Hosted by the Public Accountancy Board in collaboration with the Institute of Chartered Accountants of Jamaica

Reconciled with AML/CFT/CFP Compliance

May 19 & 20 , 2021

Christine Chambers, CAMS, FCA, MSc
FINANCIAL FORENSICS

Seminar Objectives

- At the end of today's session, you should -
  - Understand the regulatory obligations in relation to your clients (CDD/KYC procedures)
  - Have some understanding of the Risk-Based Approach
  - Have knowledge of the reporting and record keeping requirements, including document retention
  - Be aware of the revised sanctions for non-compliance with the AML/CFT/CFP programme

Regulatory Controls

The Proceeds of Crime Act, the Terrorism Prevention Act and the United Nations Security Council Resolution Implementation Act and their attendant Regulations all contain specific provisions that promote the effective implementation of legal, regulatory and operational measures for combating money laundering and the financing of terrorism and proliferation.

Regulatory Controls

Establish & implement programmes, policies, procedures & controls to detect, prevent & deter money laundering, terrorist financing and proliferation financing (including controls for group companies)

POC MLP Reg. 5 (1) & (2)
TPA Sec. 18 (1) & (2)
UNSCRIA Sec. 21(2)

Designate a Nominated Officer to be responsible for policy implementation & filing of reports

POC MLP Reg 5(3)
TPA Sec. 18 (3)
UNSCRIA Reg. 4

Report: Suspicious Transactions, Listed Entity Relationships or Transactions and Authorized Disclosures

POC MLP Reg. 5 (3)
TPA Sec. 18 (3)
UNSCRIA Reg. 5(2) & 5(3)

Establish: Risk Profile on its Operations, Risk Profiles for Business Relationships and On-going Due Diligence

POC (MLP) Reg. 7A & TP (RE) Reg. 6A

Regulatory Controls

The AML/CFT/CFP obligations of the regulated sector can be summarized as follows:

Regulatory Controls

Establish & implement programmes, policies, procedures & controls to detect, prevent & deter money laundering, terrorist financing & proliferation (including controls for group companies)

POC MLP Reg. 5 (1) & (2)
TPA Sec. 18 (1) & (2)
UNSCRIA Sec 21(2)

Designate: Nominated officer at the management level for policy implementation & filing of reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)
UNSCRIA Reg. 4

Report: Suspicious, Listed Entity Transactions, Authorized Disclosures and Proscribed Entity Reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)
UNSCRIA 5(2) & 5(3)

Establish: Risk Profile on its Operations, Risk Profiles for Business Relationships and On-going Due Diligence

POC MLP Reg. 7A & TP RE Reg. 6A

Procedures: For the proper identification & verification of customers

(CDD/KYC)

System: To evaluate the integrity and employment & financial history of employees

Programme: For training of Employees on continuing basis regarding AML and CFT obligations

Arrange: Independent audit to evaluate AML/CFT/CFP compliance

Financial Forensics

Regulatory Controls

Reg. 5(1) of POC (MLP) Regs. stipulates that ***"a regulated business shall establish and implement such programmes, policies, procedures and controls as may be necessary for … preventing or detecting money laundering."***

Sec. 18(1) of the TPA provides that ***"every entity referred to in Sec. 15(2) shall establish and implement such programmes, policies, procedures and controls as may be necessary … for enabling it to fulfill its duties ..."***

Sec 21 (2) of the UNSCRIA addresses the making of provisions as to ***"the programmes, policies, procedures and controls to be established and implemented by entities …"*** to enable compliance with this Act.

Regulatory Requirements

- The development of a regulated entity's policies and procedures **must take into account the size and nature of the business concerned. [Reg 5(1)]**
- Where the regulated business is part of a group, policies and procedures should **allow the sharing of information within the group** for purposes of **customer identification**, **transaction verification** and **risk management**. They should also safeguard the **confidentiality and use** of the information shared. **[Reg 5(2)(e)]**

Regulatory Requirements

- The programmes and controls established must be documented, e.g. in an AML/CFT/CFP Policies and Procedures Manual.
- This AML/CFT/CFP manual guides the staff on the institution's policies and the operating procedures to implement those policies.
- It must include:

Regulatory Controls

Establish & implement programmes, policies, procedures & controls to detect, prevent & deter money laundering & terrorist financing (including controls for group companies)

POC MLP Reg. 5 (1) & (2)
TPA Sec. 18 (1) & (2)

Designate: Nominated officer at the management level for policy implementation & filing of reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)

Report: Suspicious, Threshold and Listed Entity Transactions, Authorized Disclosures and Proscribed Entity Reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)

Establish: Risk Profiles for Operations, Risk Profiles for Business Relationships and On-going Due Diligence

POC MLP Reg. 7A & TP RE Reg. 6A

Procedures: For the proper identification of customers

(Customer Due Diligence/ Know Your Customer)

System: To evaluate the integrity and employment & financial history of employees

Programme: For training of employees on continuing basis regarding AML/CFT/CFP obligations

Arrange: Independent audit of the AML/CFT/CFP programme

Identification Procedures – CDD/KYC

The regulated sector must adopt and implement comprehensive Customer Due Diligence/Know Your Customer policies, procedures, and processes for all customers, particularly for customers that present a high risk for money laundering or terrorism financing.

Customer Due Diligence (CDD)

Customer Due Diligence involves identifying the customer and verifying that customer's identity.

If the customer is a legal person, or formed on a legal arrangement, customer identification will **include identifying and verifying all beneficial owners**.

Who is a Beneficial Owner?

For a Body Corporate – the individual who ultimately owns or controls the body corporate

For an Applicant for Business – the individual on whose behalf the applicant for business conducts the business or one-off transaction

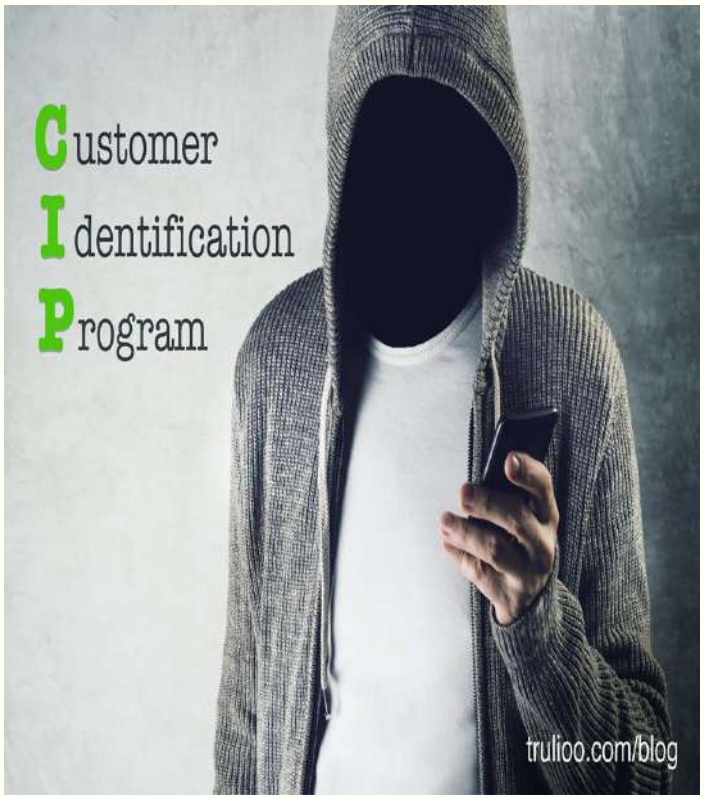
For a Trust, Settlement or Legal Arrangement - the individual who ultimately owns or controls the trust, settlement, legal arrangement

Know Your Customer (KYC)

Know Your Customer is satisfactorily confirming the customer's identity and establishing details about that customer, such as occupation, personal financial and business track record, source of funds **AND source of wealth**, the capacity in which the business is being conducted, authority to act for persons benefitting from the transaction, criminal background.

Customer Due Diligence/Know Your Customer

On completion of the Customer Due Diligence (CDD) and Know Your Customer (KYC) exercise, the regulated business should be reasonably confident that it knows the true identity of each customer and knows the types of business and transactions they are likely to engage in.



CDD/ KYC – Types of CDD

There are 3 types of CDD –

- **Standard Due Diligence**
  - **Most frequently used**
- **Enhanced Due Diligence**
  - **For higher risk customers**
- **Simplified Due Diligence**
  - **For lower risk customers**

All three are background checks on the customer to ensure that they are properly risk assessed before being onboarded.

Customer Due Diligence/Know Your Customer

Customer information has been expanded and now includes –

a) The applicant's full name, current address, TRN or other reference number, date and place of birth and mother's maiden name (if an individual) and, if applicable, information relating to the identity of beneficial owners or controllers of trusts, settlements, bodies corporate, other legal arrangements and the beneficiaries of life insurance policies.

b) Any other information used to verify the applicant's trade, profession or source of funds.

Financial Forensics

Identification of Individuals

In addition to customer information as defined, information to be obtained from all prospective individual customers includes:

- Names used (aliases, a.k.a.);
- Nationality;
- Contact numbers (work; home; cell)

Verification of Identification

The following may be used to verify CDD, KYC and transaction information:

- **Checking with issuing agencies – PICA, Electoral Office, Tax Administration**
- Utility bills or credit cards statements in the name of the applicant
- **Web search on the applicant's name**
- Other methods may be included in Bank's Policies and Procedures manual

Verification of KYC Information

The following documents may be used to verify:

Occupation – Employment letter, Contract/Agreement to provide service, public records that show customer's position.

Source of Funds – Employment letter, pay slips, pension advise of payment, bank withdrawal document, payment advise, electronic transfer confirmation.

Source of Wealth – Business & financial history of the applicant

Authority to act for another – Letter giving authority for agent/bearer to perform a specific act on behalf of the signatory, ID of signatory, ID of representative.

Identification Procedures – New Customer

In carrying out the identification and verification procedures on a new applicant, **risk management measures** are to be applied **while the identification procedures to verify the applicant's identity** is being done. [Reg 7 (1)(a)]

A **time limit** of **14 days after first contact** for the **verification of the applicant's identity** has been specified in Reg 7 (1)(b).

Identification Procedures

Individuals

Evidence of identity is satisfactory if it reasonably establishes the applicant to be the person he claims to be **and all persons on whose behalf he acts in relation to that business are who they claim to be**.

The beneficial ownership provisions are emphasized in both POCA and the TPA (often mirrored).

Customer Due Diligence (CDD)

If the customer is a person other than an individual, customer identification will include identifying and verifying the identity of the individuals who hold 10% or more of the ownership of that person and the individuals who exercise ultimate effective control over that person.

Where an individual who exercises ultimate effective control over that person cannot be identified, or there is doubt about that individual's identity, it identifies, and verifies the identity of the senior manager who makes or implements decisions with respect to the activities of that person

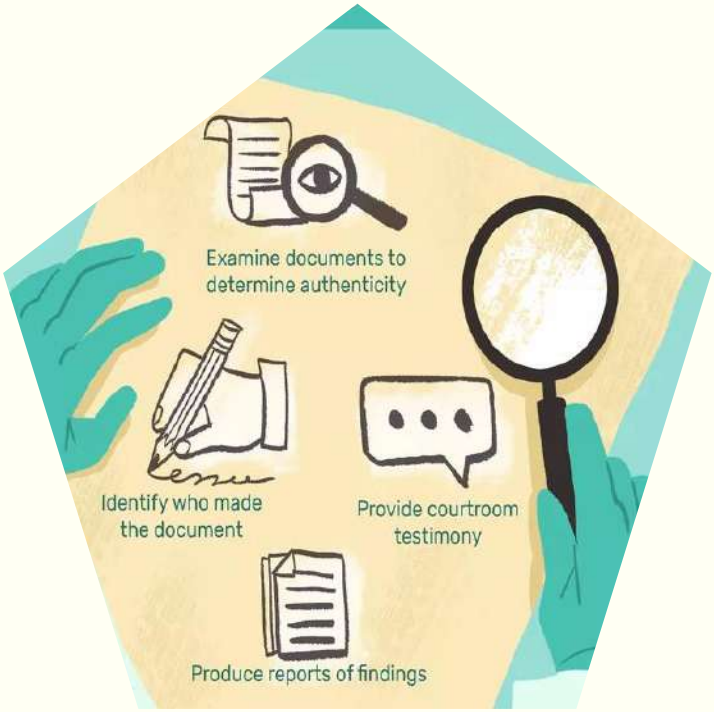
Identification Procedures

For a **body corporate,** evidence of identity is satisfactory if for any transaction involving a body corporate which is **licensed** or otherwise authorized under the **laws of the jurisdiction** in which the body corporate is **registered**, it identifies, and verifies the identity of **each director and shareholder (if any) holding ten per cent or more of the voting rights or ownership** in the body corporate.

KYC – Identification – Overseas Residents

The requirements for individuals resident overseas are the same as for local individuals, or their equivalents for their country of residence.

Particular attention should be paid to the place of origin of identity and other documents provided and the background against which they are produced, bearing in mind that standards of control vary between countries.



KYC – Identification – Overseas Bodies Corporate

Requirements are the same as for local companies. A financial institution may request certified copies of documents, notarised by a foreign official, such as a notary public, or county clerk in addition to making appropriate enquiries with overseas credit reference agencies or similar bodies.

Financial institutions **should not establish** business relationships with **foreign entities with bearer shares**.

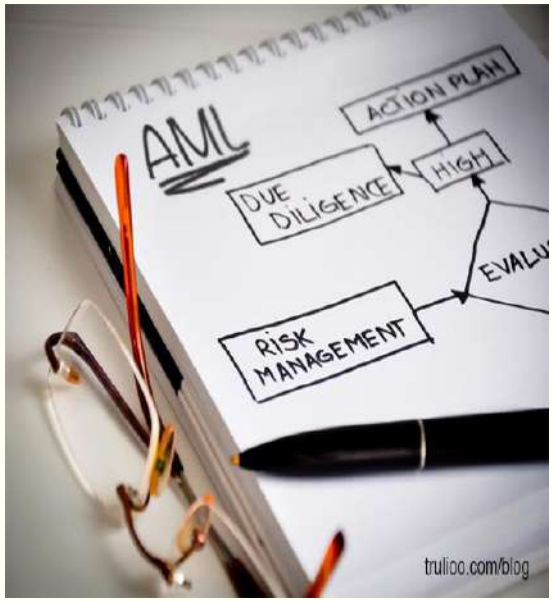
KYC – Identification – Overseas Bodies Corporate

A high level of caution should also exercised when establishing business relationships with **foreign companies that have nominee shareholders**.

If the ultimate beneficiaries or beneficial shareholders **cannot be reliably established** or there are no reliable measures in place to monitor any changes in the ownership structure, **the relationship should not be commenced**, or where a business relationship has already been established, **this relationship should be legally terminated.**

Enhanced Due Diligence (EDD)

Enhanced Due Diligence ("EDD") procedures should be engaged for all business relationships determined to be high risk. **EDD requires verification of both the source of funds and source of wealth. [Reg 7 (5)(b)]**



***** *Enhanced Due Diligence is additional information collected for higher-risk customers to provide a deeper understanding of customer activity to mitigate associated risks***

What Are High Risk Relationships?

High risk relationships or transactions include cases where the applicant for business is:

- **A Politically Exposed Person (PEP)**
- **A person not ordinarily resident in Jamaica**
- **A person resident or domiciled, or incorporated if a company, in a specified territory**
- **A person acting as a trustee for another**
- **A company with nominee shareholders or shares held in bearer form**
- **Not the ultimate beneficial owner of the assets concerned in the business relationship or one-of transaction [Reg 7A (2)(e)]**
- **Such other class or category of persons as the supervisory authority may specify and where the applicant was, but no longer is, ordinarily resident overseas. [Reg 7A (2)(f)]**

- Spouse
- Children and their spouses (including step and adopted children)
- Parents
- Brother or sister

- Head of State or Head of Government
- Members of any House of Parliament
- Minister of Government
- Member of the judiciary and senior military and police officers
- Directors and CEOs of state owned companies

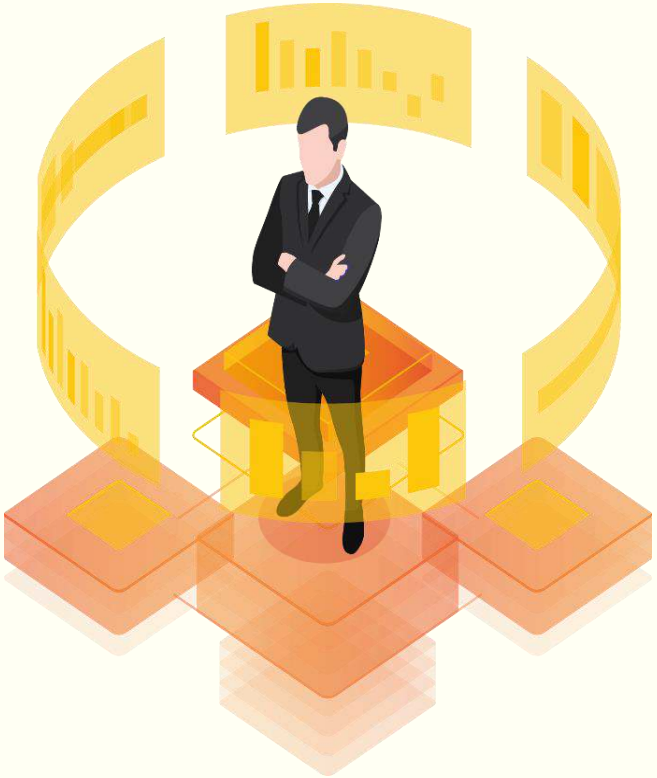
- Permanent Secretaries, CTDs or COOs of ministries, departments, executive agencies or statutory bodies
- Any official of any political party;
- persons entrusted with a prominent function by an international organization

- Business partner or associated in any other form **(whether as beneficial owner or otherwise)** in a common commercial enterprise

Politically Exposed Person

Financial Forensics

What Are High Risk Relationships?



In respect of any business relationship or one-off transaction with any category of person specified under Reg. 7A (2)(f) [i.e. was, but no longer is, ordinarily resident overseas] or any applicant for business resident, domiciled or incorporated in a specified territory, enhanced money laundering counter measures should be applied.

[POCA Reg 7B]

What Are High Risk Relationships?

Enhanced money laundering counter measures may include:

(a) The imposition of limits on those business relationships and transactions, whether in the form of threshold limits, prohibitions as to transactions with specified persons, or otherwise, at the written directive of the Competent Authority;

(b) Reporting more frequently as directed;

(c) Additional audit requirements as may be specified;

(d) Not relying on any assurances relating to identity records maintained, given by a third-party introducer, for the purpose of verifying the identity of the person or applicant for business.

Simplified Due Diligence

Where a business relationship or one-off transaction is determined to be low risk, a business in the regulated sector may apply simplified due diligence procedures with respect thereto, on certain conditions.

Simplified Due Diligence

The conditions for the application of simplified due diligence are –

(a) A proper **evaluation of risk** was conducted and **justifies the adoption** of simplified due diligence;

(b) The regulated has **identified and documented the risks** of money laundering and-

   i. **Implemented appropriate systems and controls to mitigate or reduce** those risks, and

   ii. Has **on-going reviews** of the risks identified and the systems and controls to reduce or mitigate them.

(c) Having regard to the guidance of the competent authority, the situation is **appropriate for simplified due diligence** to be applied. **[Reg 7A (5B)]**

Simplified Due Diligence

Simplified due diligence procedures include any one or more of the following –

a) requiring **only one form of Government-issued identification** or accepting forms of identification other than Government-issued identification;

b) accepting identification verification from third parties who have comparable obligations as concerns the prevention of money laundering;

c) collecting **only basic identification information**;

d) reliance on publicly available documents or such other documents as the competent authority may specify; or

e) such other procedures as the competent authority may specify.

[Reg 7A (5C)]

Simplified due diligence procedures must not be applied to high risk business relationships and one-off transactions. [Reg 7A (5A)]

Customer Information Update

Customer information must be **reviewed for accuracy and updated** at least once every 7 years or more frequently as warranted by the risk profile of the business relationship.

If customer information is not updated as required, the business relationship **should not proceed any further** and the regulated business **MUST make all required disclosures (STRs)** under Sec 94 to the Designated Authority. **[Reg 7(1)(d)]**

Regulatory Controls

Establish & implement programmes, policies, procedures & controls to detect, prevent & deter money laundering & terrorist financing (including controls for group companies)

POC MLP Reg. 5 (1) & (2)
TPA Sec. 18 (1) & (2)

Designate: Nominated officer at the management level for policy implementation & filing of reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)

Report: Suspicious, Threshold and Listed Entity Transactions, Authorized Disclosures and Proscribed Entity Reports

POC MLP Reg. 5 (3) & TPA Sec. 18 (3)

Establish: Risk Profiles for Operations, Risk Profiles for Business Relationships and On-going Due Diligence

POC MLP Reg. 7A & TP RE Reg. 6A

Procedures: For the proper identification of customers

(Customer Due Diligence/ Know Your Customer)

System: To evaluate the integrity and employment & financial history of employees

Programme: For training of employees on continuing basis regarding AML/CFT/CFP obligations

Arrange: Independent audit of the AML/CFT/CFP programme

Employee Integrity and Awareness

- **The success of an institution's AML/CFT/CFP programme is largely dependent on the integrity of its employees.**
- **Processes to maintain high integrity may include:**
  - A Code of Ethics
  - A "whistle blower" policy
  - Regular employee performance evaluations including AML/CFT/CFP
  - Appropriate disciplinary sanctions for breaches of policies

Training

- **Employees must be trained on a regular and continuing basis on the AML/CFT/CFP framework and its functions.**
- **This training should instruct employees on their legal responsibilities with emphasis on:**
  - employees' obligations under POCA (MLR) Regulations;
  - the TPA (RE) Regulations;
  - the UNSCRI (RE) Regulations;
  - the Advisories from Designated Authority; and
  - the Guidance issued by the Competent Authority, particularly those involving observation of proper:
    - Identification and verification procedures
    - Record-keeping procedures

Independent Audit

- An **independent review** of the institution's **AML/CFT/CFP risk** should be undertaken, at intervals directed by the Competent Authority, to ensure **the AML/CFT/CFP programme incorporates and is fully compliant with** all relevant local legislation, guidance issued by the Competent Authority, and directives of the Designated Authority and meets international best practices.

Risk-Based Approach

Risk-Based Approach

- An effective AML/CFT programme is risk-based.
- The core element of your AML/CFT regime is an adequate and effective risk assessment.
- The Competent Authority expects gaming machine operators to have a clear understanding of the ML and TF risks and vulnerabilities faced by the machine gaming sector.

Risk-Based Approach

- The purpose of the risk-based approach is not the elimination of risk. It is that regulated entities, especially those involved in (or that have customers involved in) activities that present high ML/TF risks, understand the risks that they face and have appropriate measures in place to manage these risks.

Risk-Based Approach

Implementation of a risk-based approach implies the adoption of a risk management process for dealing with money laundering and terrorist financing that involves:

i. **Recognising the existence of risks** (identifying potential AML/CFT risks)
ii. Undertaking **an assessment of these risks** (determining the impact on the organisation if the risk is realised)
iii. **Developing strategies to manage and mitigate** the risks identified.

Risk-Based Approach

Both the POC (MLP) Regs and the TP (RE) Regs require that all businesses in the regulated sector **establish risk profiles for their operations** generally considering their **products offered**, **delivery channels**, the national, regional and international **environment** in which it operates and **the size and nature of its operations.**

Risk-Based Approach

They must also **establish risk profiles** for all their **business relationships and one-off transactions** to determine the level of risk each poses and must **employ measures** commensurate with the risks to **effectively mitigate them**.

[Reg 7A (1)]

Risk-Based Approach

- The risk assessment should based on **practical, comprehensive** and **up-to-date understanding of threats**.
- Assessments should be **informed by the** country's **national risk assessment**.
- Where a higher risk scenario is identified, regulated businesses should **apply enhanced measures**.

Risk-Based Approach

This assessment of risk should be undertaken on an ongoing basis to account for new risks and changing circumstances.

The assessment process and its results should be documented.

Risk-Based Approach - Limitations

- There are circumstances which limit the application of a risk-based approach. Such limitations usually result from legal or regulatory mandates that certain actions be taken.
  - **The reporting of transactions identified as suspicious is not risk-based.**
  - **The identification and verification of the identity of customers who:**
    - **have a business relationship or**
    - **conduct transactions at or above a monetary threshold**

  are requirements which must be completed regardless of the risk-based approach

- The proliferation financing regime appears to be largely rules-based, although it seems some risk assessment may be required

Required Reporting

I'm done with all my paper work. Need help with yours?"

Regulatory Controls

Establish & implement programmes, policies, procedures & controls to detect, prevent & deter money laundering & terrorist financing (including controls for group companies)

POC MLP Reg. 5 (1) & (2) & TPA Sec. 18 (1) & (2)

Designate as Nominated Officer an employee who performs management functions for policy implementation & filing of reports

POC MLP Reg. 5 (3) TPA Sec. 18 (3)

Report: Suspicious and Listed Entity Transactions, Authorized Disclosures and Proscribed Entity Reports

Establish: Risk Profiles for Operations, Risk Profiles for Business Relationships and On-going Due Diligence

POC MLP Reg. 7A & TP RE Reg. 6A

Procedures: For the proper identification of customers

(Customer Due Diligence/Know Your Customer)

System: To evaluate the integrity and employment & financial history of employees

Programme: For training of Employees on continuing basis regarding AML/CFT/CFP obligations

Arrange: Independent audit of the AML/CFT/CFP programme

Financial Forensics

Required Reporting

Reports which must be submitted to the Designated Authority include:

- Threshold Transaction Report (POC (MLP) Regulations, Reg. 3) **- N/A to DNFIs**
- Suspicious Transaction Report (POCA Sec. 94 & 95, TPA Sec. 15 and UNSCRIA, Sec. 5(3A))
- Authorised Disclosure and Application for Consent (POCA, Sec. 100)
- International Transportation of Currency or Bearer Negotiable Instruments Report (POCA Sec. 101)
- Listed Entity Reports (TPA Sec. 16(3))
- Proscribed Entity Report (UNSCRIA, Sec. 5(3))

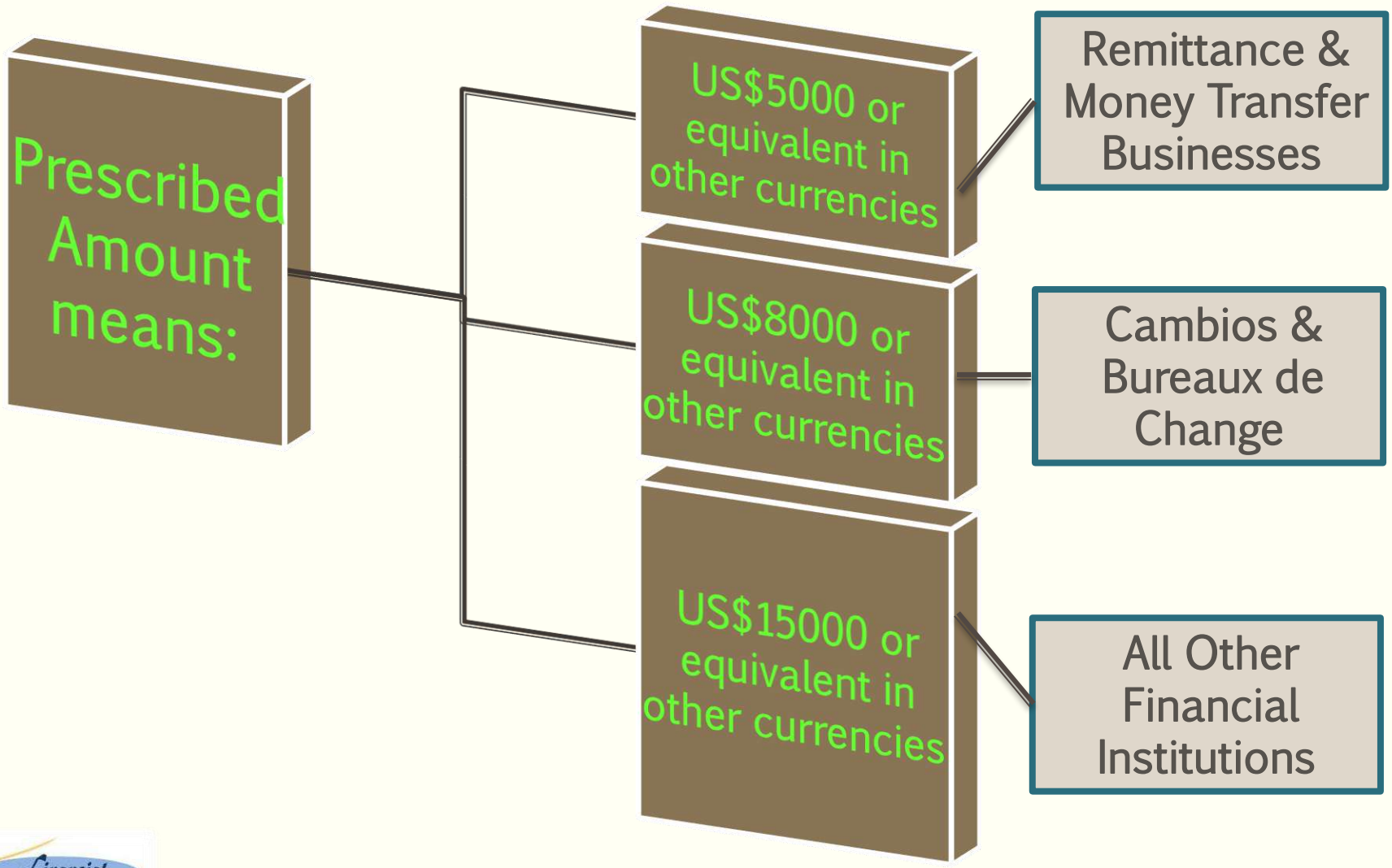
"I'm not here for committing a crime — I'm here for failing to comply with a guideline."

Required Reporting

The UNSCRI (RE) Regulations:

- made its **reporting obligations** those of the TPA (RE) Regulations for regulatory compliance; and
- for **customer identification and verification procedures,** the POC (MLP) and TPA (RE) Regulations should be relied on.

Threshold Transactions Report



Exemptions from TTR Requirements

No TTR needs to be filed for transactions carried out by:

a) Government ministries, departments or agencies;

b) Statutory bodies or authorities;

c) Companies owned or controlled by the Government or an agency of the Government;

d) Any Embassy, High Commission, Consular Office or organisations to which the Diplomatic Immunities and Privileges Act applies; or

e) Any organisation for which an order is made under section 3(2) of the Technical Assistance (Immunities and Privileges) Act.

Note however that these institutions are **NOT EXEMPT** from the **SUSPICIOUS TRANSACTION REPORTING (STR)** regime

Limit on Cash Transactions

Section 101A introduced to POCA, a J$1million limit on the payment or receipt of cash for the purchase of any property or services or for the payment or reduction of any indebtedness, accounts payable or other financial obligation.

The provision also prohibits the artificial separation of a single cash activity into a set of transactions below the prescribed limit, but which together exceeds the prescribed amount.

Limit on Cash Transactions

This limitation is not applicable to banks as defined in the Banking Services Act (**commercial banks**) or to deposit-taking institutions supervised by the Bank of Jamaica (**merchant banks and building societies**) or **cambios** licensed under the Bank of Jamaica Act.

These institutions are collectively called **"permitted persons"** in the legislation. Here the verification of the source of funds becomes critical to ensure funds are not inadvertently laundered.

Suspicious Transaction Report (POCA)

POCA refers to Suspicious Transaction Reports as "required disclosures".

A person in the regulated sector is to make a required disclosure to the Nominated Officer who will report to the Designated Authority if:

- That person knows or believes, or has reasonable grounds for knowing or believing, that another person has engaged in a transaction that could constitute or be related to money laundering; **[POCA, Sec 94 (2)(a)]**
- **AND**
- The information or matter on which the knowledge or belief is based or which gives reasonable grounds for such knowledge or belief, came to him in the course of a business in the regulated sector. **[POCA, Sec 94 (2)(b)]**

Suspicious Transaction Report (POCA)

The reports to the Designated Authority should be made by the Nominated Officer electronically using either the **POCA Suspicious Transaction**, the **POCA Suspicious Activity** or the **Authorised Disclosure** reporting options provided by the Designated Authority on the GoAML platform.

Suspicious Transaction Report (POCA)

Reports of suspicious transactions are to be made to the **Nominated Officer** as soon as reasonably practicable but **must be within 15 days after the information came to the attention of person in the regulated sector**.

Suspicious Transaction Reports **must be filed with the Designated Authority** as soon as reasonably practicable and in any event, **within 15 days of receipt by the Nominated Officer**.

Suspicious Transaction Report (POCA)

If the applicant for business is a body corporate, the reporting entity will carry out reasonable due diligence to satisfy itself about the identification of the corporate body and transaction verification.

However, if the reporting entity has reasonable grounds to suspect the involvement of money laundering and believes that doing the due diligence might alert any person of the suspicion, the regulated business should just file an STR. **[Reg 7 (4A)]**

If the regulated business is not satisfied with the outcome of the due diligence procedures, the relationship or one-off transaction should not proceed unless conducted with the permission of and in accordance with the Guidance Notes. The regulated business should also assess whether a report should be filed
[Reg 7 (4B)]

International Transportation of Currency or Bearer Negotiable Instruments Reports (Cross Border Currency Reports)

POCA Sec. 101(2) provides that:

"A person who transports or causes the **transportation of cash (including bearer-negotiable instruments**) into or out of Jamaica, **exceeding US$10,000.00** or the equivalent in any other currency or such other amount as may be prescribed, **shall … report** to the designated authority –

a) **The fact that the amount is being transported;**

b) **Particulars about the carrier;**

c) **The source of the funds;**

d) **The purpose for which the funds are being transported.**"

International Transportation of Currency or Bearer Negotiable Instruments Reports (Cross Border Currency Reports)

The **report should be made prior to the transportation** using a "Cross Border Form (CTR Form)".

Instructions on this form indicates:

A. Travellers – Persons entering or leaving Jamaica with cash or bearer negotiable instruments (BNI) shall file CTR Form with the Customs Officer in charge of the port of entry or departure.

B. Shippers and Mailers – If the BNI does not accompany the person entering or departing Jamaica, CTR Form filed on or before the date of entry, departure, mailing or shipping with the Customs Officer in charge of the port of entry or departure.

C. Persons in charge of conveyance carrying currency or BNIshall make a report on or before the date of entry, departure with the Customs Officer in charge of the port of entry or departure.

Authorised Disclosure

- Section 100 (4) defines an "authorized disclosure" as **a report**, to an authorized officer or nominated officer, **of information** or other matter **that causes the person** making the disclosure **to know or believe, or to have reasonable grounds for knowing or believing, that property is criminal property**.
- The report should be **made before doing the prohibited act**, which **requires the consent** of the Designated Authority, is done.
- However, the **disclosure may be done after** the prohibited act has been completed **where the person has a reasonable excuse** for not making the report before the act was done **and voluntarily made it** as soon as was reasonably practicable to do so.

Appropriate Consent

- Section 99 (1) of POCA **empowers the Nominated Officer to give "Appropriate Consent" for the completion of a prohibited act.**
- However, the Nominated Officer **shall not give consent** unless:
  - a **disclosure has been made to the Designated Authority** and the **Designated Authority gives consent** to the transaction

Appropriate Consent

The **application for consent must be in writing,** but the Designated Authority can give **oral notice of his consent or refusal of consent.** A **written form of the notice must be sent within 5 days** of the giving of the oral notice.

Suspicious Transaction Report (TPA)

Section 16 (3) of the Terrorism Prevention Act requires each entity to submit to the Designated Authority, all transactions, whether completed or not, which the reporting entity suspects, or has reasonable cause to suspect:

- Involve property connected with, or intended to be used in, the commission of a terrorist offence; or
- Involve, or are for the benefit of, any listed entity or terrorist group.

Suspicious Transaction Report (TPA)

Suspicious Transaction are to be reported **promptly** and in any event, **within 15 days after the suspicion** or reasonable cause for suspicion arises.

Listed Entity Report (TPA)

Every regulated entity is required to report to the Designated Authority once every four calendar months, or in response to a request made to it by the Designated Authority, whether or not it is in possession or control of any property owned or controlled by or on behalf of a listed entity. (Section 15 (3) of TPA)

Here again a Nil Report is required if there is nothing to report.

Listed Entity Report (TPA)

Effective September 2020, the reports to the Designated Authority under the Terrorism Prevention Act must now be made electronically using either the **TPA Suspicious Transaction**, the **TPA Suspicious Activity** or the **Listed Entity** reporting options provided by the Designated Authority on the GoAML platform.

Proscribed Entity Report UNSCRIA)

- Certain entities must determine on a continuing basis whether or not they are **in possession or control of assets owned or controlled by or on behalf of a person or entity proscribed** and **report the findings to the Designated Authority**
- Reports are to be submitted **every four calendar months,** or **in response to a request** made to it by the Designated Authority **[Section 5(2) & 5(3) of UNSCRIA]**.

Proscribed Entity Report UNSCRIA)

- The entities required to report are:
  - **a) Foreign companies in respect of their banking, securities, insurance, investment advice or trust business in Jamaica;**
  - **b) Financial institutions;**
  - **c) Designated non-financial institutions;**
  - **d) Any other entity designated by the Minister.**

Listed Entity Report (TPA)
Proscribed Entity Reports (UNSCRIA)

The due dates for submission of Listed Entity Reports and Proscribed Entity Reports are as follows:

SCHEDULE FOR LISTED & PROSCRIBED ENTITY REPORTS		
No.	Four Months Period	Due Date (on or before)
1	January - April	May 31
2	May - August	September 30
3	September - December	January 31

Record Keeping and Retention

Financial Forensics

Record Retention

Records **must be kept** of –

i. **each transaction and**

ii. **all correspondence, and analysis undertaken, in relation to each transaction and business relationship,**

in such a manner and form that facilitates the reconstruction of each transactions and the **provision of information to the Designated Authority or Competent Authority no later than 7 days after the request.**

Record Retention

A new section 137A was added to POCA introducing a requirement for the supervisory, competent and designated authorities to **keep statistical records**. This section also provides for the disclosure of this information to entities specified within the section.

Record Retention

For electronic transactions, regulated entities must be mindful of the provisions of the Electronic Transactions Act which treats with:

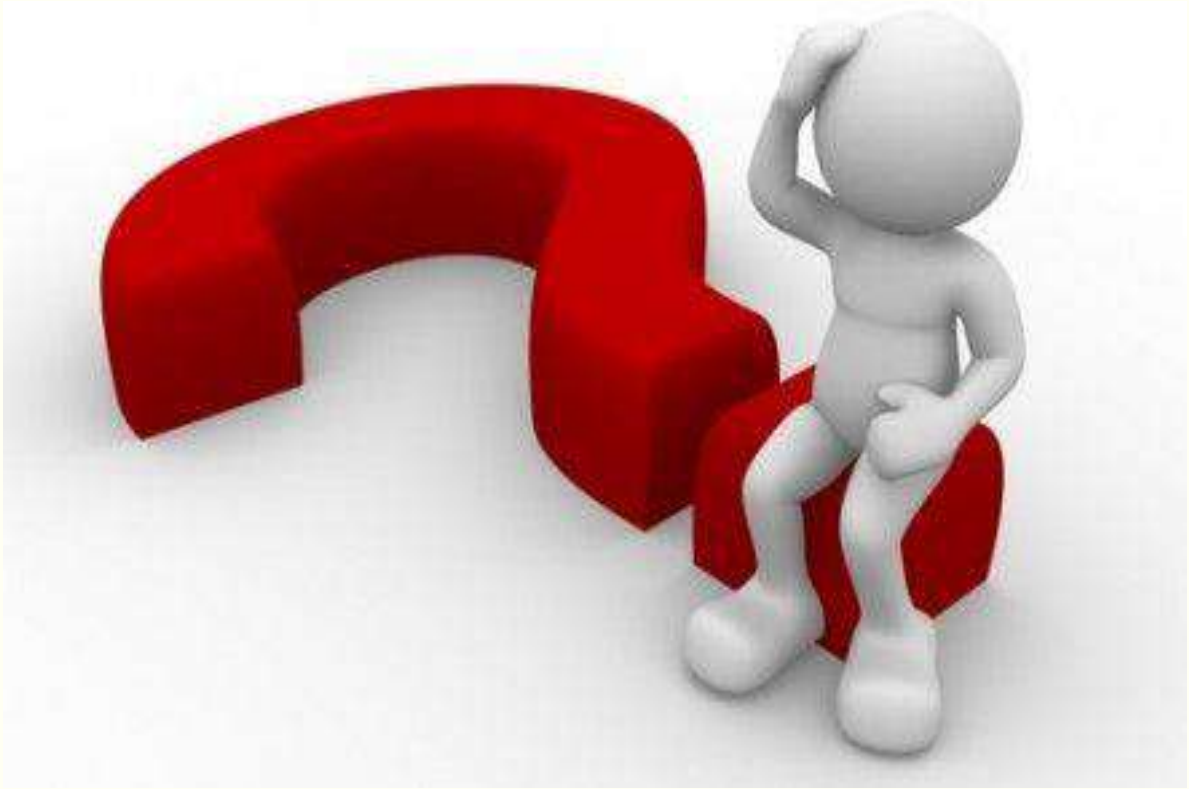
a) validity of electronic transactions (section 6);
b) requirements to give information in writing (section 7);
c) requirements for signature (section 8);
d) requirements for attestation, etc (section 9);
e) requirements to produce a document for inspection or in original form (section 10);
f) requirements for keeping information (section 11);
g) admissibility and evidential weight of information in electronic form (section 12).


RA F K IS A L N RI E,
NE L I G I S T R

Important Note

It is impossible to cover all you need to know in a session like this, so it is extremely important that you **read the relevant legislation** and **read the Competent Authority's Guidance Notes** and keep abreast of amendments and changes to them. Also try to keep pace with industry best practices and developing trends in the AML/CFT/CFP arena.

Questions



Thank You for your attention

Remember you must complete the Knowledge Test.
Pass mark is 75%.

Presenter:

Christine A. Chambers, CAMS, FCA, M.Sc.
AML/CFT Specialist & Forensics Consultant
Telephone: +1 876 381-4082
Email: finforensics@gmail.com