The Proceeds of Crime & Anti-Money Laundering Seminar for Gaming Lounge Operators

Betting Gaming & Lotteries Commission

Laurie Wiggan

April 26 & 28, 2016

What we will discuss

- The steps to be taken to develop your AML Compliance Programme

Background

- The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions.

Role of FATF

- *Global Standards*
  - Guidance & Best Practices
  - 40+ Recommendations

- *Mutual Evaluation* – ensure members are implementing the necessary measures
- *Typologies*

- FATF Decision making Body – FATF Plenary

FATF Associate Members

Caribbean Financial Action Task Force (CFATF)

www.cfatfgafic.org

Financial Action Task Force of Latin America (GAFILAT)

www.gafilat.org

DNFIs AML Requirements

Four main components:

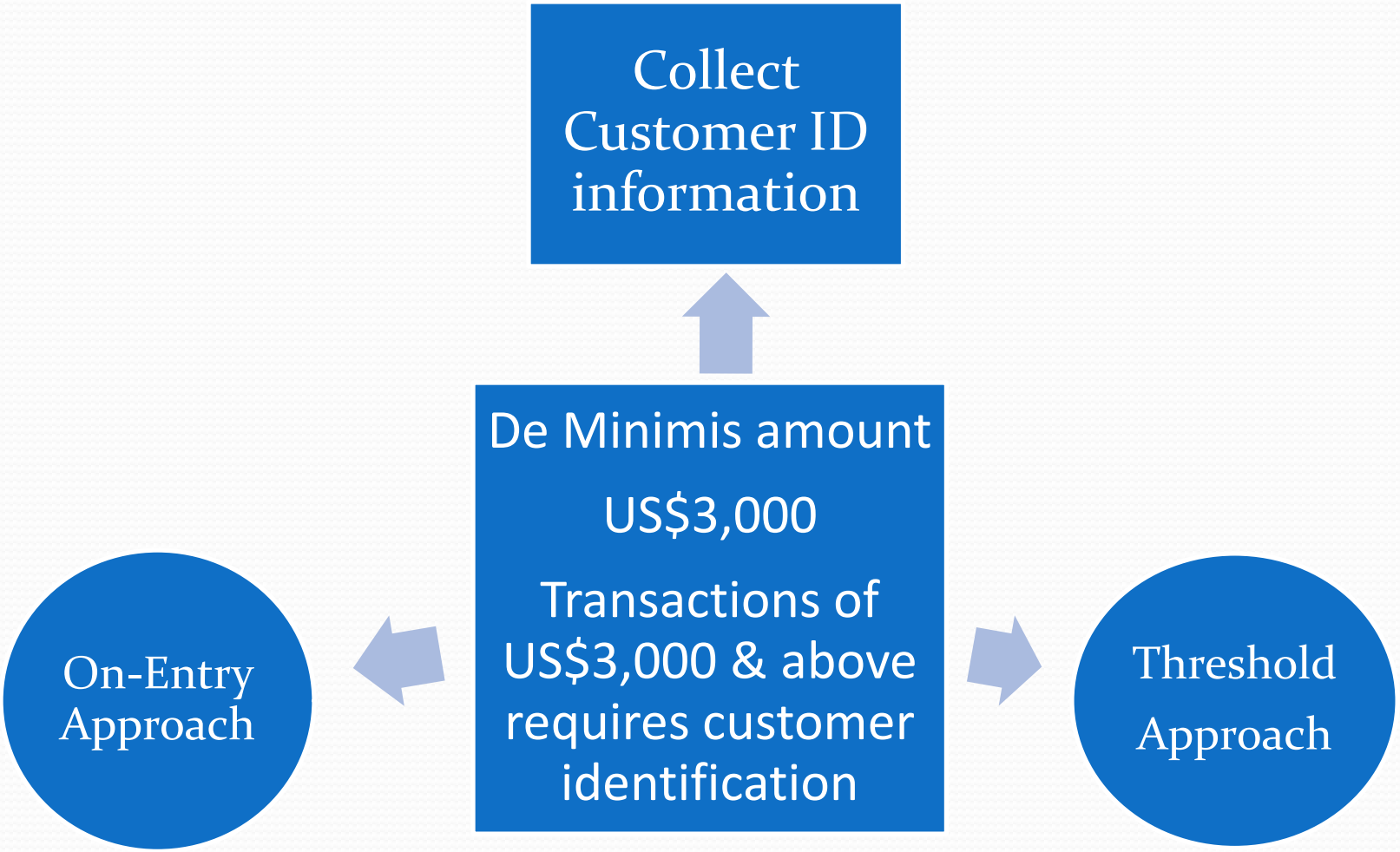
- Designation of a Nominated Officer
- The Programme – policies, procedures & control
- Training
- Independent Audit conducted by a third party

The AML Programme

- Customer Due Diligence (CDD)/Know your Customer (KYC)
- Transaction Monitoring
- Record Keeping
- Training

The AML Programme

- Revolves around the transaction requirement:



Which Approach should I choose?

On-Entry Approach

- As part of the routine registration process customer information is collected and a copy of ID is taken before customer game.
- Consider appropriate signage
- Trigger/Tracker system for alerts.

Threshold Approach

- Customer information is collected and a copy of ID taken before or immediately after the customer pays US$3,000 or more (applicable to any one transaction and cumulatively within 24 hours).
- Consider appropriate signage.
- Trigger/Tracker system for alerts.

Scenario
Lounges in Hotels & Tourist Areas

- Tourists do not always walk with IDs
  - *Signage at entrance re ID required for gaming US$3,000 or more.*
  - *Pamphlet/Notice in Guest Directory & Guest Package as well as notice to tour operators.*
- Withdrawal/Jackpot/Winnings payout – implement a payout slip which could be used for CDD.

- *Implement risk management controls to guard against fraudulent activities.*

Scenario
Lounges in independent locations

- Customer information obtained at registration & copy ID taken – monitor if the customer is categorized as high risk, conduct Enhanced Due Diligence.

- If On-entry registration does not exist, consider obtaining customer information at the point of withdrawal/cash-out.

- Withdrawal/Jackpot/Winnings payout – consider **implementing a payout slip** which could be used for CDD.

***Implement risk management controls to guard against fraudulent activities.*

Customer Due Diligence (CDD)

Three key components of CDD:

- Customer Information
- A transaction monitoring programme
- An enhanced Customer Due Diligence

Customer Information

- Government issued ID
- *Record the ID type, number, expiration date, country of issue*
  - First & Last Name
  - Permanent Address *(obtain verbally if not on Government issued ID)*
  - Date and Place of Birth
  - Nationality
- Copy of ID to be taken – in any one or a combination of electronic and hard copy

Customer Information

Implement controls for protecting the privacy of customer's personal and sensitive information

Privacy embedded into the design & architecture of your IT system.

Recap: Customer Due Diligence

Who must you undertake CDD on:
A customer
A visitor
A tourist
Regular or occasional

When you do it:
When a customer spends US$3000 or more during any period of 24 hours.
AND
When a customer withdraw funds – US$3000 or more

How do you do CDD:
- *The types of CDD*
- *CDD on individuals*
- *Verification of identity information*

The types of CDD:
- *Standard CDD*
- *Enhanced CDD/Enhanced Due Diligence (additional obligation for high risk customers: obtain verbally source of funds)*

CDD on Individuals: Obtain from customer personal information
Verification: Obtain a copy of the identification

Transaction Monitoring Programme

- ✓ Limit on Cash transactions (pay or receive cash)
  - The Proceeds of Crime (Amendment) Act 2013 Section 101A places a limit on cash transactions of J$1 million or its equivalent in any other currency.
- ✓ Create a risk profile of customers – High risk and low risk
- ✓ Implement procedures to monitor and record transactions at all premises and in particular high risk customers including PEPs.
- ✓ IT Monitoring system will help in identifying unusual or suspicious activity.

Enhanced Due Diligence

- Monitoring of high risk customers including PEPs falls under the Enhanced Due Diligence process:
- Additional obligation is to obtain source of funds (verbally) and monitor for example via a special report to determine if there is a money laundering risk.

- **There is no Threshold Transaction Reporting requirement**.

Suspicious Transaction Reporting

- All Suspicious Transaction Reports (STRs) are to be completed by the Nominated Officer and submitted to the Chief Technical Director, Financial Investigation Division.

- If an STR is filed on a particular customer and the customer continues to game, the operator is required to continuously file an STR.

Training & Awareness

- Nominated Officer must be trained and knowledgeable to provide relevant employees with guidance.
- Training at orientation and annual refresher training
- Training material could include:
  - How to obtain customer information and how to verify the identity of our customers;
  - How to identify fraudulent IDs, credit/debit cards frauds;
  - How to look out for suspicious activity and how to make a report to the Nominated Officer

Record Keeping

- Retention for 7 years:
  - customer identification
  - Records of each deposit & withdrawal of funds including transmittal of funds
  - Other documents and records as required by the Regulator
- Any one or a combination of medium: original, photocopies, computerised, electronic, scanned

Questions