

**AML/CFT GUIDANCE FOR THE GAMBLING SECTOR**

## PURPOSE AND CONTENTS

The Financial Intelligence Unit of Trinidad and Tobago (“the FIU”) provides this sector specific guidance to entities collectively referred to as ‘the gambling sector’ on their legal obligations under the Anti- Money Laundering/Counter Financing of Terrorism (AML/CFT) laws of Trinidad and Tobago. The entities collectively referred to as ‘the gambling sector’ for the purpose of this guidance include Gaming Houses, a business conducting betting transactions, on-line gambling and betting, pool betting business, the National Lotteries Control Board (“the NLCB”) and Private Members Clubs.

Accordingly, this guidance applies to you if the activities you or your business performs fall within one or more of the following categories:

1. **a business registered under the Gambling and Betting Act Chap. 11:19 (“Pool Betting business”);**
2. **the business of lotteries operated in accordance with the National Lotteries Act Chap.21:04 (“the NLCB”);**  
**NLCB”);**
3. **a private members club within the meaning of the Registration of Clubs Act Chap. 21:01.**  
**If you are registered as a members’ club and have been permitted by the relevant Licensing Committee to carry on gambling as an activity of the club on its premises these obligations apply to you.**

This guidance uses plain language to explain the most common situations under the specific laws and related regulations which impose AML/CFT obligations. It is provided as general information only. It is not legal advice and does not replace the AML/CFT Acts and Regulations. AML/CFT obligations are contained in several laws, amendments and regulations, therefore, it would be easier for the gambling sector to access the relevant provisions pertaining to their obligations in one place.

## Supervised Entity &gt; GAMBLING SECTOR

The word “**must**” indicates a mandatory requirement, “**should**” indicates a best practice and “**may**” states an option for you to consider.

This guidance, which is divided into ten (10) parts, includes:

1.	Do these obligations apply to you? - Clarification on the specified business activities which apply to the Gambling Sector.
2.	What is a Listed Business?
3.	The role and function of the FIU in the AML/CFT regime.
4.	What is Money Laundering?
5.	What is Financing of Terrorism?
6.	Why are entities in the Gambling Sector designated as a Listed Business?
7.	Examples of Money Laundering using the Gambling Sector.
8.	What are your AML/CFT legal Obligations? - An explanation of the main AML/CFT legal obligations, how they should be applied and Best Practices.
9.	Offences & Penalties.
10	Additional Resources.
Appendix – Suspicious Transactions/Activities Indicators	

**PART I****DO THESE OBLIGATIONS APPLY TO YOU?****Clarification on the specified business activities which apply to the Gambling Sector**

These obligations apply to all types of Listed Business in the gambling sector that satisfy the criteria below.

If you are an employee of a Listed Business, these obligations are the responsibility of your employer..

**Pool Betting**

Pool betting is a Listed Business described in the First Schedule to the Proceeds of Crime Act Chap. 11:27 ("the POCA") as *'any such business registered under the Gambling and Betting Act'*.

**Therefore, if you are the holder of a permit or betting office licence issued under the Gambling and Betting Act, the AML/CFT obligations detailed herein apply to you.**

**It is an offence to carry on betting transactions without the grant of a permit or betting office licence.**

**Therefore, if you carry out betting transactions, you must first apply for and obtain a permit or a betting office licence in accordance with the Gambling and Betting Act and then you MUST REGISTER with the FIU in accordance with the Financial Intelligence Unit Act of Trinidad and Tobago Chap. 72:01 ("the FIU Act"). Failure to do so may render you liable to fines and imprisonment under both the FIU Act and the Gambling and Betting Act.**

**National Lotteries On-Line Betting Games**

National Lotteries On-Line Betting Games is a Listed Business described in the First Schedule to the POCA as *'the business of lotteries operated in accordance with the National Lotteries Act'*.

The National Lotteries Control Board ("the NLCB") is a body corporate established by virtue of **Section 3 (1)** of the National Lotteries Act. The NLCB is charged with carrying on the business of promoting, organising and conducting national lotteries and for such purpose it may have and exercise such functions, powers and duties as are conferred or imposed on it by the National Lotteries Act. **As such, the NLCB, which conducts the business of lotteries operated in accordance with the National Lotteries Act, must comply with the AML/CFT obligations detailed herein.**

**Private Members' Club**

A Private Members' Club is a Listed Business described in the First Schedule to the POCA as 'a member's club which is granted a certificate under section 5(4) of the Registration of Clubs Act.'

"Members' club" under the RCA means a club not constituted for the acquisition of gain (or, in other words, not formed for the basis of acquisitions of say property or other assets), the members of which contribute to the funds out of which the expenses of conducting the club are paid and are jointly entitled to all the property and funds of the club.

A member's club granted a certificate under section 5 (4) of the Registration of Clubs Act is one which carries on gambling activities under the Gambling and Betting Act.

**Therefore, if you operate a Members' Club and are duly registered in accordance with the RCA under section 5 (4), and have been permitted by the relevant Licensing Committee to carry on gambling as an activity of the club on its premises then these AML/CTF obligations detailed as follows apply to you..**

**A members' club registered under the RCA and persons licensed under the Gambling and Betting Act shall comply with the requirements of the Financial Obligations Regulations where a customer engages in-**

- (a) a transaction of eighteen thousand dollars and over; or**
- (b) two or more transactions each of which is less than eighteen thousand dollars but together total eighteen thousand dollars or more and it appears, whether at the outset of each transaction or subsequently that the said transactions are linked.**

## PART 2

### WHAT IS A LISTED BUSINESS?

A Listed Business is any business activity or profession listed in the First Schedule of POCA. Entities operating within the gambling sector are specifically included and are subject to the POCA as well as the Anti-Terrorism Act (“the ATA”). These types of businesses face a greater risk of coming across crime proceeds and terrorist property. Business activities which have been identified as more vulnerable in the gambling sector are identified as those businesses conducting betting transactions including Pool Betting, National Lotteries Control Board operating On-Line Betting Games and Private Members’ Clubs.

If you carry on the business activities described in the First Schedule you are a Listed Business; and you MUST comply with legal obligations under the AML/CFT laws of Trinidad and Tobago and the FIU as your Supervisory Authority monitors your compliance.

The AML/CFT laws of Trinidad and Tobago in which you will find your obligations are:

- (1) Proceeds of Crime Act Chap. 11:27 as amended by Act No. 15 of 2014 - applies to all persons, but certain offences such as failure to report suspicious transactions only apply to Listed Business and Financial Institutions.
- (2) Anti-Terrorism Act Chap. 12:07 as amended by Act No. 15 of 2014 - establishes several offences where engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. The ATA applies to all persons but certain offences such as the failure to report suspicious transactions only apply to Listed Business and Financial Institutions.
- (3) Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Chap. 72:01 as amended by Act No. 15 of 2014 (“the FIU Act”);
- (4) Financial Obligations Regulations 2010 as amended by The Financial Obligations (Amendment) Regulations, 2014 (LN No.392) ;

Supervised Entity > GAMBLING SECTOR

- (5) Financial Intelligence Unit of Trinidad and Tobago Regulations 2011 as amended by the Financial Intelligence Unit of Trinidad and Tobago (Amendment) Regulations, 2014 (LN No. 403) ; and
- (6) Financial Obligations (Financing of Terrorism) Regulations 2011.

These laws are available on the FIU's website – <http://www.fiu.gov.tt/>

### **PART 3**

#### **THE ROLE AND FUNCTION OF THE FIU IN THE AML/CFT REGIME**

The Financial Intelligence Unit of Trinidad and Tobago ("FIU") was established by the FIU Act pursuant to Recommendation 29 of the 40+9 Recommendations of the Financial Action Task Force (the FATF)(previously Recommendation 26). Recommendation 29 mandates all its member jurisdictions to establish a Financial Intelligence Unit to serve as the information analysis related arm in efforts to combat Money Laundering, Financing of Terrorism and related crimes.

The FIU was created as an administrative type FIU, in that it does not have law enforcement or prosecutorial powers. Rather, it is a specialised intelligence agency which is legally responsible for producing financial intelligence for Law Enforcement Authorities (LEAs).

The FIU became operational in 2010 upon proclamation of the FIU Act. It is an autonomous department within the Ministry of Finance and the Economy.

The FIU works in very close partnership with Financial Institutions and Listed Businesses to ensure that those individuals and entities comply with their obligations to report certain information to the FIU. The FIU supervises and monitors Listed Businesses for compliance with their AML/CFT obligations.

#### **(1) Analyses and Produces Intelligence Reports**

Essentially, the FIU is responsible for producing financial intelligence that is then disclosed to LEAs for investigation. To do this, the FIU receives suspicious transaction reports and suspicious activity reports ("STRs/SARs") as well as financial information from various reporting entities such as banks, credit unions and other financial institutions, accountants, attorneys-at-law,

money services businesses, art dealers, motor vehicle sales, real estate, private members' clubs. A total of seventeen (17) different reporting sectors **must** provide STRs/SARs and financial information to the FIU.

When the FIU receives the STRs/SARs and information, the FIU conducts an analysis and looks for links between the financial information received, other relevant information from different sources, information provided by LEAs, as well as from other international partners.

The FIU receives many reports of suspicious transactions from reporting entities; but within those reports are legitimate transactions. The FIU's analysis is therefore, to ascertain those transactions on which there are reasonable grounds to suspect transactions are related to Money Laundering or Financing of Terrorism or related crimes.

Once the analysis leads to the belief that the transaction is related to suspicions of Money Laundering or Financing of Terrorism, the FIU sends an *Intelligence Report ("IR")* to the LEAs who will investigate the matter. The LEAs who investigate IRs from the FIU are the Commissioner of Police, Comptroller of Customs and Excise, Chief Immigration Officer and Chairman of the Board of Inland Revenue.

Only transactional information and information relating to the suspicion of Money Laundering and Financing of Terrorism are contained in the Intelligence reports. For example, the name and other information of the person who actually submitted the report would not be provided to LEAs.

## **(2) Supervises for AML/CFT Compliance**

Another important function of the FIU is to ensure compliance with obligations under the POCA, the ATA, the FIU Act and Regulations made under those Acts. The FIU is the Supervisory Authority for Listed Businesses and non-regulated financial institutions which have obligations under those Acts and Regulations and is responsible for making sure that they are meeting those obligations.

Activities related to the FIU's compliance mandate include educating and providing guidelines (such as this one), and enhancing public awareness of Money Laundering and Financing of Terrorism to allow entities who have AML/CFT obligations to be aware and know exactly what they need to do in terms

Supervised Entity > GAMBLING SECTOR

of meeting their obligations. The FIU also gives guidance as to implementation of compliance programmes, conducts on-site inspections and takes action to ensure that the law is being complied with the entities it supervises.

## **PART 4**

### **WHAT IS MONEY LAUNDERING?**

The offence of money laundering is the process by which funds derived from criminal activity (“dirty money”) are given the appearance of having been legitimately obtained through a series of transactions in which the funds are ‘cleaned’. Money Laundering allows criminals to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.

For money laundering to take place, first, there must have been the commission of a criminal activity which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies. There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and “shell” companies or as in the case of drug trafficking or other serious crimes, the proceeds may be in the form of cash which needs to enter the financial system by some means.

There are three (3) acknowledged methods in the Money Laundering process. However, the broader definition of Money Laundering offences in POCA includes even passive possession of criminal property.

#### **(1) Placement**

Placement is where funds derived from criminal activities are brought into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of Placement include depositing cash into bank accounts or using cash to purchase assets. Techniques used include “Structuring” or “smurfing” – where instead of making a large deposit transaction and in order to avoid suspicion, this is broken up into smaller cash deposits into single or multiple accounts sometimes using other persons to deposit the cash. -



## **(2) Layering**

This takes place after the funds have entered into the financial system and involves the movement of the funds. Funds may be shuttled through a complex web of multiple accounts, companies and countries in order to disguise their origins. The intention is to conceal, and obscure the money trail in order to deceive LEAs, to make the paper trail very difficult to follow and to hide the criminal source of the funds.

## **(3) Integration**

The money comes back to criminals “cleaned”, as apparently legitimate funds. The laundered funds are used to fund further criminal activity or spent to enhance the criminal's lifestyle.

Successful Money Laundering allows criminals to use and enjoy the income from their criminal activity without suspicion which is why the AML/CTF legislative and compliance regimes are important crime fighting tools.

## **PART 5**

### **WHAT IS FINANCING OF TERRORISM?**

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike Money Laundering, funds can come from both legitimate sources as well as from criminal activity for the financing of terrorism.

Funds may involve low dollar value transactions and give the appearance of innocence and can be from a variety of sources. Funds may be derived from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organise fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

---

Unlike Money Laundering, which involves always proceeds derived from criminal activity, with Financing of Terrorism you may have both legitimate funds as well as funds derived from criminal activity being used in support of executed and planned terrorist activity. Similar to money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence and to distance the funds from the crime or the source and to obscure the intended destination and purpose.

## **PART 6**

### **WHY ARE ENTITIES IN THE GAMBLING SECTOR DESIGNATED AS A LISTED BUSINESS?<sup>1</sup>**

The FATF, an inter-governmental body established in 1989, sets international standards with the aim of protecting the international financial system from misuse. These standards have been revised and expanded to cover emerging threats of money laundering well beyond drug money and to deal with the issue of funding terrorist activities. In 2012 the FATF reviewed its recommendations and reissued 40 Recommendations on Combating Money Laundering, the Financing of Terrorism and Proliferation. All member countries must implement effective measures to bring their national systems into compliance with these revised FATF Recommendations. FATF Recommendation 28 specified that certain non-financial businesses and professions (referred to as Listed Businesses), should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary measures to detect and deter money laundering and financing of terrorism.

While there are no legal casinos operating in Trinidad and Tobago, a March 2009 report by the FATF identified that there are seventy-two (72) registered Private Members Clubs that operate like casinos. There are also various games of chance and gambling forms ranging from casino and card room gaming, lotteries on-line gaming, race and sports wagering and charitable gaming, such as raffles, bingo and other low technology games.

---

<sup>1</sup> The information reproduced in this Part is taken from the Financial Action Task Force (FATF) Report Vulnerabilities of Casinos and Gaming Sector – March 2009

## Supervised Entity > GAMBLING SECTOR

The entities which comprise the gambling sector i.e. pool betting businesses, the NLCB and Private Members' Clubs are by definition non-financial institutions. As part of their operation they offer gambling for entertainment however they also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering. Many entities in the gambling sector conduct financial activities such as: accepting funds on account; conducting money exchange; foreign currency exchange; debit card; cashing facilities; cheque cashing; etc. In many cases these financial services are available 24 hours a day.

It is the variety, frequency and volume of transactions that makes the gambling sector particularly vulnerable to money laundering. These entities are by nature a cash intensive business and the majority of transactions are cash based. During a single visit to a Private Members' Club, for example, a customer may undertake one or many cash or electronic transactions, at either the "buy in" stage, during play, or at the "cash out" stage. It is this routine exchange of cash for chips or plaques, TITO (ticket in ticket out) tickets, and certified cheques, as well as the provision of electronic transactions to and from casino deposit accounts, clubs in other jurisdictions and the movement of funds in and out of the financial sector, which makes the gambling sector an attractive target for those attempting to launder money.

Private Members' Clubs and other such venues are consistently targeted by criminals for criminal influence and criminal exploitation. Criminals attempt to infiltrate or influence these businesses to facilitate theft, fraud, money laundering and other crimes. Gambling venues attract ancillary criminal activities including loan sharking, vice and other crimes.

## PART 7

### EXAMPLES OF MONEY LAUNDERING USING THE GAMBLING SECTOR - CASES TAKEN FROM FATF REPORT, OCTOBER 2010

#### **Case 1 - Proceeds of drugs trafficking used to purchase chips and claim funds as winnings**

Offence: Drug importation

Jurisdiction: Australia

Technique: Chip purchase and cash out

Mechanism: Casino

Instrument: Casino chips, chip to cash transfer, casino cheques

A cargo consignment addressed to a person contained approximately 3.4 kilograms of black opium resin, concealed within the contents. The person was arrested when attempting to collect the consignment. Further investigation revealed the person to be a regular customer of a casino, having conducted approximately 50 betting transactions, predominantly chip cash- outs totalling AUD 890 000. Very little casino gaming play was recorded for the person and it was assumed that he used the proceeds from previous importations to purchase chips and claim the funds as winnings.



#### **Case 2 - Proceeds from bank hold up laundered through book-makers**

Offence: Money Laundering

Technique: Low Risk Bets, playing games with low return and high win, betting on favourites.

Mechanism: Bookmakers, Multiple bank accounts

Instrument: Cash, cheques

During police investigations into armed robberies, it came to light that another individual had been placing a vast number of bets at various book-makers within one city. He always followed a similar pattern whereby the stakes were high and the odds low. In other words, he bet on "favourites" who were likely to win, although this likelihood meant that the sum received by the bet maker if he did win was relatively small. Consequently, he made a 7% net loss over a long period of time. This would be quite a serious loss for a professional gambler. He never received his winnings personally, but had cheques made out to a total of 14 different bank accounts in the names of 10 third parties. It was discovered that several of the cheques were issued in the names of the armed robbers and their immediate families. The link between the money launderer and the original criminals was established. The former was convicted of money laundering and sentenced to 5 years imprisonment. He had laundered approximately USD 3.3 million through this system.

### **Case 3 - Overseas nationals purchase winning jackpots with illegal proceeds**

Offence: Drug trafficking & money laundering

Technique: Buying winning lottery tickets

Mechanism: Lotteries

Instrument: Winning jackpots, cash

Indicators: purchasing winning jackpots; depositing winning cheques followed by immediate withdrawal

AUSTRAC referred a matter relating to a group of overseas nationals buying winning jackpots at various clubs in Sydney from legitimate winners. The suspects deposited approximately AUD1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means. This matter was referred to partner agencies for further investigation.

## **PART 8**

### **WHAT ARE YOUR AML/CFT LEGAL OBLIGATIONS?**

The AML/CFT laws of Trinidad and Tobago impose obligations on you to:

- I. *Register with the FIU;*
- II. *Submit Reports to the FIU;*
- III. *Not to "Tip-off";*
- IV. *Keep Records;*
- V. *Ascertain client identity;*
- VI. *Ascertain whether the client is acting for a Third Party;*
- VII. *Appoint a Compliance Officer and an Alternate Compliance Officer*  
;
- VIII. *Develop and implement a written compliance programme approved by senior management and reasonably designed to ensure compliance with the law.*

#### **I. REGISTRATION WITH THE FIU**

You **must** register with the FIU for the purpose of identifying yourself as an entity which is supervised by the FIU if you perform any of the specified activities.

All entities/persons subject to supervision by the FIU MUST register with the FIU within three (3) months of commencing business activity or incorporation as a company under the laws of Trinidad and Tobago, whichever is the earlier.

You **must** also notify the FIU of a change of address of your registered office or principal place of business within six (6) months of such change.

**(1)      *How to Register***

Register on **the FIU's Registration Form**, which you may access by [clicking here](#).

The registration process is very simple and free of charge. On-line pre-registration is available through the FIU's website. However, you must download and print the completed pre-registration form. To complete the registration process you must sign your printed pre-registration form and **manually submit this to the FIU**. Register on **the FIU Registration Form** which **you may access by [clicking here](#)**.

**(2)      *Offences***

- Failure to register within the time stipulated is an offence and you are liable on summary conviction to a fine of \$50,000 and to a further fine of \$5,000 for each day the offence continues
- Failure to notify the FIU of a change of address of your registered office or principal place of business within 6 months is an offence and you are liable on summary conviction to a fine of \$20,000
- Failure to notify the FIU of changes of Directors, Owners, Partners or Compliance Officer within six months of such a change is an offence and you are liable on summary conviction to a fine of \$20,000.

**II.      SUBMITTING REPORTS TO THE FIU**

You are required to send to the FIU two (2) types of reports:

- (1) reports of Suspicious Transactions or Activities; and**
- (2) reports of Terrorist Funds in your possession.**

The relationship between reporting entities and the FIU is a key one, because the FIU can only perform its analytical function as a crime fighting tool to produce financial intelligence if the various reporting entities report the critical information where there is a suspicious basis.

**Failing to report to the FIU knowledge or suspicion of crime proceeds or terrorist property is a criminal offence.** If you continue to deal with such a transaction or funds knowing or having reasonable grounds to believe that the funds are crime proceeds or terrorists' funds and you do not report it to the FIU then you may have committed the offence of money laundering or financing of terrorism yourself.

**a) Reports of Suspicious Transactions/Activities**

- i. You must submit a Suspicious Transaction Report or Suspicious Activity Report (STR/SAR) to the FIU where you know or have reasonable grounds to suspect:
- that funds being used for the purpose of a transaction are the proceeds of a crime; or
  - a transaction or an attempted transaction is related to the commission or attempted commission of a Money Laundering offence; or
  - that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism.

The STR/SAR must be submitted **within fourteen (14) days of the date the transaction was deemed to be suspicious.**

- ii. You **must also** submit a STR/SAR to the FIU **immediately** if a designated entity\* attempts to enter into a transaction or continue a business relationship. **You must not enter into or continue a business transaction or business relationship with such entity.**

**\*A designated entity means any individual or entity and their associates designated as terrorist entities by the Security Council of the United Nations or any individual or entity listed on the consolidated list circulated by the FIU.**

Report using the **STR/SAR Form** which you may access by [clicking here](#).

You may access the **Security Council of the United Nations List ("the UN list")** by [clicking here](#).

[Click Here](#) for **STR Reporting Standard No 1 of 2011** to guide you in completing the STR/SAR form.

iii. ***Defining Knowledge and Suspicion***

The first criterion provides that, before you become obliged to report, **you must know or have reasonable grounds for suspecting**, that some other person is engaged in Money Laundering or Financing of Terrorism.

If you actually 'know' that your client is engaged in Money Laundering, then your situation is quite straightforward – the first criterion is met. However, knowledge can be inferred from the surrounding circumstances, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge.

You are also required to report if you have 'reasonable grounds' to suspect that the client or some other related person is engaged in Money Laundering or Financing of Terrorism. By virtue of this second, 'objective' test, the requirement to report will apply to you if based on the facts of the particular case, a person of your qualifications and experience would be expected to draw the conclusion that those facts should have led to a suspicion of Money Laundering or Financing of Terrorism. The main purpose of the objective test is to ensure that the Gambling Sector (and other regulated persons) are not able to argue that they failed to report because they had no conscious awareness of the Money Laundering activity, e.g. by having turned a blind eye to incriminating information which was available to them.

**iv. *Attempted Transactions***

You also have to pay attention to **suspicious attempted transactions**. If a client attempts to conduct a transaction, but for whatever reason that transaction is not completed, and you think that the attempted transaction is suspicious, you must report it to the FIU.

Example of suspicious attempted transaction: a visitor walks into your members' club. He says he would like to play the slot machines; he has \$5,000 in cash to spend. He says his name is John X but when you ask him for identification he replies that he left it in his car. You insist he provide it. He goes away to get it but does not return. If you think from all the information you have that this is unusual or the transaction is related to some crime you have to report that attempted transaction to the FIU.

**NOTES:**

It is only when you know or reasonably suspect that the funds are criminal proceeds or related to Money Laundering or Financing of Terrorism that you have to report: you do not have to know what the underlying criminal activity is or whether illegal activities have actually occurred.



Money Laundering can take place with any amount of money/cash. If you think a \$ 1,000 transaction is suspicious, you must report it to the FIU.

You must report suspicious transactions/activities and attempts by a terrorist entity\* to enter into a transaction or continue a business relationship **on the STR/SAR Form which you may access by [clicking here](#)**.

[Click here](#) for **Guidance Note on Suspicious Transaction/Activity Reporting Standards** to guide you in completing the STR/SAR form.

**v. *Identifying a Suspicious Transaction/Activity***

You must determine whether a transaction or activity is suspicious based on your knowledge of the customer and of the sector. You are better positioned to have a sense of particular transactions which appear to lack justification or cannot be rationalized as falling within the usual methods of legitimate business. While general indicators may point to a suspicious transaction, sector-specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

***What are the risk indicators for Gambling and Betting activities?***

Gambling and Betting activities can be used to facilitate money laundering through each of the three money laundering stages: placement, layering and integration and/or the financing of terrorism.

The following circumstances may indicate a risk of money laundering or terrorism financing occurring:

- betting activity is inconsistent with the financial situation and/or known occupation of the person gambling;
- purchase of winning tickets from other punters (gamblers) at a premium;
- purchasing of winning jackpots or winning lottery tickets at a premium;
- playing games with low returns but high chances of winning, such as Baccarat;
- placing bets whereby the stakes are high and the odds low;

Supervised Entity > GAMBLING SECTOR

- simultaneous “put” and “call” transactions (in essence, “side bets” on a win/lose game) on behalf of the same client.

See the [Appendix](#) (end of document) for a list of red flags and suspicious indicators of which you should be cognizant.

**(b) Reports of Terrorist Property/Funds**

- You **must report immediately** to the FIU the existence of funds within your business where you know or have reasonable grounds to suspect that the funds belong to an individual or legal entity who:
  - commits terrorist acts or participates in or facilitates the commission of terrorist acts or the financing of terrorism; or
  - is a terrorist entity.
- You **must report immediately** to the FIU where you know or have reasonable grounds to believe that a person or entity named on the UN list or the consolidated list circulated by the FIU has funds in Trinidad and Tobago.
- is a Listed Entity as included in the Trinidad & Tobago Consolidated List of Court Orders.  
[Click here](#) for Trinidad & Tobago Consolidated List of Court Orders web page.

Report the existence or suspicion of terrorist funds on the **Terrorist Funds Report - FIU TFR Form** which you may access by [clicking here](#).

**III. NO TIPPING-OFF**

When you have made a suspicious transaction report to the FIU, you or any member of your staff must not disclose the fact or content of such report to any person. It is an offence to deliberately tell any person, including the customer, that you have or your business has filed a suspicious transaction report about the customer’s transactions.

You must also not disclose to anyone any matter which may prejudice money laundering or financing of terrorism investigation or proposed investigation.

This prohibition applies to any person acting, or purporting to act on behalf of the business including any agent, employee, partner, director or other officer, or any person engaged under a contract for services.

#### IV. RECORD KEEPING

You are required to keep a record of each and every transaction for a specified period. Record keeping is important for use in any investigation into, or analysis of, possible money laundering or financing of terrorism offences. Records must be kept in a manner which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

You must keep the following records in electronic or written format for at least six (6) years or such longer period as the FIU directs. The records must be kept for six (6) years after the end of the business relationship or completion of a one-off transaction:

- (1) All domestic and international transaction records;
- (2) Source of funds declarations;
- (3) Client identification records;
- (4) Client information records;
- (5) Copies of official corporate records;
- (6) Copies of suspicious transaction reports submitted by your staff to your Compliance Officer;
- (7) A register of copies of suspicious transaction reports submitted to the FIU;
- (8) A register of all enquiries made by any Law Enforcement Authority or other competent authority;
- (9) The names, addresses, position titles and other official information pertaining to your staff;
- (10) All Wire transfers records (originator and beneficiary identification data); and
- (11) Other relevant records.

#### V. ASCERTAINING IDENTITY

You must identify and verify the identity of customers as part of your customer due diligence obligations (CDD). This applies where:

- a person may engage in a financial transaction as a one-off or occasional transaction in the sum of TTD 90,000 or more;
- where there are two or more one-off transactions which in total amounts to TTD 90,000 or more in value and it appears that the transactions are linked; and

- there is a one-off or occasional wire transfer of TTD 6,000 or more or where there are two or more wire transfers which collectively total TTD 6,000 or more and it appears that the transactions are linked.

With respect to private members' clubs you must carry out CDD where a customer engages in a transaction of TTD \$18,000 or more and where a customer engages in two or more transactions which may be less than TTD 18,000 but together the value is TTD18,000 or more and it appears the transactions may be linked.

Conducting customer identification at entry could be, but is not necessarily, sufficient. You must ensure that you are able to link customer due diligence information for a particular customer to the transactions that the customer conducts.

If you are unable to identify and verify a client's identity or obtain sufficient information about the nature and purpose of a transaction, you must **NOT** carry out a transaction for that client or enter into a business relationship with the client and you must terminate any business relationship already established. You should also consider submitting a STR/SAR to the FIU.

### High Risk Clients/ Transactions

There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced due diligence (EDD) measures have to be taken. You must take specific measures to identify and verify the identity of the following high risk persons (individuals or entities):

- (1) Any person who conducts a large cash transaction or receives a large pay-out i.e. equal to or over TTD 90,000;
- (2) Any person who conducts business transactions with persons and financial institutions in or from other countries which do not or which insufficiently comply with the recommendations of the Financial Action Task Force ("the FATF");

[Click here](#) for **FATF High Risk and Non-Cooperative Jurisdictions**;

- (3) Domestic and Foreign Politically Exposed Persons (PEPs);

[Click here](#) for **Customer Due Diligence Guide No. 1 of 2011** for the categories of persons who are PEPs;

- (4) Any client or transaction or service or product type that you have identified as posing a higher risk to your business e.g., transactions which involve high levels of funds or cash;
- (5) Any individual or entity who conducts complex, unusual large transactions, (whether completed or not), unusual patterns of transaction and insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
- (6) Any individual or entity who conducts business transactions with persons and financial institutions in or from other countries which do not or insufficiently comply with the recommendations of the FATF; [Click here](#) for **FATF High Risk and Non-Cooperative Jurisdictions**.
- (7) Any individual or entity for whom you have to send a suspicious transaction report to the FIU (reasonable measures and exceptions apply e.g. to avoid **tipping-off**).

You must apply EDD to high risk customers and situations as detailed in Part II which include, but are not limited to:

- (1) Obtaining additional information on the customer e.g., additional form of Government issued identification;
- (2) Obtaining details of the source of the client's funds, source of wealth of the customer and the purpose of the particular transaction if relevant;
- (3) Verifying the source of funds for the transaction e.g., if client states the cash is from his bank account, ask for proof;
- (4) Obtaining approval from a senior officer to conduct the transaction;
- (5) Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;
- (6) Ongoing monitoring (e.g., monthly, quarterly, annually or on a transaction basis) of the client's account throughout the relationship; and
- (7) Implementing any other customer identification policies and procedures to prevent money laundering and financing of terrorism.

#### **VI. Is the Client acting for a Third Party?**

You must take reasonable measures to determine whether the client is acting on behalf of a third party. Such cases will include where the client is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, you must obtain information on the identity of the third party and their relationship with the client.

In deciding who the beneficial owner is in relation to a client who is not a private individual, (e.g. a company or trust) you should look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support.

Particular care should be taken to verify the legal existence and trading or economic purpose of corporates and to ensure that any person purporting to act on behalf of the company is fully authorized to do so.

**[Click here](#) for Customer Due Diligence Guide No. 1 of 2011  
for more information**

#### **VII. APPOINT A COMPLIANCE OFFICER AND AN ALTERNATE TO THE COMPLIANCE OFFICER**

You must appoint a senior employee at managerial level as Compliance Officer ("the CO"). The individual you appoint will be responsible for the implementation of your compliance regime. The identity of the CO must be treated with the strictest confidence by you and your staff.

You must also appoint an alternate to the CO ("ACO") who shall be a senior employee (in the case of financial institutions) and/or other such competent professional approved in writing by the relevant supervisory authority in the case of a listed business. The alternate shall discharge the functions of the CO in his absence.

You must obtain the approval of the FIUTT for the person chosen as the CO and the alternate to the CO. If you change your CO you must inform the FIU immediately and get the FIU's approval for the new CO.

If you are a small business, employing five (5) persons or less, the CO must be the person in the most senior position.

If you are the owner or operator of the business and do not employ anyone, you can appoint yourself as CO to implement a compliance regime.

If you are a business employing over five [5] persons, the CO should be from a senior management level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed CO in a large business should not be directly involved in the receipt, transfer or payment of funds.

Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on your type of business, your CO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

Your CO and ACO should have the authority and the resources necessary to discharge his or her responsibilities effectively. They must:

- (1) have full responsibility for overseeing, developing, updating and enforcing the AML/CFT Programme;
- (2) have sufficient authority to oversee, develop, update and enforce AML/CFT policies and procedures throughout the company; and
- (3) be competent and knowledgeable regarding AML/CFT issue, risks and legal framework.

Depending on your type of business, your CO/ACO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator of the business.

The CO's/ACO's responsibilities include:

- a) Submitting STRs/SARs and TFRs to the FIU and keeping relevant records;
- b) Acting as Liaison officer between your business and the FIU;
- c) Implementing your Compliance Programme;
- d) Directing and enforcing your Compliance Programme;
- e) Ensuring the training of employees on the AML/CFT;
- f) Ensuring independent audits of your Compliance Programme; and
- g) Record keeping of STRs/SARs

For consistency and ongoing attention to the compliance regime, your appointed CO may choose to delegate certain duties to other employees. For example, the CO may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the CO retains full responsibility for the implementation of the compliance regime.

## VIII. DEVELOP, A COMPLIANCE PROGRAMME

After you have registered with the FIU as a reporting entity, you **must** develop a written Compliance Programme (“CP”). If you are an organization the CP should be approved by senior management.

[Click here](#) for the CP Check list.

The CP is a written document explaining your system of internal procedures, systems and controls which are intended to make your business less vulnerable to being used by money launderers and terrorist financiers. Your CP will contain measures that ensure that you comply with your reporting, record keeping, client identification, employee training, and other AML/CFT obligations. These policies, procedures and controls, must be communicated to employees, and when fully implemented, will help reduce the risk of your business being used for money laundering or to finance terrorism.

A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, your compliance regime will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations as well as the vulnerability of your business to money laundering and terrorism financing activities.

In accordance with Regulation 7 of the Financial Obligation Regulations (as amended), the CP shall be designed to include policies, procedures and controls for:

- a) customer identification, documentation and verification of customer information and other customer due diligence measures;
- b) identification and internal reporting of STRs/SARs;
- c) adoption of a risk-based approach to monitoring financial activities;
- d) external and independent testing for compliance;
- e) An effective risk-based audit function to evaluate the CP;
- f) internal control and communication as may be appropriate to forestall money laundering;
- g) retention of transaction records and other information;
- h) a list of countries, published by the FIU which are non-compliant, or do not sufficiently comply with the FATF’s Recommendations; and



- i) adoption of risk-management and procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

[Click here](#) to access the **Guide to Structuring an AML/CFT Compliance Programme**

## **IX. IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME**

Your obligations include implementing your written CP. The FIU may conduct an onsite examination to determine the effectiveness of implementation of the measures outlined in your CP.

The FIU may conduct an on-site examination to determine whether the measures outlined in your CP are effectively implemented.

All employees involved in the day-to-day business should be made aware of the policies and procedures in place in the business to prevent money laundering and financing of terrorism.

You must conduct internal testing to evaluate compliance by your staff with your CP, in particular, CDD record keeping and suspicious transactions reporting.

In addition, you must conduct internal testing and external independent testing to evaluate the effectiveness of your systems and controls and implementation of same. Such reviews must be well documented and should be available to the FIU.

## **PART 9**

### **OFFENCES & PENALTIES**

Non-compliance with your obligations under the AML/CFT laws and regulations may result in criminal and or administrative sanctions.

[Click here](#) to access a summary of the Offences and Penalties under the AML/CFT laws and regulations of Trinidad and Tobago.

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT laws. You may access the laws on the FIU's website, [www.fiu.gov.tt](http://www.fiu.gov.tt) under "Legal Framework".

[Click here](#) to access the laws.

## PART 10

### ADDITIONAL RESOURCES

Additional reference materials include:

- I. the AML/CFT laws available on the FIU's website, [www.fiu.gov.tt](http://www.fiu.gov.tt) under "Legal Framework".
- II. FATF Report – Vulnerabilities of Casinos and Gaming Sector – March 2009 at <http://www.fatf-gafi.org/topics/methodsandtrends/documents/vulnerabilitiesofcasinosandgamingsector.html>
- III. The FATF recommendations at [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)



Revised August, 2017

Susan Francois  
Director

**APPENDIX**

**AML/CFT Suspicious Indicators for the Gambling Sector**

Gambling at gaming venues — casinos, pubs, clubs, racing and sports betting facilities— is a traditional channel for the placement(moving, dispersing or disguising funds) and layering (reinvesting funds) phases of the money laundering cycle.

Money launderers exploit this high cash turnover and the large volume of transactions to camouflage illegitimate transactions among legitimate gambling activity.

The following circumstances may indicate a risk of money laundering or terrorism financing occurring:

- Betting activity is inconsistent with the financial situation and/or known occupation of the person gambling;
- Purchase of winning tickets from other punters (gamblers);
- Substantial cash redemptions of negotiable gaming chips despite the absence of, or minimal, gaming activity;
- Frequent deposits of personal bank cheques exchanged for chip purchase vouchers but limited gambling activity undertaken;
- Frequent deposits of gambling cheques followed by immediate withdrawal of funds with cash or cheques;
- Filling a gambling machine with credits and collecting the pay-outs with little gambling activity (this occurs particularly in VIP sections of gaming venues where there is no limit on credits);
- Gambling chips handed to a third party for the purposes of redemption;
- Multiple chip redemptions on the same day;
- Buying casino chips and cashing them in with no or little gaming activity;
- A client depositing with either a book-maker or a casino, substantial amounts of cash for gambling purposes, but requesting cheque for repayment of funds not used;
- Suspicious identification documentation presented for gambling purposes when opening an account.

*(continued on next page)*

- Putting money into slot machines and claiming the accumulated credits as a jackpot win;
- Playing games with low returns but high chances of winning, such as Baccarat;
- Sports betting and the purchasing of winning jackpot;
- Exchanging large amounts of small denomination bank notes for larger denominations without gambling;
- Wiring funds to a casino account followed by a withdrawal by casino issued cheque;
- Inserting significant numbers of bank notes into a slot machine and collecting payment of the built up credits by way of a casino issued cheque;
- Loaning funds for gambling to legitimate businessmen with repayment of the funds being a discounted amount;
- Frequent claims for winning jackpots;
- Customers watching/hanging around jackpots sites but not participating in gambling;
- Betting against associates/intentional losses: This occurs in games which provide money launderers the option to bet against an associate so that in most cases one party will win. These are “intentional losses” where money launderers are intentionally losing to one of their party, who is able to receive a cheque or wire transfer of “legitimate” winnings;
- VIP rooms and high-stakes gambling: VIP rooms offer exclusive access to high-stakes gaming tables to players. VIP members can place high-value bets in these rooms. High-stakes gaming is vulnerable to abuse because it is common for players to gamble with large volumes of cash, the source and ultimate ownership of which may not be readily discernible. In compliance with AML regulatory obligations, you must closely monitor and track VIP and high-stakes gaming activity.

**Please note that this is not an exhaustive list of suspicious indicators.**