ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය | நிதியியல் உளவறிதற் பிரிவு | Financial Intelligence Unit

Guidelines – 02/2018

18 April 2018

Ref: 037/08/001/0005/017

To: CEO / General Manager

Dear Sir / Madam

Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Casinos and Gambling Houses, No. 2 of 2018

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Designated Non-Finance Business (Customer Due Diligence) Rules No. 1 of 2018.

Yours faithfully

D M Rupasinghe
Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක 30, ජනාධිපති මාවත, තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව
14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை த. பெ. இல. 590, கொழும்பு 01, இலங்கை
Level 14, No. 30, Janadhipathi Mawatha, P. O. Box. 590, Colombo 01, Sri Lanka.
94 11 2477125 / 509
94 11 2477692
fiu@cbsl.lk
www.fiusrilanka.gov.lk

Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Casinos and Gambling Houses, No. 2 of 2018

PART I

Introduction

1. The Financial Intelligence Unit (FIU) acting within the powers vested with it under the Financial Transactions Reporting Act, No. 6 of 2006 (hereinafter referred to as "FTRA"), issued the Designated Non-Finance Business (Customer Due Diligence) Rules No. 1 of 2018 (hereinafter referred to as "CDD Rules") by Gazette Extraordinary No 2053/20 dated 2018.01.10 which is applicable to institutions carrying out non-financial businesses and professions.
2. As described in the CDD Rules these Guidelines shall apply to casinos, gambling houses or conducting of a lottery, including to a person who carries on such a business through the internet when their customers engage in financial transactions (hereinafter referred to as "Institution(s)").
3. These Guidelines are issued for the purpose of identifying, assessing and managing Money Laundering (ML) and Terrorist Financing (TF) risks.
4. For the purpose of these Guidelines, unless the context otherwise requires:

   AML/CFT means Anti-Money Laundering and/or Countering the Financing of Terrorism as recommended by the Financial Action Task Force;

   CDD means Customer Due Diligence;

   EFT means Electronic Fund Transfer;

   FATF means Financial Action Task Force, the global policy setter against money laundering and financing of terrorism

   FIU means the Financial Intelligence Unit which is designated for the purposes of the Financial Transactions Reporting Act, No 6 of 2006 [Gazette (Extraordinary) No: 1437/24 dated 23.03.2006], and charged with the implementation and administration of the provisions of said Act;

ML means the offence of money laundering, which was penalized in terms of Section 3 of the Prevention of Money Laundering Act, No 5 of 2006;

ML/TF means money laundering and or terrorist financing;

PEPs means Politically Exposed Persons, including individuals in Sri Lanka or abroad who are, or have been, entrusted with prominent public functions. For example: heads of state or of government, politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. The family members and close associates of PEPs are also considered to be PEPs by virtue of business relationships that involve reputational risks similar to those of the relevant PEPs themselves. This is not intended to cover middle ranking or more junior officials in the foregoing categories;

STRs means Suspicious Transaction Reports filed in terms of Section 7 of the Financial Transactions Reporting Act, No 6 of 2006;

TF means the offence of terrorist financing, which was penalized in terms of Section 3 of the Convention on the Suppression of Terrorist Financing Act, No 25 of 2005;

UNSCR means the United Nations Security Council Resolutions.

PART II

Compliance

Compliance Officer

5. Each Institution is required to appoint a Compliance Officer. The appointed officer should be responsible for the implementation of the Institutions' AML/CFT compliance requirements. The Compliance Officer should have the authority and the resources necessary to discharge his or her responsibilities effectively.
6. According to the management structure of the Institution, the Compliance Officer should report on regular basis to the board of directors or senior management or to the owner or

chief executive officer of the Institution. The Compliance Officer should be from the senior management level and have direct access to higher management or the board of directors.

7. For consistency and ongoing attention to the AML/CFT requirements, the Compliance Officer may choose to delegate certain duties to other employees of the Institution. However, where such a delegation is made, the Compliance Officer remains responsible for the implementation of the AML/CFT compliance requirement.

AML/CFT Compliance Policies and Procedures

8. Each Institution must establish written policies and procedures to assess ML/TF risks. These policies and procedures must be implemented in an effective manner to prevent, detect and remedy instances of non-compliance. It is important that the policies and procedures are communicated, understood and adhered in a timely manner within the Institution. These policies and procedures should be communicated to those who work in the areas relating to customer interactions.
9. Each Institution's AML/CFT compliance policies and procedures must include an assessment of risks related to ML/ TF. The assessment must be conducted in a manner that is appropriate to the nature of the Institution's business. This ML/TF risk assessment must be conducted notwithstanding any existing policies and procedures on customer identification, record keeping and reporting requirements.
10. The extent and level of detail of each Institution's AML/CFT compliance policies and procedures will depend on the specific needs and the complexity of the Institution, as well as the Institution's assessed risk to ML/TF.
11. The Institution's AML/CFT compliance policies and procedures must be approved by senior management and/or board of directors of the Institution. The AML/CFT compliance policies and procedures must include, at a minimum, ML/TF risk assessment and risk mitigation measures, customer identification and verification, record keeping, submission of mandatory reports to the FIU and ensuring independent audits of the Institutions' compliance policies and procedures. For example:

    (a) In the case of reporting obligations relating to any suspicion of TF, the compliance policies and procedures of the Institution should include the screening

of customers against UNSCR and other lists which are available on the FIU website (http://fiusrilanka.gov.lk) and elsewhere.

(b) Institutions should apply an enhanced level of caution when dealing with transactions involving countries or territories that have not yet established adequate AML/CFT measures that consistent with international standards. Institutions may refer the FATF website (http://fatf-gafi.org) and other sources for this information.

12. Board of directors and senior management are required to understand the statutory duties on AML/CFT compliance vested upon the board of directors, the staff and the Institution. Senior management and the board of directors are ultimately responsible for making decisions related to policies, procedures and processes that mitigate and manage the risks of ML/TF within the business.
13. The Institution should have a screening policy when hiring employees to ensure high standards.

Compliance with United Nations Security Council Resolutions

14. The Institution should cross-check whether any customer or beneficiary appears on any designated list issued in compliance with United Nations Act, No. 45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing (UNSCRs 1267 , 1373, 1718, 1540) and any other subsequent Resolutions.
15. It is required to immediately freeze funds, financial assets or economic resources of individuals and entities who are designated by the United Nations Security Council based on such person's/entity's connections with terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing. The Institution should have measures in place to identify and immediately freeze funds, financial assets or economic resources, of such designated persons and entities.
16. Upon freezing or lifting of such freezing of funds, other financial assets and economic resources of designated individuals and entities, or upon the occurrence of an attempted transaction by or for designated individuals or entities, Institutions shall, not later than 24

hours from the time of finding out such customer, inform to the Competent Authority with a copy to the FIU.

17. The Institution should ensure that no funds, financial assets or economic resources are made available to or for the benefit of such designated persons or entities or their beneficiaries.

Risk-Based Approach

18. A risk-based approach is a process that allows the Institution to identify, assess the risks of ML/TF, to develop controls to mitigate the identified ML/TF risks and ongoing monitoring of those controls. Each Institution must use their own judgment, knowledge and expertise to develop an appropriate risk-based approach for their particular organization, structure and business activities.
19. In the context of ML/TF, the risk-based approach is a process that encompasses the following steps:

    (A)Identify the ML/TF risk;

    (B) Assess the ML/TF risks;

    (C) Design and implement controls to manage and mitigate the ML/TF risks;

    (D)Monitor and improve the effective operations of the risk based controls.

(A) Identify the ML/TF Risk

20. The Institution must be aware of ML/ TF risks inherent to the business activities. As a first step of the risk-based approach, the Institution should identify the ML/TF related risks that may arise from customers, countries or geographical areas and products, services, transactions or delivery channels, as well as from proposed innovations thereof. A second step may be to identify all entry and exit points for funds used by customers. Such entry and exit points are potentially useful to a money launderer during the placement and integration stages of the money laundering process.

21. Each institution must identify the ML/TF risks that may be associated with the products and services that are offered by the Institution based on their utility for ML/TF. For example, any financial service offered by an Institution that converts the form of funds or ownership of funds is potentially useful to a money launderer during the layering phase of the money laundering process such as a person who exchanged Rupees 1,000,000 for chips, and passes the chips to another person has effectively transferred ownership. If that person then exchange the chips for a casino cheques the form has also been converted.

(B) Assess the ML/TF Risks

22. A risk assessment is an analysis of potential threats and vulnerabilities of ML/ TF to which the Institution is exposed. The complexity of the assessment depends on the nature, size and ML/TF risks faced by the Institution.
23. When conducting a risk assessment, the Institution must consider and document the following factors:

    (a) types of customers and customer relationships;

    (b) types of products and services and the delivery channels through which they are offered;

    (c) the geographic origins and locations of the customers;

    (d) other factors related to the Institution's business activities;

    (e) whether the customer's name is appearing in any UNSCR designated list.
24. The risk assessment requires detailed knowledge of business operations and sound judgment exercised by the assessors so the risks for ML/TF can be determined according to each individual factor as well as combinations of factors. The risk assessment will continuously change over time as the various risk factors evolve.

(C) Design and Implement Controls to Manage and Mitigate the ML/TF Risks

25. Risk mitigation is about implementing controls to address risk factors that are the source of the risk (i.e. threats, vulnerabilities) in a timely manner which is tolerable to the Institution is achieved. Controls should be in the form of written policies and procedures.
26. The Institution may develop and implement the following different types of mitigation measures through the Institution's compliance policies, procedures and internal controls:

(a) reducing or avoiding the risk; for example, if a casino identifies and assesses as unacceptably risky wire transfers from jurisdictions that are known to have ineffective AML/CFT controls or high levels of corruption, then the risk can be reduced by putting a cap on the size and frequency of such transfers for individual customers or the risk can be eliminated by refusing to accept such transfers.

(b) controlling the risk; for example, building on the wire transfer example, the casino can apply enhanced due diligence to verify the legitimate source of funds and/or require that any winnings or cash-outs be returned to the customer exclusively through a wire transfer to the account from which the original wire transfer was received (**Appendix 1** contains sample EFT controls). The casino can also apply enhanced monitoring to the gambling activities of the customer to ensure the absence of money laundering indicators.

(c) transferring the risk; for example, again, building on the wire transfer example, the risk of funding accounts in some jurisdictions is sometimes transferred to licensed junket operators, which provide funds transfer services to their customers and with whom the casino may develop a relationship, subject to proper controls.

(D) Monitor and Improve the Effective Operations of the Risk Based Controls

27. The effective management of risk is a continuous and dynamic process. The Institution should ensure that the process of managing the risks of ML/TF is subject to regular review and is updated as new or emerging risks are identified, whether caused by changes in the scale or nature of operations, new products, new services, new customer types, etc.

Development of Training and Awareness Programmes

28. The Institution is required to provide training on AML/CFT compliance to board of directors, senior management, employees, agents or any other individuals authorized to act on behalf of the Institution.
29. Such training should consist of raising awareness of the internal policies and procedures for preventing ML/TF. The training programme should provide a clear understanding of

Institution's AML/CFT compliance policies and procedures and the related individual's responsibilities.

PART III

Customer Due Diligence

Identification and Verification of Customer and Beneficial Owners

30. Each Institution is required to conduct CDD on customers and beneficial owners, including occasional and one-off customers, when they engage in inward and outward financial transactions that aggregate in either direction to the equivalent of United States Dollars 3,000 or more, regardless of the actual currency of the transaction(s), in a single business day. For this purpose, a "business day" is defined as any continuous 24-hour period that an Institution uses for keeping its business books and records. Institutions may use only one definition of a "business day" and must consistently apply the definition across all customers and customer activity when aggregating transactions to determine CDD requirements. For this purpose, a "financial transaction" includes all inward transfers of funds from the customer to Institution and all outward transfers of funds from Institution to the customer. Such transfers may include, but are not limited to, the purchase or sale of gambling chips or any other gambling instrument, purchase of casino cheques, or cashing of customer cheques, purchase or redemption of lottery tickets, inbound and outbound wire transfers, purchase and redemption of "ticket-in/ticket-out" documents. For example, if a casino patron buys the equivalent of United States Dollars 1,000 in casino chips using Sri Lankan Rupees and subsequently redeems the equivalent of United States Dollars 4,000 in casino chips for Sri Lankan Rupees then that customer does not need to be identified prior to completing the purchase. However, it is required to identify the customer prior to completing the redemption in accordance with these guidelines described herein. Likewise, a customer purchasing the equivalent of United States Dollars 3,000 in casino chips the Institution is required to conduct CDD prior to completing the purchase.

31. Due to the difficulties inherent in aggregating the value of a customer's transactions on a business day, an Institution may wish to identify all customers as a condition of extending services of the Institution (perhaps through the issuance of player/membership cards).
32. If the Institution cannot satisfactorily apply due diligence measures in relation to a customer and/or beneficial owner, the Institution shall not carry out a transaction for that customer. Further, the Institution may also consider submitting an STR to the FIU.
33. If the actions of a customer appear as designed to deliberately avoid CDD requirements, then the Institution should consider submitting an STR to the FIU. For example, a customer who purchases the equivalent of United States Dollars 2,000 in chips just prior to the expiration of a business day and then purchases the same amount just after commencement of a new business day, without making meaningful wagers in the interim period, may be structuring his transactions to avoid CDD requirements.
34. Customers and beneficial owners that are identified as high risk should be subject to enhanced due diligence measures such as additional scrutiny and verification of identification information and source of funds.

High Risk Customers/Transactions

35. There are customers / types of transactions / products which may pose higher ML/TF risk to the Institution. In such a situation, the Institution is required to take additional measures. As examples:
    (a) any customer who has links with countries which do not or which insufficiently comply with the recommendations of the FATF (For High Risk and Non-Cooperative Jurisdictions please refer to FAFT website; (http://fatf-gafi.org);
    (b) any customer linked with a country that has been identified by a national authority as a jurisdiction of concern for drug trafficking, human trafficking, money laundering, terrorism or illicit financing;
    (c) any country that has been identified by a reputable organization as having high levels of public corruption;
    (d) any customer who conducts complex or unusual transactions, (whether completed or not), unusual patterns of transactions for the customer profile, transactions that match

patterns associated with unlawful activity, and transactions which have no apparent lawful purpose;

(e) domestic and foreign PEPs, to include their family members and close associates;

(f) any customer or transaction, product type that the Institution has identified as posing a higher risk to the business. For example, gambling games that allow customers to play opposite sides of a bet (e.g. odd vs even numbers in roulette), such that the net bet is very low risk and the pure intention may not be to gamble, are at higher risk of ML. In this case, an unusually low "hold percentage" of a game might be an indicator of activity that is intended to place funds with little or no risk;

(g) customers that have a sudden unexplained increase in their gambling activity or method of funding their gambling activity are higher risk.

Specific Customer Due Diligence Requirements

Casinos

36. The CDD requirement shall be carried out at all entry or exit points for funds, including the following;

    (a) when customers exchange cash for gambling chips and/or playing chips at the gaming tables;

    (b) when customers exchange cash and/or vouchers for chip warrants at the cashier counters;

    (c) when customers request cheques or wire transfers for payments of winnings and/or capital; or

    (d) when customers use their membership cards or temporary or casual cards (if any) in respect of the e-cash out facility at the cashier counters or cash dispenser machines or gaming tables.

37. In relation to bank intermediated transactions, CDD shall be conducted prior to customers being allowed to use the funds.

38. The casino is also required to carry out CDD on junket operators and its customers.

Gambling Houses

39. Gambling houses are required to obtain and check the accuracy of the following information;
    (a) ticket number;
    (b) registration number and address of the outlet where the winning ticket was purchased; and
    (c) winning amount.
40. Gambling houses are required to conduct CDD on the third party when the winner requesting for payment to a third-party account.

Identification of Third Parties

41 The Institution must take reasonable measures to determine whether the customer is acting on behalf of a third party, where the customer is an agent of the third party who is the beneficiary and/or who is providing the funds for the transaction. In cases where a third party is involved, the Institution must obtain information on the identity of the third party and their relationship with the customer, for CDD purposes.

PART IV

Reporting

Duty of Submitting Suspicious Transactions Reports

42 In making the assessment to submit an STR, an Institution may refer to the list of red flags as mentioned in **Appendix II**. Industry-specific indicators would also help the Institution to better identify suspicious transactions whether completed or attempted. Some examples of ML using casinos and gambling houses are given in **Appendix III**.

43 Each Institution must pay attention to attempted suspicious transactions. If a customer attempts to conduct a transaction, but for whatever reason that transaction is not completed, and if the Institution determines that the attempted transaction is suspicious, the Institution must report it to the FIU.

44 The Institution shall submit STRs using the format as prescribed in Suspicious Transactions (Format) Regulations of 2017, Gazette (Extraordinary) No: 2015/56 dated April 21, 2017 (Schedule V).

45 The Compliance Officer should maintain a register of STRs.

Reporting of Cash and Electronic Transactions

46 Every Institution is required to adhere to the requirements stipulated in Financial Transactions Reporting Regulations No. 1 of 2008, Gazette (Extraordinary) No: 1555/9 dated June 25, 2008.

PART V

Record Keeping

47 The Institution shall take appropriate steps to put in place and maintain a system for record keeping as stipulated in the FTRA, which allows data to be retrieved easily and quickly whenever required, or when requested by the FIU.

PART V1

Penalties for Non-Compliance

48 Failure to comply with the legislative requirements shall lead to penalties. In addition, there may be other actions including regulatory and disciplinary measures against the Institution.

Issued on 18 April 2018

Appendix I

Sample casino internal controls for Electronic Fund Transfers

- Electronic Fund Transfers (to include wire transfers) will not be accepted, or will be immediately reversed, from any jurisdiction that is identified by the FATF as a High Risk and Non-Cooperative Jurisdiction or that is believed by the Institution to be a country with unacceptable jurisdictional risk.
- Electronic Fund Transfers may not be redeemed for cash, neither in whole nor in part, and may only be used to fund gambling and entertainment activities offered by the casino to the customer.
- Unused balances from Electronic Fund Transfers, including winnings from gambling activities funded by such transfers to the extent that they do not exceed the size of the transfer, must be returned to the customer via the identical channel and to the identical account from which it was received. No other type of redemption (e.g. cash, cheque, third party transfer) is permissible.

Appendix II

Anti-Money Laundering/Countering Financing of Terrorism suspicious indicators (red flags) for casinos and gambling houses

- Customers purchasing and redeeming chips or depositing and withdrawing funds with no gambling or minimal gambling;
- Customers requesting multiple payments of winnings and capital to the account of a third party;
- Multiple players requesting for payments to the same beneficiary;
- Gamblers who appear to be cooperating by placing offsetting bets against each other;
- Structuring the purchase or redemption of chips or other instruments to avoid trigging CDD requirements or other reporting requirements (whether real or perceived);

- "Bill stuffing" by feeding currency to gambling devices that accept cash and then cashing out (e.g. by receiving a TITO ticket or other such instrument) with minimal or no actual gambling;
- Customers befriending/attempting to befriend casino employees;
- Dramatic or rapid increase in size and frequency of transactions for an established customer;
- Gambling activity that is inconsistent with the financial situation and/or known occupation of the person gambling;
- Purchase of winning tickets from punters (gamblers);
- Purchasing of winning jackpots or winning lottery tickets at a premium;
- Exchanging large amount of small denomination bank notes for larger denominations without gambling;
- Frequent claims for winning jackpots;
- Customers watching/hanging around jackpots sites but not participate in gambling;
- Customers passing significant values in chips or TITO tickets to other customers;
- Loaning funds for gambling to customers with repayment of the funds being a discounted amount;
- Gambling patterns that appear designed to wager large sums at low risk over a period time, thus achieving a predictable low rate of loss prior to cashing out.
- Customers reluctant to provide information to complete CDD requirements, or that provide doubtful or unverifiable identification information, or who in any other way appear to deliberately impede the Institution's CDD process.

Appendix III

Examples of ML using casinos and gambling houses –

Cases taken from Financial Action Task Force 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 totaling AUD 890000. 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
Instruments: Cash, cheques

During police investigations into armed robberies, it came to light that another individual has 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 the system.

Case 3 – Overseas nationals purchase winning jackpots with illegal proceeds

Offence: Drug trafficking & money laundering
Technique: Buying winning lottery tickets
Mechanism: 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 AUD 1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of funds used to buy winning jackpots was suspected to be from illegal means. This matter was referred to partner agencies for further investigation.

***Appendices I-III include contents from publicly available AML/CFT resources**