tr>
<tr>
<td>10.3.19 Status of Requests for the Production of Information</td>
<td>45</td>
</tr>
<tr>
<td>10.3.20 Other Statistics</td>
<td>46</td>
</tr>
<tr>
<td>11. International</td>
<td>47</td>
</tr>
<tr>
<td>11.1 Egmont Group</td>
<td>47</td>
</tr>
<tr>
<td>11.2 Memorandum of Understanding</td>
<td>48</td>
</tr>
<tr>
<td>11.3 Caribbean Financial Action Task Force (CFATF)</td>
<td>48</td>
</tr>
<tr>
<td>12. Typology</td>
<td>49-51</td>
</tr>
<tr>
<td>13. Glossary of Terms</td>
<td>52</td>
</tr>
</tbody>
</table>
1. **MESSAGE FROM THE DIRECTOR**

The Financial Intelligence Unit (FIU) is a member of the Egmont Group of Financial Intelligence Units, an anti-money laundering and combating the financing of terrorism organization consisting of one hundred and fifty-one (151) FIUs as of June 2015. The unit, which was established by an Act of parliament in December 2000, became the 54th member of Egmont in June 2001. It is the national centre responsible for receiving, analyzing, obtaining, and disseminating information which relates to, or may relate to the proceeds of offences specified in the schedule of the Proceeds of Crime Act of the Bahamas, as amended.

For the period under review, the FIU received a total of three hundred and six (306) Suspicious Transaction Reports (STRs) from financial institutions in the Bahamas, inclusive of domestic/offshore banks, offshore banks, casino, trust company, stockbroker, domestic banks, money remittance services, financial advisor, company service provider, credit union, insurance company, and lawyer for analysis. The 306 suspicious transaction reports received in 2016 represents a 3.08% increase in STRs received over the same period in 2015. A number of these reports after analysis were forwarded to the Commissioner of Police for investigation. During the same period, a number of requests for assistance were received from the Royal Bahamas Police Force, foreign financial intelligence units, and regulatory agencies in the Bahamas. The FIU provided invaluable assistance to these entities in the continuous fight against criminal conduct, inclusive of money laundering and terrorist financing.

The FIU intends to further increase its public announcements and notices to ensure that the financial sector and general public are fully aware of new and evolving criminal trends, inclusive of cyber crimes and corruption. The obligation to report suspicious transactions will also be highlighted.

Training of management and staff of financial institutions continues to be a top priority, and in 2016, the unit provided AML/CFT training to one thousand, one hundred and fifty-one (1151) persons, from forty-one (41) different financial institutions. These entities included the Bahamas Association of Compliance Officers (BACO), insurance companies, trust services, banking and corporate services, lawyers and Designated Non-Financial Businesses and Professions (DNFBPs). Staff of the FIU for the year under review, have also attended a number of local and international plenary, conferences, courses and seminars and are fully qualified and experienced in anti money laundering and combating the financing of terrorism trends and the methodology needed to combat its scourge. FIU personnel continue to attend Training Courses facilitated by the Egmont Group of Financial Intelligence Units, as well as other vital training programs conducted by the Caribbean Financial Action Task Force (CFATF) and other expert organizations both locally and internationally.

The FIU is cognizant of the new trends that has, and continue to develop as transnational criminals seek more ingenious ways to commit their criminal acts. We are aware of the prevalence of “hacking” and the many cyber crimes, inclusive of identity theft, advance fee fraud schemes, Nigerian Letter or 419 frauds, ponzi schemes, phishing and other sophisticated fraudulent activities that results. In 2016 the FIU committed to placing greater focus on the issue...
of illicit trafficking of firearms and ammunition and the proceeds derived there from. The threat posed by transnational criminals, in particular that of prolific firearms and ammunition traffickers is ever present, and therefore all law abiding citizens in the Commonwealth of the Bahamas, and indeed the world, must be aware of this threat to global finance, stability, and security. The FIU has taken note of the increased numbers of STRs received in 2016, which relates to fraudulent activities perpetrated by criminals using various social media, including Facebook and email to target unsuspecting victims. An increase in fraud matters against online account holders has also been reported to the FIU for the period under review.

The fight against transnational criminals requires recommitment by all and a redoubling of our collective efforts. At the FIU, we seek to work hand in hand with all stake holders, as we do all that we can to protect our precious financial services industry and the good reputation of the Commonwealth of the Bahamas. We invite and encourage all financial institutions, as defined in the Financial Transactions Reporting Act, Chapter 368, Statute Law of the Bahamas, as amended to duly appoint a Money Laundering Reporting Officer (MLRO) for their respective institution, and to ensure that the MLRO is registered with the FIU. Financial institutions and the general public are also encouraged to continue reporting all suspicious transactions to the FIU.

I take this opportunity to thank the Government of the Bahamas for its continued commitment, support and funding of the FIU. I also wish to thank the dedicated staff of the FIU of the Bahamas for their loyalty and hard work. Additionally, I wish to thank the Royal Bahamas Police Force, other law enforcement agencies, the Group of Financial Service Regulators, financial institutions, foreign Financial Intelligence Units and our many other partners for their tireless efforts in the fight against transnational criminal networks.

_______________________________
Mr. Reuben S. Smith, QPM; RVM
Director
Financial Intelligence Unit

June 29th, 2017
2. MANAGEMENT TEAM

Director: Mr. Reuben S. Smith
Deputy Director: Mr. Basil H. Collie
Legal Counsel: Mrs. Joann Creary
Accountant: Mrs. Kateryann Johnson
Head of Analysis: Mr. Nathaniel Taylor
Manager, Human Resources: Ms. Willamae S. G. Kemp
Manager, Information Technology: Mr. Derrington A. Rahming

ORGANIZATION CHART
3. **INTRODUCTION**

In 2016, the Financial Intelligence Unit continued to provide invaluable service to the Government and people of The Bahamas, as well as to the international law enforcement efforts against the scourge of money laundering (ML) and terrorist financing (TF).

The work of the dedicated men and women of the FIU has commanded the respect and admiration of the financial services sector, regulators and law enforcement officials both locally and internationally.

The FIU has maintained a successful working relationship with its international counterparts, namely, the Egmont Group of Financial Intelligence Units (Egmont), Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF). The FIU is also a member of the Group of Financial Services Regulators (GFSRs) of The Bahamas. As a part of this collaboration the FIU is dedicated to protecting, preserving and enhancing the integrity of the financial services industry in The Bahamas.

The Government of The Bahamas continues to provide adequate funding to the FIU, which assist greatly in the efficiency, effectiveness and development of the Unit. With this support and the collaborative efforts of our counterparts, the FIU plays a pivotal role in combating money laundering and terrorist financing.

The FIU is aware of the formula for success and accedes to the fact that no country or territory can isolate themselves in this fight. It indeed requires the assistance of the government, other regulatory agencies, FIUs and law enforcement authorities.

Notwithstanding the successes that have been realized by many countries to date in combating ML & TF, the need for enhanced collaboration is essential. Thus, issues are being examined and discussed by the Financial Action Task Force (FATF) and other international standard setting bodies in determining the way forward. Through participation in the activities of these international standard setting bodies, the FIU is placed in a unique position to inform and advise the policy makers of issues, which require redress and provide advice on the required time frame to adequately address the same.

Thanks to the Government of The Bahamas, the FIU is intimately involved in the AML/CFT process and pledges its full support to provide advice and recommendations to the relevant agencies. This collaborative approach, allows policy makers to act proactively in the best interest of The Bahamas.

We trust that you would find this Annual Report informative.
4. **FUNCTIONS OF THE FINANCIAL INTELLIGENCE UNIT**

The Financial Intelligence Unit (the “FIU”) from its inception has been an integral element in the fight against money laundering and terrorist financing. The FIU’s mandate is derived from Section 4, Financial Intelligence Unit Act, enacted in 2000, which stipulates that the agency’s core responsibility is to receive, analyse, obtain and disseminate information as it relates to or may relate to money laundering, terrorist financing and other offences as specified in the Schedule of the Proceeds of Crime Act, chapter 93 as amended.

Subsequent to the introduction of various financial legislations, enacted to assist in the global fight against money laundering and terrorist financing, financial institutions are now subject to strict reporting and recordkeeping requirements. The FIU Act, as a result, gave the FIU the authority to receive the disclosure of information that can be utilized in analyzing suspicious transaction reports that are received from financial institutions, outlining incidences of suspected money laundering or terrorist financing transactions. In the furtherance of combating money laundering and terrorist financing, the FIU has the power to order the suspension of a transaction or freeze an individual’s account, where there is a suspicion that the transaction or the funds in the account are related to proceeds of criminal conduct, money laundering, or terrorist financing.

Institutions, that are considered financial institutions, not only have the duty to report suspicious transactions, but have an obligation to also produce information that the FIU deems necessary in carrying out its mandate. Combating money laundering and terrorist financing is more than a national fight but an international one, which requires a reciprocal relationship with other FIUs. The Bahamas is committed to corresponding, cooperating and assisting foreign FIUs in succeeding in this global fight against money laundering and terrorist financing.
5. MONEY LAUNDERING

Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of illegally gained money. In practice, criminals are trying to disguise the origins of money obtained through illegal activities so it appears as if it was obtained from legal sources. Otherwise, they can't use the money because it would connect them to the criminal activity, and law-enforcement officials would seize it.

Also, money laundering is a crucial step in the success of drug trafficking, terrorist activities and white collar crimes, to name a few.

The basic money laundering process has three steps:

I. Placement: At this stage, the launderer inserts the dirty money into a legitimate financial institution. This is often in the form of cash bank deposits. This is the riskiest stage of the laundering process for the launderer because large amounts of cash are pretty conspicuous, and banks are required to report high-value transactions.

II. Layering: Layering involves sending the money through various financial transactions to change its form and make it difficult to follow. Layering may consist of several bank-to-bank transfers, wire transfers between different accounts in different names in different countries, making deposits and withdrawals to continually vary the amount of money in the accounts, changing the money's currency, and purchasing high-value items (boats, houses, cars) to change the form of the money. This is the most complex step in any laundering scheme, and it's all about making the original dirty money as hard to trace as possible.

III. Integration: At the integration stage, the money re-enters the mainstream economy in legitimate-looking form - it appears to come from a legal transaction, arranging for the source of funds to appear legitimate without suspicion of their initial criminal source.

It is important to note that the primary purpose of organized crime is to make profits. Like any business, the purposes of profit are to enjoy it and re-invest it in future activity. For the organized criminal, however, profit close to the source of the crime represents a particular vulnerability and unless the criminal can effectively distance himself or herself from the crime, which is the source of the profit, they remain susceptible to detection and prosecution.

With this in mind, the aforementioned process has devastating social consequences. For one thing, if done successfully, it allows the criminals to maintain control over their proceeds and ultimately to provide a legitimate cover for their source of income. Money laundering plays a fundamental role in facilitating the ambitions of the drug and firearm trafficker, the terrorist, the organized criminal, the fraudster as well as the many others who need to avoid the kind of attention from the authorities that sudden wealth brings from illegal activities. By engaging in this type of activity the criminals hope to place the proceeds beyond the reach of any asset forfeiture laws.
FIGHTING MONEY LAUNDERING

Preventative measures aimed at denying criminals the access to the financial system tend to rely heavily on the private sector’s cooperation. With this in mind, the prime method of anti-money laundering is the requirement for financial intermediaries to know their customers - usually termed KYC (Know Your Customer) requirements. With good knowledge of their customers, financial intermediaries will often be able to identify unusual or suspicious behaviour, including false identities, unusual transactions, changing behaviour, or other indicators that laundering may be occurring. However for institutions with millions of customers and thousands of customer-contact employees, traditional ways of knowing their customers must be supplemented by technology.

TERRORIST FINANCING

Terrorist activities take money, and one way to combat terrorists is to cut off their access to funds.

Unfortunately, it is difficult to precisely define terrorist financing. Terrorism can be conducted without large scale funding and terrorist financing does not always rely on the proceeds of crime or necessarily involve money laundering. Therefore, to understand terrorist financing, it is perhaps more useful to describe the ways funds are raised, moved and used in terrorist activity, rather than attempting to arrive at a specific definition.

Funding of terrorist organizations may be derived from criminal activities such as hijacking, kidnapping and extortion, fraud, thefts and narcotics trafficking.

A key difference between terrorist groups and traditional criminal organizations is that funding for terrorist groups may also include income derived from legitimate sources (such as fundraising in the name of charitable or relief organizations) or from a combination of lawful and unlawful sources.

On 31st December 2004, the Anti Terrorism Act, 2004 was enacted within the Commonwealth of The Bahamas and the Royal Bahamas Police Force has since made counter-terrorism measures a priority.

During the year 2015, the Financial Intelligence Unit received no STRs from financial institutions, which were suspected of being related to terrorist financing

De-Risking
A New Threat to the Financial Sector

The Financial Action Task Force (FATF) defines de-risking as the “phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage risk in line with FATF’s risk-based approach”

De-risking, according to the FATF is being driven by many different factors. FATF also reported that de-risking is a serious concern for the FATF and the FATF style regional bodies, to the extent that de-risking may drive financial transactions underground which creates financial exclusion and reduces transparency, thereby increasing money laundering and terrorist financing risks.

In November, 2015 the FATF issued a statement concerning its efforts to combat de-risking. In order to ensure that AML/CFT measures are being implemented effectively and in line with a risk based approach, the FATF sought to clarify regulatory expectations in four (4) areas relevant to de-risking. The four areas as listed by the FATF can be found on the FATF website under the heading ‘FATF Takes Action To Tackle de-risking. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html
6. **IMPROVING THE QUALITY OF SUSPICIOUS TRANSACTION REPORTS**

Suspicious Transaction Reports (STRs) are one of the main weapons in the fight against money laundering and other financial crimes since these reports generate leads that the Royal Bahamas Police Force use to initiate money laundering investigations. Several key areas to note are as follow:

- It is critical that the MLRO provide the FIU with as much information as possible highlighted by an in depth narrative outlining the series of events in relation to the suspicious activity. Essentially, the MLRO must give a detailed narrative which would identify the five basic elements of information – Who? What? When? Where? and Why?

- The reporting of suspicious transactions is not limited to cash in The Bahamas. Transfers to and from the financial system are also under the umbrella of ‘reporting of suspicious transactions’ and this can provide useful information on the ‘layering’ stage of the money laundering process.

- The keeping of comprehensive transaction records (a requirement by law) by financial institutions provides a useful audit trail and gives useful information on people and entities involved in laundering schemes once discovered.

- A financial institution’s compliance regime should contain ongoing compliance training, at least once a year, in order to keep staff and colleagues up to date.

Ultimately, identifying suspicious activity, and providing support to law enforcement, is critical to the FIU’s mission to safeguard the nation’s financial sector. The ability to analyze data to identify issues, trends and patterns in STR reporting, and educate financial institutions and regulatory partners, is equally critical to our mission. The information gained through STRs is key to carrying out that mission.

**CYBER CRIME**

Cyber-crime is rapidly gaining attention, largely, because it is an entirely new form of crime. Most, though not all, cyber-crime is directly related to criminal activities that have existed in the bricks and mortar society for decades or longer. Indeed, these activities have taken on a scale and scope that was unknown just a few decades earlier and by all appearances, the criminal groups responsible for these crimes only gained the ability to expand their enterprises as a result of the American War on Drugs.

A generalized definition of cyber crime may be “unlawful acts wherein the computer is either a tool or target or both.” The computer may be used as a tool in the following kinds of activity: financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases: unauthorized access to computer/ computer system / computer networks, theft of information contained in the electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

As detailed below, “cyber criminals” are broadly classified into four grouping depending upon their objectives.

- Children and adolescents between the ages of 6 – 18 years driven by a desire to know and explore things as well as to prove themselves among peers;
• Organized hackers who are motivated to penetrate corporate or public sites and databases in order to fulfill political objectives or fundamentalist ideology;
• Professional hackers / crackers who, motivated by money, are primarily employed to hack the sites of rivals to get credible, reliable and valuable information; in some case they are even employed to crack the system of their employer basically as a measure to make it safer by detecting loop holes early;
• Discontented employees who have either been terminated or are dissatisfied with their employer and as revenge, hack the system of their employer.

Cyber crimes may be directed against individuals in the form of harassing e-mails, cyber stalking, obscene material, indecent exposure, e-mail spoofing, defamation, cheating, fraud, viruses, bullying, computer vandalism, intellectual property, internet time theft or unauthorized access/control over computer system.

Cyber crimes directed against an organization may take the form of distribution of pirated software, cyber terrorism against a central government or agency, possession of unauthorized information i.e. trade secrets or unauthorized access/control over computer system.

Cyber crimes directed against society at large may take the form of pornography, indecent exposure, drug / human trafficking, financial crimes, sale of illegal articles, on-line gambling, terrorism and forgery.

Globalism and the internet have transformed radically the nature of criminal activity. In particular, the internet has made it easy for organized crime groups to commit crimes across borders, taking advantage of the obstacles which law enforcement officials encounter when trying to work together across international boundaries. This is particularly challenging for the global community, considering the linkage between narcotics trafficking and related criminal activities of money laundering, terrorism, human trafficking, and cyber-crime. This linkage can be traced in one way or another to the Drug War.

Closely related to cyber crime is the phenomenon of cyber laundering. This is a new way to hide the proceeds of crime. The advance of technological solutions of electronic payments and online gambling has eliminated the need for time and space as compared to the traditional way of money laundering to achieve Cyber laundering. Any means other than the provided ways to transfer goods and services using cyber space technologies and information systems for personal benefits using deception is considered as cyber laundering.

At present, no meaningful financial statistics are readily available to gauge the level of cyber crime at a global level, although anecdotal evidence would suggest same to be in the billions of dollars annually.

FIREARMS TRAFFICKING
The trafficking in Illegal firearms is the movement of firearms from the legal to illegal marketplace through an illicit method for an unlawful purpose, usually to obtain profit, power, or prestige or to supply firearms to criminals or gangs.

Globally, smuggling has become the quintessential criminal activity of criminal organizations, and trafficking in firearms is, together with drugs and trafficking in persons, one of the most lucrative of such criminal activities. Available 2012 statistics estimates the market for illegal small firearms and light weapons at $1Billion annually.
A comprehensive global treaty (The Arms Trade Treaty), designed to curb the movement of illegal firearms and ammunition has been ratified by sixty-nine (69) states as of May 21st, 2015. Fifty (50) ratifications were required for the treaty to enter into force. The United Nations Office for Disarmament Affairs UNODA reported that 130 states have signed the treaty.

In The Bahamas, the excessive accumulation and uncontrolled infiltration of small arms and light weapons continues to present a significant challenge to law enforcement agencies and by extension to national security. The availability of illegal firearms has contributed to an escalation in serious crimes including murder, armed robbery, armed conflicts, gang violence, house breakings, and organized crime. Proceeds derived from trafficking in firearms is a predicate offence under the POCA, as amended with the attendant penalties.

CORRUPTION

There is no comprehensive and universally accepted definition of corruption. The origin of the word is from the Latin corruptus (spoiled) and corrumpere (to ruin; to break into pieces). The working definitions presently in vogue are variations of "the misuse of a public or private position for direct or indirect personal gain".

Many specific forms of corruption are clearly understood as such, and are the subject of numerous legal and academic definitions. Many are criminal offences, some of the more commonly encountered forms of corruption are listed below.

“GRAND” AND “PETTY” CORRUPTION

“Grand corruption” is an expression used to describe corruption that pervades the highest levels of government, engendering major abuses of power. A broad erosion of the rule of law, economic stability and confidence in good governance quickly follow. Sometimes it is referred to as “state capture”, which is where external interests illegally distort the highest levels of a political system to private ends.

“Petty corruption”, sometimes described as “administrative corruption”, involves the exchange of very small amounts of money, and the granting of small favours. These, however, can carry considerable public losses, as with a government official who waves through a consignment of high-duty goods having been bribed a mere $50 or so.

The essential difference between grand corruption (“state capture”) and petty corruption (day-to-day administrative corruption) is that the former involves the distortion of central functions of government by senior public officials; the latter develops within the context of functioning governance and social frameworks.

Corruption is said to be “systemic” where it has become ingrained in an administrative system. It is no longer characterised by actions of isolated rogue elements within a public service. Some acts of corruption are extortion, embezzlement, misappropriation, bribery, and fraud.
HUMAN SMUGGLING

People smuggling (also called people or human smuggling) is a form of transnational organized crime. It is the facilitation, transportation, attempted transportation, or illegal entry of a person or persons across an international border, in violation of one or more countries laws, either clandestinely or through deception, such as the use of fraudulent documents. The term is understood as and often used interchangeably with migrant smuggling, which is defined by the United Nations Convention Against Transnational Organized Crime also known as the ‘Palermo Convention’ of 2004. The Bahamas is a signatory to this Convention.

Human smuggling is a secretive, illicit activity, and one that is increasingly controlled by transnational organized crime syndicates, due to significant financial gains attached. The Bahamas is affected by people smuggling, be it in the capacity of country of origin, transit, or destination via periodic apprehension of persons of various nationalities inside and external to the region.

This activity, specifically migrant smuggling, constitutes ‘criminal conduct’ under the Proceeds of Crime Act, 2000, as amended and Section 47 of the Immigration Act. A significant contributing factor behind the success of smuggling operations comes from the participation of both local citizens and foreign nationals in this activity which keeps law enforcement on constant alert.

Human smuggling can generate substantial profits for those involved, which in turn can fuel corruption and organized crime in countries traveled from, through, or to during the smuggling process. Smugglers' fees vary from destination to destination, but on the whole, they have risen dramatically over the years. A 2009 estimate placed the human smuggling business at $20 Billion annually.

As, opportunities to migrate legally are severely limited, migrants, including asylum seekers, have increasingly resorted to illegal entry and unauthorized stays, and ever-larger numbers use the services of smugglers to evade the system, compounding their vulnerability to exploitation and in some cases certain death.

TRAFFICKING IN PERSONS

Trafficking in persons is a serious crime and a grave violation of human rights. The war against terrorism, narcotics, and irregular migration has moved this issue up the international policy agenda.

Article 3 (a) of the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons defines Trafficking in Persons as the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

Every year, thousands of men, women and children fall into the hands of traffickers, in their own countries and abroad. Almost every country in the world is affected by trafficking, whether as a country of origin, transit or destination for victims.

The list of offences under The Trafficking in Persons (Prevention and Suppression) Act, 2008 constitutes
'criminal conduct' under the Proceeds of Crime Act, 2000, as amended.

FRAUD

Fraud is a false representation of a matter of fact whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed that deceives and is intended to deceive another so that the individual will act upon it to her or his legal injury. Put otherwise, fraud is dishonesty calculated for advantage or profit. Because of the link between fraud and money laundering, it is important that such matters are reported to the FIU.

To establish fraud, it must be proved that the defendant's actions involved:

(a) a false statement of a material fact;
(b) knowledge on the part of the defendant that the statement is untrue;
(c) intent on the part of the defendant to deceive the alleged victim;
(d) justifiable reliance by the alleged victim on the statement; and
(e) injury to the alleged victim as a result.

In The Bahamas, where a person or entity is convicted of fraud by the Courts, judgment has generally taken the form of fines, prison sentences, an Order for Restitution to the victim(s) or a combination of same.

Fraud is often perceived to be a victimless crime. In reality it presents risks to individuals, businesses and institutions as well as the government. Aside from the direct financial loss, fraud places a severe emotional strain on individuals, their families and friends, and at a macro level, can damage The Bahamas’ international reputation as a safe place to do business and can impact public confidence in the services offered by the public, private and voluntary sectors.

It is not possible to identify the overall level of organised criminal activity locally against each fraud type or victim, as not all cases of fraud are reported. However, very few areas of everyday life have not been impacted by fraud, which can be broadly classified into four general categories, each of which has many subcategories:

(a) **Individual Fraud**: Any fraud that targets an individual directly, e.g. advance fee fraud, miracle health scams, ponzi schemes, pyramid schemes. Individual frauds can differ from frauds affecting businesses and other organizations;
(b) **Corporate Fraud**: Any fraud committed against a business e.g. cheque frauds, false accounting frauds, insurance frauds, pilferage, travel and subsistence fraud. Fraud impacting businesses can be both general frauds that target any business to sector specific frauds;
(c) **On-Line Fraud**: This fraud is perpetrated primarily via the internet, e.g. charity donation frauds, inheritance frauds, lottery scams and plastic card scams; and
(d) **Advance Fee Fraud**: The fraudster targets victim to make advance or up-front payment for goods, services and/or financial gains that do not materialize, e.g. career opportunity scams, psychic scams, impersonation of officials, West African Letters Scams.

The increasing globalisation of fraud continues with much of it driven by enhanced communications infrastructure, in particular the increased availability of high speed internet access and low levels of regulation and law enforcement capabilities in some countries.
SCAMS

Such schemes continue to surface with the ultimate objective being to try and separate unsuspecting individuals or businesses from their money or property. Methods employed in such endeavors would appear to be limited only by resourcefulness and creativity of the criminal elements and in some instances are multi jurisdictional in scope. Schemes which have surfaced locally include: e-mails, investments with guaranteed returns; front end fees; real estate sales/development; cheque fraud; counterfeit currency; pyramids; misappropriation of inventory; stealing by reason of employment/service; etc.

419 Letter

Are more commonly known as Nigerian scam letters. These scams are reminiscent of advance fee fraud in which victims are defrauded for monetary gain. There are various methods used in these scams. One common example of such a scam is that an individual will receive a letter stating that they have won some funds in another jurisdiction but in order for the funds to be released that individual is asked to remit funds to process the documents for the release of the funds. Before the explosion of technology these letters were commonly transmitted via traditional mail or faxed, however, in this age of technology the use of the internet has become the popular method of transmission. Although these scams are referred to as Nigerian scams one should not be disillusioned in thinking that they are isolated to that region.

Phishing

Phishing is defined as an attempt to acquire sensitive information such as passwords, usernames, account and credit card information often for the purpose of utilizing the information for malicious reasons. Phishing scams usually masquerade as trustworthy communication from a legitimate entity. Such communication originating from social websites, banks, auction sites, and online payment processors have been commonly used in these scams. Generally, phishing emails will contain a link to a website which will be infected with malicious malware. On the website the unsuspecting person will be directed to divulge sensitive information which will be used by the fraudster. It is with this information fraudsters have the ability to hack into other persons emails and accounts. The website that persons are normally directed to will appear legitimate on the face of it but in the background social engineering techniques are used to deceive unsuspecting persons.

It is advised that persons take caution with such emails and if at any time an email communication contains a link directing to an external site; it is safer to not respond to the email and refrain from clicking on the link. If there is any question as to the legitimacy of the email communication enhance due diligence should be applied to confirm the authenticity of the same. It is also a wise practice to never provide sensitive information to other individuals who have no verified legitimate reasons for needing the same.

PUBLIC NOTICE

The FIU has noticed that a trend has been developing relative to email and telephone scams that are consequently affecting many financial institutions within the jurisdiction. The Unit hereby advises all financial institutions and the general public that before any financial transaction is
conducted online, pursuant to instructions given via telephone, or otherwise, that they are aware of
the nature, manner and source of the proposed transaction. It is recommended that the true
identity of the sender or caller be verified. To this end the verification of the sender or caller’s true
identity can be achieved by using the verification policies and procedures currently in place by the
financial institution. As such we are advising financial institutions to review their respective policies
and procedures with a view of ensuring that stringent mechanisms are in place to prevent the
ability of fraudsters to successfully bypass the institution’s policies and procedure. Persons are
further advised that before acting on any proposed transaction it should be fully investigated and a
determination made by relevant qualified personnel within the financial institution, as to the
authenticity of the transaction request.
Appointment of Money Laundering Reporting Officer (MLRO)

The Financial Intelligence Unit of The Bahamas hereby advises that all entities that are defined as a “financial institution” pursuant to Section 3 of the Financial Transactions Reporting Act, Chapter 368 are required under Section 5(a) of the Financial Intelligence Unit (Transactions Reporting) Regulation, 2001 to identify and appoint a person the Money Laundering Reporting Officer, who shall be registered with the Financial Intelligence Unit.

An entity, defined as a financial institution and carrying on business as such, without complying with Section 5(a) and other provisions under the said regulation shall be guilty of an offence and liable on summary conviction or conviction on information to a fine not exceeding $100,000.00.

Obligation to Report Suspicious Transaction Report

Pursuant to Section 14, Financial Transactions Reporting Act, 2000 where a person conducts or seeks to conduct any transaction by, through or with a financial institution and the financial institution has knowledge, suspects or reasonable grounds to suspect that the transaction or propose transaction involves proceeds of crime as defined or listed as an offence under the Proceeds of Crime Act, 2000 has a strict duty to report such transaction or proposed transaction as soon as practicable after forming the suspicion, to the Financial Intelligence Unit.

Obligation to Provide Training

Section 6(1) of the Financial Intelligence (Transactions Reporting) Regulations, 2001 states as follows:

(i) A financial institution shall take appropriate measures from time to time for the purpose of making all relevant employees aware:

(a) Of the provisions of the Financial Intelligence Unit Act, 2000, the Financial Transactions Reporting Act, 2000, the Financial and Corporate Service Providers Act, 2000, the Proceeds of Crime Act, 2000, these regulations and any statutory provision relating to money laundering; and
(b) Of the procedures maintained by the institution in compliance with the duties imposed under these Regulations.

(2) A financial institution shall provide all relevant employees from time to time and in any case at least once per year with appropriate training in the recognition and handling of transactions carried out by or on behalf of any person who is, or appears to be, engaged in money laundering.

The Financial Intelligence (Transactions Reporting) Regulations, 2001 also requires financial institutions to establish and maintain

- Identification procedures
- Record-Keeping procedures and
- Internal reporting procedures in compliance with the said regulations.

Section 8 states:
(i) A financial institution carrying on business without complying with the requirements of these regulations, shall be guilty of an offence and shall be liable:

(a) On summary conviction to a fine of $10,000.00
(b) On conviction on information:--
   i) For a first offence, to a fine of $50,000.00
   ii) For a second or subsequent offence to a fine of $100,000.00.
7. **TRAINING**

The Financial Intelligence Unit’s staff continued to take steps to ensure that training modules are available for each profession, addressing the issues of AML/CFT inherent in their various areas of activity.

Listed below are the training/presentations of the FIU for the financial sector during the year 2016.

<table>
<thead>
<tr>
<th>Dates</th>
<th>Organization/Entity</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 23 February, 2016</td>
<td>Arner Bank &amp; Trust</td>
<td>5</td>
</tr>
<tr>
<td>2. 7 - 8 March, 2016</td>
<td>Resort World Bimini</td>
<td>57</td>
</tr>
<tr>
<td>3. 14 March, 2016</td>
<td>SIS Solutions Limited</td>
<td>4</td>
</tr>
<tr>
<td>4. 3 March, 2016</td>
<td>Securities Commission FCSP Briefing</td>
<td></td>
</tr>
<tr>
<td>5. 18 March, 2016</td>
<td>Insurance Management - Abaco</td>
<td>6</td>
</tr>
<tr>
<td>6. 13 April, 2016</td>
<td>AIBT Regulators Forum</td>
<td></td>
</tr>
<tr>
<td>7. 10 March, 2016</td>
<td>FirstCaribbean Bank International</td>
<td>34</td>
</tr>
<tr>
<td>8. 6 April, 2016</td>
<td>Binnmicle Advisors Limited Claymore Corporate Services &amp; The Heritage Trust Company Limited</td>
<td>8</td>
</tr>
<tr>
<td>9. 27 April, 2016</td>
<td>Biscayne Capital</td>
<td>11</td>
</tr>
<tr>
<td>10. 15 April, 2016</td>
<td>C. Yvette McCartney-Meredith</td>
<td>5</td>
</tr>
<tr>
<td>11. 31 May, 2016</td>
<td>Pacifico Global Advisors Limited</td>
<td>5</td>
</tr>
<tr>
<td>12. 25 April, 2016</td>
<td>Argus Advisors</td>
<td>3</td>
</tr>
<tr>
<td>13. 12 May, 2016</td>
<td>Callenders</td>
<td>32</td>
</tr>
<tr>
<td>14. 19 - 22 April, 2016</td>
<td>Commonwealth Bank</td>
<td>91</td>
</tr>
<tr>
<td>15. 18 - 20 May, 2016</td>
<td>J.S. Johnson &amp; Company Limited</td>
<td>82</td>
</tr>
<tr>
<td>16. 17 May, 2016</td>
<td>Higgs &amp; Johnson</td>
<td>55</td>
</tr>
<tr>
<td>17. 23 June, 2016</td>
<td>Providence Advisors</td>
<td>17</td>
</tr>
<tr>
<td>18. 21 June, 2016</td>
<td>Commonwealth Bank Fraud Workshop</td>
<td>14</td>
</tr>
<tr>
<td>19. 23 August, 2016</td>
<td>Summit Insurance &amp; IBM</td>
<td>23</td>
</tr>
<tr>
<td>20. 24 August, 2016</td>
<td>Juliur Baer Bank &amp; Trust</td>
<td>19</td>
</tr>
<tr>
<td>21.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Company Name</td>
<td>Count</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>16 September, 2016</td>
<td>Caystone Solutions</td>
<td>20</td>
</tr>
<tr>
<td>22. 23 September, 2016</td>
<td>Genesis Fund Services Limited</td>
<td>15</td>
</tr>
<tr>
<td>23. 23 September, 2016</td>
<td>BACO Grand Bahama</td>
<td></td>
</tr>
<tr>
<td>24. 14 October, 2016</td>
<td>International Protector Group (IPG)</td>
<td>10</td>
</tr>
<tr>
<td>25. 13 October, 2016</td>
<td>CIBC Trust Company (Bahamas) Limited</td>
<td>32</td>
</tr>
<tr>
<td>26. 19 October, 2016</td>
<td>Leno Corporate Services Limited</td>
<td>11</td>
</tr>
<tr>
<td>27. 24 - 25 October, 2016</td>
<td>Winterbotham Trust Company</td>
<td>47</td>
</tr>
<tr>
<td>28. 15 November, 2016</td>
<td>Societe Generale</td>
<td>36</td>
</tr>
<tr>
<td>29. 15 November, 2016</td>
<td>BACO Annual MLRO Day</td>
<td></td>
</tr>
<tr>
<td>30. 16 November, 2016</td>
<td>Pictet Bank &amp; Trust</td>
<td>64</td>
</tr>
<tr>
<td>31. 18 November, 2016</td>
<td>Hailsham Legal Services (Eleuthera)</td>
<td>2</td>
</tr>
<tr>
<td>32. 22 - 24 November, 2016</td>
<td>Colina Insurance Limited</td>
<td>235</td>
</tr>
<tr>
<td>33. 25 November, 2016</td>
<td>Equity Trust Bahamas Limited</td>
<td>17</td>
</tr>
<tr>
<td>34. 30 November, 2016</td>
<td>State Bank of India</td>
<td>7</td>
</tr>
<tr>
<td>35. 5 December, 2016</td>
<td>FC Capital Investments Limited</td>
<td>3</td>
</tr>
<tr>
<td>36. 6 December, 2016</td>
<td>Credit Suisse AG</td>
<td>97</td>
</tr>
<tr>
<td>37. 7 December, 2016</td>
<td>Resort World Bimini, Miami Office</td>
<td>20</td>
</tr>
<tr>
<td>38. 12 December, 2016</td>
<td>Andbank</td>
<td>15</td>
</tr>
<tr>
<td>39. 13 December, 2016</td>
<td>Grand Bahama Power Company Ltd.</td>
<td>21</td>
</tr>
<tr>
<td>40. 15 December, 2016</td>
<td>Harry B. Sands, Lobosky &amp; Company</td>
<td>20</td>
</tr>
<tr>
<td>41. 16 December, 2016</td>
<td>SYZ Trust</td>
<td>8</td>
</tr>
</tbody>
</table>

Total number of persons trained: 1151
8. **ANNUAL TRAINING COMPARISON 2012 – 2016**

**WHAT DOES THIS GRAPH REPRESENT?**

The graph shows a comparison of the number of individual trained each year for the years 2012 through 2016.

**WHAT DOES THE GRAPH INDICATE?**

The number of persons trained increased dramatically from 2012 to 2016 and over the last year there was a percentile increase of 20.90%.
### OVERSEAS TRAINING, SEMINARS, CONFERENCES AND MEETINGS ATTENDED BY STAFF MEMBERS OF FIU

<table>
<thead>
<tr>
<th>DATE</th>
<th>INSTITUTION</th>
<th>NATURE AND LOCATION</th>
<th>NUMBER OF PARTICIPANTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 6- 9, 2016</td>
<td>Anti-Money Laundering &amp; ST Training</td>
<td>Bimini, Bahamas</td>
<td>Two</td>
</tr>
<tr>
<td>Mar 17, 2016</td>
<td>Anti-Money Laundering &amp; ST Training</td>
<td>Marsh Harbour, Abaco</td>
<td>One</td>
</tr>
<tr>
<td>May 26 - 27, 2016</td>
<td>XLII Meeting of the Group of Experts for the Control of Money Laundering</td>
<td>Washington, D.C.</td>
<td>One</td>
</tr>
<tr>
<td>June 6 - 9, 2016</td>
<td>CFATF XLII Plenary Meeting</td>
<td>Montego Bay, Jamaica</td>
<td>Three</td>
</tr>
<tr>
<td>June 27 - 29, 2016</td>
<td>FINTRAC STR Workshop</td>
<td>Miami, Florida</td>
<td>One</td>
</tr>
<tr>
<td>July 11 - 12, 2016</td>
<td>AML/CFT Anti-fraud &amp; Financial Crimes</td>
<td>St. Johns, Antigua</td>
<td>Two</td>
</tr>
<tr>
<td>Sept 26 - 28, 2016</td>
<td>15th Annual ACAMS Conference</td>
<td>Las Vegas, Nevada</td>
<td>Two</td>
</tr>
<tr>
<td>Sept 23, 2016</td>
<td>Baco’s Northern Bahamas Conference</td>
<td>Nassau, Bahamas</td>
<td>One</td>
</tr>
<tr>
<td>Nov 6 - 8, 2016</td>
<td>AICPA National Forensic Accounting Conference</td>
<td>Nashville, Tennessee</td>
<td>One</td>
</tr>
<tr>
<td>Nov 7 - 11, 2016</td>
<td>CFATF XLIV Plenary Meeting</td>
<td>Turks &amp; Caicos Islands</td>
<td>Three</td>
</tr>
<tr>
<td>Nov 14 - 16, 2016</td>
<td>4th Annual Caribbean &amp; Americas Gaming Regulations Forum</td>
<td>Miami Beach, Florida</td>
<td>One</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
<td>Location</td>
<td>Quantity</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------</td>
<td>-----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Dec 6 - 8, 2016</td>
<td>Anti-Money Laundering &amp; Suspicious Transaction Training</td>
<td>Miami Office</td>
<td>One</td>
</tr>
<tr>
<td>Dec 13, 2016</td>
<td>Anti-Money Laundering &amp; Suspicious Transaction Training</td>
<td>Freeport, Grand Bahama</td>
<td>One</td>
</tr>
</tbody>
</table>
10. **ANNUAL STATISTICS OF THE FINANCIAL INTELLIGENCE UNIT**

10.1 **REPORTING PERIOD**

The reporting period has been defined as being the period 1st January to 31st December 2016.

10.2 **GENERAL FINDINGS**

A total of three hundred and six (306) Suspicious Transaction Reports were received by the FIU during the year under review. [The status of the reports includes the FIU’s processing of the reports up to 31st January 2017.]

- Thirty Seven (37) of the reports were forwarded to the Commissioner of Police for investigation.
- Fifty Five (55) of the reports were analyzed and closed by the FIU.
- Two hundred and fourteen (214) of the reports are pending.

There was an increase of approximately 3.08% in Suspicious Transaction Reports received. By comparison, a total of two hundred and ninety seven (297) Suspicious Transaction Reports were made to the Financial Intelligence Unit for the period 1st January to 31st December 2015.

For the period under review, approximately 12.09% of the Suspicious Transaction Reports were forwarded to the Commissioner of Police for investigation.
10.3 DETAILED STATISTICS

10.3.1 OVERVIEW OF 2016

SUMMARY CALENDAR YEAR (1st January – 31st December 2016)

<table>
<thead>
<tr>
<th>NUMBER OF REPORTS</th>
<th>Absolute</th>
<th>Relative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Received</td>
<td>306</td>
<td>100.00%</td>
</tr>
<tr>
<td>Passed onto the Police</td>
<td>37</td>
<td>12.09%</td>
</tr>
<tr>
<td>Closed</td>
<td>55</td>
<td>17.97%</td>
</tr>
<tr>
<td>Pending</td>
<td>214</td>
<td>69.93%</td>
</tr>
</tbody>
</table>

TYPE OF INSTITUTION

- Casino: 44 (14.37%)
- Company Service Provider: 3 (.98%)
- Credit Union: 2 (.65%)
- Domestic Banks: 9 (2.94%)
- Domestic/Offshore Banks: 121 (39.54%)
- Offshore Banks: 67 (21.99%)
- Financial Advisor: 4 (1.30%)
- Insurance Company: 2 (.65%)
- Lawyer: 2 (.65%)
- Money Remittance Service: 7 (2.28%)
- Other: 1 (.32%)
- Stockbroker: 13 (4.24%)
- Trust Company: 31 (10.13%)

REPORTED VALUES IN BSD

<table>
<thead>
<tr>
<th>(Total Effective Assets At Time Of Report)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Total</td>
<td>$214,364,104.00</td>
</tr>
<tr>
<td>Total reports passed onto the Police</td>
<td>38,276,344.00</td>
</tr>
<tr>
<td>Total reports closed</td>
<td>2,306,884.00</td>
</tr>
<tr>
<td>Total reports pending</td>
<td>173,780,876.00</td>
</tr>
<tr>
<td>Average value of report (total)</td>
<td>$700,536.28</td>
</tr>
<tr>
<td>Average value of reports passed onto Police</td>
<td>1,034,495.78</td>
</tr>
<tr>
<td>Average value of reports closed</td>
<td>41,946.34</td>
</tr>
<tr>
<td>Average value of reports pending</td>
<td>812,060.18</td>
</tr>
</tbody>
</table>
10.3.2 MONTHLY STATISTICS OF INCOMING REPORTS

The graph shows the monthly totals of Suspicious Transaction Reports for the year 2016.

There was a total of three hundred and six (306) Suspicious Transaction Reports received during 2016. The number of reports fluctuated from month-to-month throughout the entire year averaging approximately twenty five (25) reports per month. The majority of the reports were received during March, September and December.
10.3.3 COMPARATIVE SUSPICIOUS TRANSACTIONS REPORTING

The graph shows a comparison of the monthly totals of Suspicious Transaction Reports for the years 2014 through 2016.

The number of reports fluctuated from month-to-month throughout the years 2014-2016.
10.3.4 DISCLOSING INSTITUTIONS

The graph gives a breakdown of the Suspicious Transaction Reports filed by financial institutions.

The Banks submitted the greatest number of the reports (64.70%), and the remainder was received from other financial institutions.
10.3.5 GROUNDS FOR SUSPICIOUS TRANSACTION REPORTS

The graph shows the reasons that prompted the financial institution to file Suspicious Transaction Reports.

As in previous years, during the year 2016, the industry saw the continued application of enhanced due diligence policies. The Financial Intelligence Unit’s Anti-Money Laundering and Suspicious Transaction Guidelines provided financial institutions with a wide category of grounds for disclosure of Suspicious Transaction Reports.
10.3.6 TYPE OF CURRENCY

The graph provides a breakdown of the various currencies, which were utilized in facilities, by the subject of the Suspicious Transaction Reports.

The BSD and USD were utilized in 38.67 % and 53.31 % respectively, of the facilities subject of the reports and the remainder was a mixture of several other currencies.
10.3.7 NATURE OF OFFENCES – DISCLOSING INSTITUTIONS’ SUSPICION

The graph shows the offences suspected by the financial institution of having been committed at the time the reports were submitted to the Financial Intelligence Unit.

In approximately 46.07% of cases, the financial institution at the time it submitted the Suspicious Transaction Report, did not know the nature of the offence. Thus, other suspicious circumstances led to the filing of the reports. Fraud and Other illicit matters* were suspected in 19.60% and 13.72% respectively of the reports received.

It should be noted that the suspicions of a financial institution at the time of submission of the reports to the Financial Intelligence Unit, might differ from those of the Financial Intelligence Unit during analysis of the said reports.
10.3.8 NATURE OF OFFENCES – FINANCIAL INTELLIGENCE UNIT’S SUSPICION

The graph shows the offences suspected by the Financial Intelligence Unit of having been committed upon completion of analysis of the reports, or upon receipt of other financial or criminal intelligence.

The Financial Intelligence Unit did not detect any criminal activity in 15.03% of the Suspicious Transactions Reports received. Fraud and Other illicit matters were detected in 6.20% and 1.96% respectively of the reports received.
10.3.9 **NATIONALITY OF CONTRACT PARTNERS**

The graph shows the nationality of contract partners who were the subjects of the Suspicious Transaction Reports.

Bahamians represented 33.00% of the contract partners, 31.04% were citizens from Brazil, China, Grenada, Unknown and the USA, whereas the others were from various countries around the world.
10.3.10 DOMICILE OF CONTRACT PARTNERS

The graph shows the domicile of contract partners who were the subjects of the Suspicious Transaction Reports.

Residents of The Bahamas represented 45.75% of the contract partners, 27.45% were residents of Brazil, Italy, Mexico, Unknown and the USA, whereas the others were from various countries around the world.
10.3.11 NATIONALITY OF BENEFICIAL OWNERS

The graph shows the nationality of beneficial owners who were the subjects of the Suspicious Transaction Reports.

Bahamians represented 33.00% of the beneficial owners, 31.64% were citizens of Brazil, China, Grenada, Unknown and the USA, whereas the others were from various countries around the world.
10.3.12 DOMICILE OF BENEFICIAL OWNERS

The graph shows the domicile of beneficial owners who were the subjects of the Suspicious Transaction Reports.

Residents of The Bahamas represented 45.75% of the beneficial owners, 27.45% were residents of Brazil, Italy, Mexico, Unknown and the USA, whereas the others were from various countries around the world.
10.3.13 SUSPICIOUS TRANSACTION REPORTS - TRENDS

The graph shows the status of the customers of the financial institutions who were the subjects of the Suspicious Transaction Reports.

Long-standing customers of the disclosing institutions accounted for 64.05% of the reports received, whereas new customers accounted for 21.89% of the reports.
10.3.14 INVESTIGATIVE BODIES INVOLVED

The Royal Bahamas Police Force is the primary agency in The Commonwealth of The Bahamas charged with the responsibility of investigating criminal offences under the Proceeds of Crime Act, Chapter 93 and the Anti Terrorism Act, 2004.

Two specialist bodies exist within the agency, mandated to investigate financial crimes: the Business and Technology Crime Unit, Formerly the Commercial Crime Section of the Central Detective Unit, and the Tracing and Forfeiture/Money Laundering Investigation Section of the Drug Enforcement Unit.

A total of thirty-seven (37) Suspicious Transaction Reports were forwarded by the Financial Intelligence Unit to the Police for investigation.

Section 55 of the Proceeds of Crime Act also gives Customs Officers powers of investigation in certain cases. Sub-Section (1), (2), (3) of section 55 reads;

(1) For the purposes of section 46, “police officer” includes any officer of the Customs Department at any port of entry or departure in The Bahamas.
(2) A police officer may arrest without warrant any person whom he reasonably believes has committed an offence under this act.
(3) An officer of Customs Department may, in any case relating to the commission of an offence under this act, exercise all or any of the powers in relation to investigations into an offence which is arrestable without warrant conferred on a police officer by the Criminal Procedure Code Act.
10.3.15 NUMBER OF REQUESTS FOR INFORMATION RECEIVED FROM FOREIGN FINANCIAL INTELLIGENCE UNITS

The graph shows the countries from which the FIU received requests.

There were ninety three (93) requests.

The Financial Intelligence Unit of the USA, (FinCEN), SOCA of the United Kingdom (MROS) of Switzerland, (UIF) of Argentina and (TRACFIN) of France submitted 40.86% of requests.
10.3.16 STATUS OF REQUESTS FOR INFORMATION RECEIVED FROM FOREIGN FINANCIAL INTELLIGENCE UNITS

The graph gives a breakdown of the status of the requests received.

The Financial Intelligence Unit provided assistance in 79.56% of the requests, which were received and 20.43% of the requests are being processed.
10.3.17 REQUESTS FOR INFORMATION SENT TO FOREIGN FINANCIAL INTELLIGENCE UNITS

The graph shows the countries to which the FIU submitted requests.

There were forty eight (48) requests.

(FinCEN), the FIU of the USA, (UIF), the FIU of Argentina, (FIBA), the FIU of Brazil, and (MROS), the FIU of Switzerland were the recipient of the majority of the requests.
10.3.18 STATUS OF REQUESTS FOR INFORMATION SENT TO FOREIGN FINANCIAL INTELLIGENCE UNITS

The graph gives a breakdown of the status of the requests submitted.

The Financial Intelligence Unit received assistance in 72.91% of the requests, which were submitted, and Thirteen (13) requests or 27.09% are being processed.
10.3.19 STATUS OF REQUESTS FOR THE PRODUCTION OF INFORMATION

The graph shows that a total of seven hundred and seventy five (775) requests were made to financial institutions and law enforcement agencies in The Bahamas.

Responses, which provide relevant information, were received in respect to 76.51% of the requests, while one hundred and eighty two (182) requests or 23.48% are being processed.
9.3.20 OTHER STATISTICS

During the year under review, a total of thirty eight (38) Requests for Assistance were received from the Royal Bahamas Police Force. Assistance was granted in twenty nine (29) or 76.31% of the Requests and nine (9) Requests or 23.68 % are awaiting the provision of additional information, which was requested of the Police.
10. **INTERNATIONAL**

10.1 **EGMONT GROUP**

Recognising the benefits inherent in the development of a FIU network, in 1995, a group of FIUs met at the Egmont Arenberg Palace in Brussels and decided to establish an informal group for the stimulation of international co-operation. Now known as the Egmont Group of Financial Intelligence Units, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and terrorist financing and to foster the implementation of domestic programs in this field. This support includes:

- expanding and systematizing international cooperation in the reciprocal exchange of information;
- increasing the effectiveness of FIUs by offering training and promoting personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs;
- fostering better and secure communication among FIUs through the application of technology, such as the Egmont Secure Web (ESW);
- fostering increased coordination and support among the operational divisions of member FIUs;
- promoting the operational autonomy of FIUs; and
- promoting the establishment of FIUs in conjunction with jurisdictions with an AML/CFT program in place, or in areas with a program in the early stages of development.

The Financial Intelligence Unit of The Bahamas is an active participant in the Egmont “Outreach” Working Group. The FIU continues to co-monitor and co-sponsor with the FIU of BVI (FIA), the FIUs of Montserrat, with the FIU of the USA (FinCEN), the FIU of Dominican Republic, and with the FIU of BVI (FIA) the FIU of Haiti for membership in the Egmont Group.

On July 3rd, 2013 at the 21st Egmont Group Plenary in Sun City South Africa, Trinidad and Tobago, which was sponsored by BVI and The Bahamas, was accepted along with seven other FIUs as new Egmont members. In June 2014 at the 22nd Egmont Group Plenary held in Peru, Jamaica, another jurisdiction co-sponsored by The Bahamas became an Egmont member. As of June 2015 Egmont Group membership stood at 151 FIUs globally.
10.2.  MEMORANDUM OF UNDERSTANDING

In June 2015, FIU Bahamas signed a Memorandum of Understanding (MOU) with Jamaica. The signing of this agreement allows the signatories to better cooperate and share intelligence necessary to combat the increase in criminal conduct in their respective jurisdictions. A number of MOUs which are expected to greatly assist in the cooperation and collaboration with foreign FIUs in AML/CFT matters are presently being processed by the FIU.

10.3.  CARIBBEAN FINANCIAL ACTION TASK FORCE (CFATF)

The CFATF is comprised of twenty-seven (27) member countries whose goal is to develop and promote strategies in the fight against Money Laundering and the Financing of Terrorism at national, regional, and international levels.

The Bahamas is an active member of CFATF and presently serve on the organization’s Risk Trends and Methods Group, formerly the Typologies Working Group. The Caribbean Financial Action Task Force is presently conducting studies on important regional and transnational issues, inclusive of:

(i) The trafficking of small arms and ammunition and
(ii) Lotteries and ponzi schemes.
1. Yellow Bird Bank made a suspicious transaction report to the Financial Intelligence Unit in regards to their client a Mr. John White. Yellow Bird Bank, during its due diligence came across a media source which indicated that Mr. White was arrested by the police in a European country, for organized fraud, money laundering and criminal association. Due to the bank’s findings a decision was made to report the matter to the Financial Intelligence Unit. The Financial Intelligence Unit during its analysis of the matter made a request to the European country’s FIU in regards to the matter. The European country FIU answered the request and confirmed that Mr. White confessed to his involvement in a criminal organization dedicated to various fraudulent activities amounting to over € 500,000,000.00 being defrauded using foreign banks accounts and companies to launder fraud proceeds. The European FIU also requested information on Mr. White’s accounts in the Bahamas and requested that the funds on the account be frozen. The Financial Intelligence Unit after receipt of the request, quickly reported the matter to the Royal Bahamas Police Force and placed a 72 hours freeze order under (Section 4(2)(b) of the Financial Intelligence Unit Act, Chapter 367) on the accounts. An additional 5 days freeze order under (Section 4(2)(c) of the Financial Intelligence Unit Act, Chapter 367) was also placed on the account by request of the Royal Bahamas Police Force.

Indicators:
- Media report
- Ongoing criminal investigation by a foreign country.

2. Financial Intelligence Unit received a suspicious transaction report from Blue Jeans Securities Limited about a client (Mrs. Jane Brown), who through her online trading account proceeded to trade in the securities markets using her credit card. Blue Jeans Securities Limited stated that Mrs. Jane Brown through her trades had lost up to $15,000.00 almost the whole balance of her account. After realizing her lost Mrs Brown reported the same to her credit card company and had them reverse all payments in regards to her trade through Blue Jeans Securities Limited. The reversal was completed and Blue Jeans Securities Limited was now forced to put her account in the negative for $15,000.00. Due to this fact Blue Jeans Securities Limited believed that Mrs. Brown intentionally and dishonestly had her credit card deductions reversed to regain the loses that she sustained. Blue Jeans Securities Limited was force to absorbed the loss of her trades.

Indicators:
- Credit Card reversals after trading losses

3. More Money Bank Limited made a suspicious transaction report to the Financial Intelligence Unit stating that one of their client (Mr. Broke) saving account was hacked. On 23rd April 2016 an internal report was filed on some unauthorized transfers from Mr. Broke’s account. According to the internal report the client stated that he received an e-mail from the bank and click on a link embedded in it. Days later numerous transfers from Mr. Broke’s account occurred and were transferred to numerous third party clients of the bank. The bank could not discover any connections or the reasons for the transfers to the other third-party clients. The bank through its internal investigation discovered that when the funds were place on the third-party accounts they

Financial Intelligence Unit
Commonwealth of The Bahamas
were immediately withdrawn by ATM and in-branch withdrawals. Attempts were made to contact other third-parties to alert them of the fraud and to recover the stolen money to no avail. The bank refunded Mr. Broke’s account and made a report to the financial intelligence unit. The Financial Intelligence Unit analyzed the report and sent the matter on to the police force for investigation due to the apparent fraudulent activity.

Indicators:
- Unauthorized account transfers
- No connection of the third parties to the victim
- Immediate withdrawals of ill-gotten funds
- The inability to contact third-parties.
- The appearance of organized fraud

Egmont Cases

4. One morning, the inhabitants of a small town in Europe were woken by the noise of a violent robbery of their local bank. The operation was successful and the robbers escaped with a sizeable amount of cash.

A special law-enforcement squad was set up to investigate the robbery. After intensive investigations, the squad succeeded in arresting the ringleaders of the attack. Some of the arrested criminals even confessed where they had hidden their shares of the haul. Marco, a law-enforcement professional for more than 20 years and a member of the squad, was one of the agents who were given the responsibility for locating, freezing and returning the stolen money.

Due to the strong intelligence gained from interrogations, some of the money was quickly located, but after a while the process slowed down. Some members of the squad-team noticed irregularities in the investigation. There seemed to be a mismatch between the suspects’ confessions about the quantity and whereabouts of the funds and the effective amounts seized. Mounting concern lead to a request for an internal investigation to determine whether there had been any untoward activity.

Internal affairs initiated an investigation. They soon suspected that one of the agents might have embezzled part of the haul for personal benefit. Marco became the focus of their attention. Internal affairs searched Marco’s home and workplace. Some evidence of paperwork advertising financial institutions offering investment accounts in other countries was found, but there was no indication that Marco actually had any accounts there.

The magistrate in charge of the investigation immediately sent a mutual legal assistance request to the country in which the financial institutions named in the paperwork were based. He demanded that the banks associated with investment fund business — freeze any assets relating to Marco. Unfortunately, the courts in the neighboring country had to turn down his request because there was no indication as to which financial institution had a business relationship with Marco. ‘Fishing’ expeditions based on minimal evidence are not permissible in a number of countries.
A few months later, the neighboring country’s national FIU received a transaction report on Marco. While investigating the transaction, the FIU came across the mutual legal assistance request. Through the Egmont network, the FIU immediately contacted the national FIU in the originating country and learnt that Marco, who performed the disclosed transaction, was the same Marco who was suspected of embezzling the money. The account statements furthermore confirmed that Marco had placed assets into his accounts at the same time he was suspected of having done so.

The FIU passed on the disclosure to the magistrate who had first had to turn down the mutual legal assistance request. He was now able to grant the request and at the time of reporting, the funds were frozen pending prosecution and recovery action.

Indicators:
- Possible client relationship to previous crimes

5. The national FIU in a Northern European country received two suspicious transaction reports, which triggered a financial investigation:

Dennis, Muriel and Patrick worked for a drugs trafficking organisation, although they had no criminal records and had not been identified by the police as being in any way involved in drugs trafficking activities. Other members of the trafficking organisation transferred large amounts of money into accounts that the three had opened in a bank in the Northern European country. Shortly after the transfers, the money was withdrawn in cash. At this stage the bank became concerned and decided to disclose to the national FIU. Daniel, Muriel, and Patrick transported the money in cash form to other European jurisdictions where it was still possible to obtain anonymous numbered accounts. Once within the jurisdictions, they opened more than 40 different accounts between them to make the fund movements as complex as possible for any investigation by the authorities in that country. The cash that they had smuggled into the country was split up into the various accounts. The three individuals used the receipts from the banks where they had withdrawn the money to ‘prove’ the legal origin of the funds - and because they spread the anonymous accounts across a range of banks they were able to use the same documentation in support of multiple account openings. Once the accounts had been successfully opened, the three returned to their initial country with the account documentation.

However, following an investigation by FIU and police, the three were arrested upon their return and convicted to a total of ten years imprisonment for drug trafficking offences and drug money laundering. Approximately US$6,000,000 was confiscated in total.

Indicators:
- Multiple transfers into a personal account
- Large scale cash transactions
- Unrealistic wealth compared to client profile
## GLOSSARY OF TERMS

<table>
<thead>
<tr>
<th>Terms</th>
<th>Meanings of Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beneficial Owners</td>
<td>Individuals who were disclosed as being the ones benefiting from the proceeds of the facility</td>
</tr>
<tr>
<td>Closed</td>
<td>Analysis completed by FIU and report not forwarded to the Royal Bahamas Police Force for investigation</td>
</tr>
<tr>
<td>Contract Partners</td>
<td>Corporate entities and/or individuals in whose name the facility was established with the financial institution</td>
</tr>
<tr>
<td>Domestic</td>
<td>Banks conducting domestic banking only</td>
</tr>
<tr>
<td>Offshore</td>
<td>Banks conducting offshore banking only</td>
</tr>
<tr>
<td>Domestic/Offshore</td>
<td>Banks conducting a combination of domestic and offshore banking</td>
</tr>
<tr>
<td>D.I.</td>
<td>Disclosing institution</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>Pending</td>
<td>Open with ongoing analysis by the FIU</td>
</tr>
<tr>
<td>Police</td>
<td>Royal Bahamas Police Force</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>Terrorist financing</td>
<td>Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>CFATF</td>
<td>Caribbean Financial Action Task Force</td>
</tr>
<tr>
<td>DNFBPs</td>
<td>Designated Non Financial Businesses and Professions</td>
</tr>
</tbody>
</table>