Financial Intelligence Centre
Republic of Namibia

PO Box 2882
Windhoek
Namibia

Phone: + 264 61 283 5286
Fax: + 264 61 283 5918
Helpdesk@fic.na

GUIDANCE NOTE NO. 02 OF 2023

GUIDANCE ON RISK MANAGEMENT, CUSTOMER DUE DILLIGENCE, DETECTING AND REPORTING SUSPICIONS: CASINOS AND ONLINE GAMBLING SERVICE PROVIDERS

First Issued: 14 April 2023

Table of Contents

DEFINITIONS AND ABBREVIATIONS

“Accountable Institution (AI)” means a person or entity listed in Schedule 1 of the Act;

“Act” refers to the Gaming and Entertainment Control Act, 2018 (The Act);

“Business relationship” means an arrangement between a client and an accountable or reporting institution for the purpose of concluding transactions on a regular basis;

“Casino”, in relation to licensed premises, means a room in or a part of the premises in which games are played or gambling machines are kept and played (The Act);

“Casino licence” means a casino licence issued under section 34 of the Act;

“CDD” means Customer Due Diligence;

“Client and Customer” have their ordinary meaning and are used interchangeably herein;

“Customer Due Diligence” (CDD) means a process which involves establishing the identity of a client, the identity of the client’s beneficial owners in respect of legal persons and monitoring all transactions of the client against the client’s profile;

“Enhanced Due Diligence” (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and includes, amongst others, taking measures as prescribed by the Centre to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF;

“Establish Identity” means a two-tier process consisting of *ascertainment or collecting* of certain identification information, and *verification* of some of the information against reliable documentation or information;

"FATF" means the Financial Action Task Force;

“FIA” refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

“FIC” means the Financial Intelligence Centre;

"Gambling" means a form of gambling, including a game or the casting of a lot in which luck is an element and by which a prize may be won, whether or not an element of knowledge or skill is included in the process of determining the winner, as per the Act;

"Gambling activity" means an activity that meets the requirements of section 29 of the Act;

"Gambling game" means an activity that meets the requirements of section 31 of the Act;

"Gambling house", in relation to a licensed premise, means a room in, or a part of, the premise in which a gambling machine is kept and played, as per the Act;

"Gambling house licence" means a gambling house licence issued under section 35 of the Act;

"Gambling machine", the Act described such to include a totalizator and mechanical device, electrical device, video, electronic device, electro-mechanical device or other devices, contrivance, machine, device, equipment or software, other than an amusement machine, that is available to be played or operated on payment of a consideration and:

- may entitle the player or operator to a pay-out or deliver a pay-out to the player or operator as a result of playing or operating the gambling machine; or
- is used, or is designed to be used, in determining the result of a gambling activity;

"ML" means Money Laundering;

"Online game" means a gambling game prescribed as an online game under section 73 of the Act which is played or made available to be played through the use of communication technology that allows a person utilising money, electronic checks, electronic transfers of money, credit cards, debit cards or any other instruments, to transmit to a computer information to assist in the placing of a bet or wager and other corresponding information related to the display of the game, game outcomes or other similar information, but excludes a bet or wager placed through communication technology with a bookmaker or an operator of a totalizator;

"Online provider" means a person to whom an online game licence has been issued, as per the Act. Herein, the scope covers those issued with gambling licenses as Reporting Institutions[1] and chose to use online services as a means to avail their services, thus exposing the country to ML/TF/PF risks. For ease of reference, such online providers are referred to as Online Gambling Service Providers (OGSPs) or Online Operators;

"PEPs" means Political Exposed Persons (See FIC Guidance Note 01 of 2019);

[1] Item 3, Schedule 3 of the FIA.

“PF” means proliferation financing;

“Records” means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device;

“Regulations” refer to the FIA Regulations unless otherwise specified;

“Single Transaction” means a transaction other than a transaction concluded in the course of a business relationship;

“SAR” refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

“SNMA” refers to a Sanction Name Match Activity report. When an actual or potential sanctions match is detected, institutions should file a SNMA with the FIC. With effect from 1 April 2023, such should no longer be reported through SARs, nor STRs;

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the FIA;

“TF” means Terrorist Financing;

“TPFA” refers to Terrorist & Proliferation Financing Activity report. Reporting any other Activity (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF;

“TPFT” Terrorist & Proliferation Financing Transaction report. Used for reporting any other transaction (actual transaction) which may point to, or be linked to potential terrorism, TF or PF;

“Transaction” means a transaction concluded between a client and an accountable or reporting institution in accordance with the type of business carried on by that institution, and includes attempted transactions.

1. BACKGROUND

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (The FIA). This document avails guidance on effective implementation of a risk based internal control system, focusing on customer diligence as well as detecting and reporting of suspicions as per the FIA. Part A focuses on carrying out risk assessments at institutional level and the overall Risk Based Approach (RBA) while Part B breaks down the elements of an effective RBA framework. The guidance herein is directed to Casinos and Online Gambling Service Providers (OGSPs)/Online Operators.

Item 5 of Schedule 1 of the FIA lists persons that carries on the business of casinos as Accountable Institutions. Such is limited to entities or persons issued with a valid Casino license by the Casino Board, as per section 34 of the Gaming and Entertainment Control Act, 2018 (The Act). Item 3 of Schedule 3 equally lists persons who carries on the business of gambling houses, totalisators/totalizators or bookmakers as Reporting Institutions, regardless of the delivery channels of such services[2]. OGSPs or Online Operators fall within the general definition of such Reporting Institutions.

It should be noted that the Exchange Control Rulings and Regulations, at present, prohibit foreign OGSPs from availing such services to the domestic market. Local institutions (e.g banks) are expected to ensure compliance with such prohibition through restricting delivery channels which may enable remittances to such foreign service providers or undue accessibility to such services. At the time of issuing this guidance, regulatory considerations are ongoing to align the domestic framework to international developments in this regard.

It is common cause that services offered by Casinos and OGSPs have been subject to Money Laundering (ML) abuse domestically. Internationally, there are trends and typologies which suggest such abuse to advance Terrorism and Proliferation Financing (TF/PF) activities. To help mitigate ML/TF/PF risks, the Financial Intelligence Centre (FIC) issues this Guidance to help

[2] The availing of such services via an online platform is merely a chosen method of delivery. The principal regulated and designated service remains the same.

Casinos and OGSPs implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures.

2. COMMENCEMENT

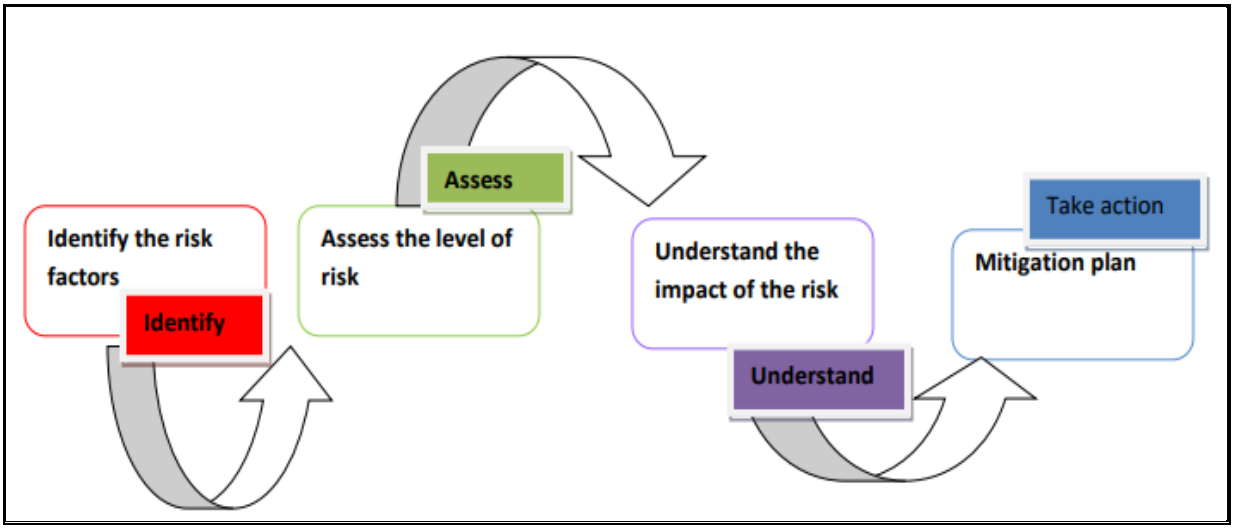
This Guidance Note comes into effect on **17 April 2023**.

PART A

PRACTICAL RISK ASSESSMENTS IN CASINOS AND ONLINE OPERATORS (OGSPs)

3. UNDERSTANDING RISK AND THE RISK BASED APPROACH

The Risk-Based Approach (RBA) speaks to a control system premised on an entity's understanding of risks it may be exposed to. As shown in the diagram below, such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). The key features are identifying risks, assessing such risks to understand its levels and impact, followed by a mitigation plan aligned to such risk levels. An effective control implementation is also characterised by documenting ML/TF/PF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which risks are tracked.



Risk Based Approach implementation framework

Money launderers look for cash-based service industries with high turnover rates. Casinos are cash based high turnover businesses. The ease with which Casinos accept cash as a means for clients to introduce proceeds, which may be from illicit activities, is a major draw card for potential money launderers. Similarly, the ease with which cash or proceeds introduced (in Casinos) can be withdrawn and presented elsewhere in the financial system naturally distances such from illicit origins. OGSPs are targeted as they are a non-face-to-face platforms with limited CDD and thus vulnerable to ML/TF abuse.

As a control framework, the RBA ensures efficiency of operations within AML/CFT/CPF activities. If duly implemented, the RBA ensures prudent balancing of compliance costs to business and customers by prioritising and directing controls to where they are most needed, in a prudent manner. This ensures high risk clients and services are accorded controls which are commensurate to risk while lower risk clients and services are not burdened with unwarranted due diligence.

3.1 ML Risks in Casinos and OGSPs

It may be difficult to distinguish a money launderer using illicit funds from an innocent patron gambling legally. As a result, purporting illicit funds to be winnings from gambling is a simple method of gaining the impression that they have been won legitimately. In some Casinos, if the winnings are redeemed for a casino payment, such is endorsed as verified which further legitimises the proceeds/money. With OGSPs the fact that winnings can be paid to a client's bank account or redeemable wallet provides the necessary validation or legitimacy to advance ML/TF.

Casinos are by nature a cash intensive business and many transactions are cash based. During a single visit to a casino, 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[3].

Casinos and OGSPs, as part of their risk assessment process, should assess the ML/TF/PF vulnerabilities and high-risk factors associated with each of their products/services. Below are some examples of higher risks:

3.1.1 Use of Stored Value Instruments

Casinos and OGSPs use a variety of value instruments to facilitate gambling/gaming on the part of their customers. The most common value instruments are chips, which are used in lieu of

[3] The 'buy in' stage is when a customer enters a casino and purchases casino chips, tickets, or gaming machine credits in order to commence gambling. The 'cash out' stage is when a customer converts casino chips, tickets or gaming machine credits for cash, casino cheque, credits an account or transfers funds to another casino.

cash for gaming or gambling transactions. Value instruments are used in the placement and layering phases of money laundering activity. Typically, illicit funds are placed when they are used to purchase chips, and then layered when, after minimal play, the chips are redeemed for pay-outs. This provides the appearance of legitimacy to the source of the funds, especially if OGSPs/Casinos confirm that the pay-outs represent gambling/gaming winnings.

3.1.2 Refining

Refining in land-based Casinos is the conversion of small denomination bank notes to large denomination bank notes. The method is commonly associated with drug trafficking, as drug dealers accumulate a large amount of smaller denomination bank notes through the course of their activities. Refining can occur at Casinos that make use of 'Ticket In/Ticket Out' (TITO) tickets or through currency exchange and such services.

3.1.3 Front Money Accounts

Some of the larger Casinos allow customers to establish accounts with them. There are generally two types of accounts that are offered: credit accounts and front money accounts. A credit account allows the customer to borrow funds from the casino, which are to be repaid within an agreed upon period of time. Front money accounts are more widely available in Namibian Casinos than credit accounts and allow a customer to deposit money with the Casino, which they can draw upon for gambling/gaming purposes.

Soe online services locally enable client to load credits into one of their slots or land-based operations while others can be loaded with transfers directly from a bank account. OGSPs need to ascertain that funds being introduced to their platforms in whatever delivery channels do not unduly expose them to ML/TF/PF risks. Funds from bank accounts could present lower risks as they may have been subjected to the necessary due diligence. Care however needs to be taken to ensure risk mitigation given individual clients' risk profiles.

3.1.4 Junkets[4] and International Players

Locally, FIC reviews suggest local Casinos are either not aware of Junket operations or do not have measures that can deliberately identify and target such in order mitigate risks they may pose.

While casinos deal with most of their customers face-to-face, for junkets, the junket organiser is an intermediary between the Casino and the player. The inclusion of junket services is to alert the sector of such operations which may pool funds from different sources and avail such to different people who introduce themselves as individual clients to a Casino. If funds are pooled from higher risk sources, the Casino operations are exposed.

The junket organiser also controls the financial transactions of the entire junket group. The practice of pooling potentially large sums of money into the hands of the junket organisers creates obscurity of the source and ownership of the funds of the various players. It also provides an opportunity to conceal the real ownership of illicit funds. Junket operators may also employ third parties to lead tours in order to distance themselves from the junket and any ML conducted on behalf of criminals.

The fastest growing revenue stream for some casinos are players, mainly from Asia, visiting for short periods often in the form of an organised junket. This is a significant source of revenue for some casinos. Junket participants utilise the junket organiser to move their funds to and from the Casino. Prior to departing for Namibia (or any country), the junket organiser will typically pool money from the junket players and bring the pooled funds into Namibia through international funds transfers.

[4] Junket operators are best described as a mixture of a travel agency, VIP hospitality service, and semi-banking firms. These companies have the objective of reaching out to high rollers and provide them with specialized offers to come and gamble at a particular casino.

It is not clear if OGSPs are exposed to junket services but it is logical to assume that people making use of such services can easily pool funds from other sources of similar nature, presenting OGSPs to enhanced ML/TF/PF risks.

3.1.5 Chip Dumping

In some cases, Online Operators do not follow through with player verification in a timely manner. Launderers can take full advantage of loopholes like this by using illegitimate (fake) IDs to create bogus accounts with which to move funds. A criminal can easily pump money in and out of an online gambling operation and then close the account before the casino realises anything untoward has happened. Chip dumping occurs when one player purposely loses a large sum of money to another. These players could be sitting in the same room so all the 'winning' player needs to do is make a withdrawal and they will have 'clean money'.

3.1.6 Exposure to Cryptocurrencies

Cryptocurrencies are mostly poorly regulated and thus present higher ML/TF/PF risks. Some illegitimate online operators (especially on the international front) allow criminals to exchange cryptocurrencies for funds. Risks in these transactions are higher as such cryptocurrencies could be proceeds of funds being laundered.

3.2 Other methods of ML/TF/PF in Casinos

a. *Purchase of chips from 'clean' players at a higher price* – Gaming chips frequently change hands between patrons in VIP rooms. Money launderers are willing to suffer some loss in order to legitimise their illicit proceeds. Further, the loss with the purchase of chips from clean players is potentially lower than with gambling, where there is no guarantee of a return. The principles can be the same in OGSPs;

b. *Combining winnings and cash into Casino pay-outs/cheques* – Although this technique is possible, it is unlikely as it does not afford patrons the level of anonymity associated with

other methods. It is helpful that local Casinos rarely make pay-outs directly to client bank accounts as such enhances risks. Care needs to be taken when clients request pay-outs to be transferred to their bank accounts; and

c. *The exchange of cash for Casino chips, TITO tickets and certified pay-outs/cheques* – Ticket In/Ticket Out is a gambling/gaming machine system that allows a machine to accept either banknotes or tickets with a credit value printed on them (Ticket In) to commence play. TITO also prints tickets with a credit value when a player wishes to cash out of the gaming machine (Ticket Out). The player can then redeem their ticket for cash at a cashier's desk or insert the ticket into another TITO machine.

3.3 TF Risks in Casinos

Namibia has not observed potential TF exposure within the Casino sector. This does not however mean the sector is not vulnerable to such abuse. OGSPs, given their ability to facilitate movement of proceeds in the financial system are inherently more vulnerable to TF abuse, especially when clients can introduce the possibility of international transfers directly or indirectly.

The 2020 NRA notes that whilst Namibia is not considered high-risk for TF, even small-scale financing raised from within Namibia could have significant impact. In light of this assessment, it is prudent for all Accountable Institutions as per the FIA to consider the vulnerabilities and risk factors associated with TF and the potential red flags that may indicate TF activity. Accountable Institutions should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds across borders. The NRA equally found that Namibia's porous borders present a significant vulnerability which enhances the ease with which proceeds can be moved around.

TF covers a wide range of terrorism-related activity, including operational funds, equipment, salaries and family compensation, social services, propaganda (e.g radicalization), training, travel, recruitment and corruption. It is not necessary for Accountable Institutions to identify the

purpose of TF, as a pre-requisite for reporting. Any potential TF-related information or suspicion must be reported to the FIC promptly and without delay. What is helpful is that such report be as accurate as possible, timely and treated with urgency and sensitivity.

As per the various domestic SRAs[5], NRAs and consideration of TF trends internationally, the FIC highlights the following as primary TF threats Accountable Institutions, including Casinos, should consider:

a. *Overseas groups able to inspire support through ideology* – Individuals may be inspired to contribute to overseas terrorist groups by travelling to conflict zones, which requires self or third-party funding. Radicalised individuals may also choose to contribute to terrorism by raising and contributing funds;

b. *Well-resourced groups with established networks* – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups;

c. *Domestic terrorism* – given the low-to-non-existent level of domestic support for terrorist causes and absence of terrorist networks, it is more likely that financiers of domestic terrorism (if it were to happen domestically) could manifest in Namibia as isolated disaffected individuals or small groups.

OGSPs need to duly identify their clients, assess their risk profiles to minimize abuse from those who may use online transferring capabilities of pay-outs or redemptions to advance TF.

3.3.1 Nature of TF

The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behaviour and funding can come from legitimate as well as illicit sources. OGSPs and Casino's must appreciate that the methods used to monitor ML (as

[5] Sectoral Risk Assessments

stated herein) can also be used for TF, as the movement of those funds often relies on similar methods to ML. Internationally the TF processes are considered to typically involve the following three stages:

a. *Raising funds* (through donations, legitimate wages, selling items, criminal activity);
b. *Transferring funds* (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell); and
c. *Using funds* (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)

The risks associated with TF are highly dynamic. As such, Casinos and OGSPs need to ensure that their prevention and combatting measures are current, regularly reviewed and flexible. It is important to maintain preventative and combatting awareness as well as effective transaction monitoring systems that incorporate dynamic TF risks, along the more static risks associated with ML.

As seen from the 2020 NRA, the value of funds moved through Namibia connected to TF is likely to be much lower than other forms of illicit capital flows. However, if funds connected to TF were to be associated with Namibian institutions, it would likely have an adverse effect on Namibia's reputation. Outside of the obvious harm caused as a result of TF, any domestic institution with this activity could see their reputation severely damaged. If such institution's combatting and prevention measures were found to be inadequate or ineffective, they could also face civil and potentially criminal charges as per the FIA and PACOTPAA[6].

3.3.2 Namibia as a Conduit for TF

One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit Namibia as a source or conduit for funds to capitalise on Namibia's reputation as being a lower risk

[6] Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014).

jurisdiction for TF. For instance, funds originating in or passing through Namibia may be less likely to attract suspicion internationally.

TF through the DNFBPs[7] and the gambling sector in particular can be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of Namibia. It could also involve remittance agents sending funds overseas. For Casinos and OGSPs, proceeds from supposed winnings could be moved in the financial system to advance TF with the casino-association providing a form of legitimacy.

The same methods explained above through which Casinos and OGSPs can be abused to advance TF are similar for PF. The due diligence and RBA, especially screening of clients/parties to transactions against sanctions lists is essential in combatting both TF and PF within the sector.

3.4 Foundation for RBA: Conducting Risk Assessments

The object of understanding client and transaction risks is to help the Casino and OGSPs determine the level of due diligence such client should be subjected to, in view of the services they wish to make use of. The principle in AML/CFT/CPF due diligence is that low risk clients making use of low risk services should be subjected to minimum or simplified due diligence. On the other hand. Higher risk clients should be subjected to Enhanced Due Diligence (EDD). The nature and extent of EDD is dependent on the level of assurance/comfort that a Casino or OGSPs needs to gain in reducing its ML/TF/PF risk exposure.

Casinos and OGSPs, like all other Accountable Institutions are best placed to understand their risk exposure and thus implement controls to manage same. This section avails basic guidance around the RBA. A Casino and OGSPs must:

[7] Designated Non-Financial Businesses and Professionals.

3.4.1 Undertaking ML/TF/PF Risk Assessments[8]

The comprehensiveness of which should be aligned to the nature, complexity and risk exposure of their proposed products and services (or amendments to such). The main elements Accountable Institutions are required to consider in risk assessments are: client risk profiles, product/service vulnerabilities and delivery channels associated with such products and services. Below is brief guidance on such elements in relation to the Casino and OGSPs sector:

3.4.1.1 Evaluate Client Risk Profiles

The risk profiles of clients who make use of Casino and OGSPs products and services determine the level of due diligence they will be subjected to. Section 23 of the FIA prescribes obligations with regards to the treatment of "Risk clients". Where a client has been identified as high risk, Casinos and OGSPs must apply EDD measures. The 2020 NRA observed that Casino services attract foreign clients from all over the world. Some from countries without reliable identification infrastructure. There is a possibility that such clients could be linked to complex and opaque legal structures internationally.

Casinos and OGSPs naturally attract high net worth individuals, including domestic and international Politically Exposed Persons (PEPs). Inherently, PEPs[9], foreign nationals or other such type of persons whose Customer Due Diligence (CDD) information cannot be effectively or readily verified with relevant domestic authorities may present enhanced risk exposure. PEPs need to be subjected to Enhanced Customer Due Diligence (EDD). See FIC's 2019 Guidance on PEPs. In the case of foreign customers, the periodic risk assessment should indicate the inherent risk level of countries, in order to aid risk considerations for foreign clients. The reliability

[8] FIA section 39(1) [Read with FIA section 23]: An accountable institution, on a regular basis, must conduct ML/TF/PF activities risk assessments taking into account the scope and nature of its clients, products and services, as well as the geographical area from where its clients and business dealings originate. Persons much measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the services they aim to provide. You should rank each service as low, medium or high risk. The control measures should describe how the entity will reduce each level of risk, especially the medium and higher risk rated levels. The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

[9] Annexure A, attached hereto lists type of persons who meet the description of PEPs. See FIC Directive No. 02 of 2020 on PEPs as well as Guidance Note No. 01 of 2019 on the definition and due diligence required for PEPs: Both documents are available on the FIC Website under the "Publications" folder.

of national identification systems in foreign countries and the effectiveness of AML/CFT/CPF controls in such countries should always be considered. Below are examples of clients/activities which introduce higher ML/TF risks:

a. ***Unknown Customers:*** *It is common cause that the FIA requires identification for Casinos and OGSPs only when they transact in transaction(s) above NAD 24,999.99. Unknown customers present a higher risk than known customers. Customers could thus deliberately transact below the said identification threshold and remain below the minimum AML/CFT/CPF requirement for due diligence. Laundering would be easy as such customers can purchase large amounts of chips with currency at table games, engage in minimal or no play, and then redeem the chips for large denomination bills (e.g. NAD 100 or NAD 200.00 notes). The risk is further escalated if Casino or OGSPs sends funds to client account via EFT or wire transfers. Measures should be in place to only enable EFTs when absolutely satisfied that laundering risk is reduced;*

   Casinos and OGSPs should implement procedures and systems to assist in the identification of unknown customers redeeming large amounts of chips for possible dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid due diligence undertaken at a threshold level. This could extend to measures such as not cashing out such customers or cashing out by paying in small denomination bills, which are harder to hide or transport, as well as maintaining surveillance photographs and filing suspicious activity reports with physical descriptions;

b. ***High spenders[10]:*** *Given the variations among Casinos and OGSPs, the level of spending considered to be relatively high for an individual customer will vary among operators, and even among Casinos and OGSPs owned and managed by the same operator. Customers may become high spenders because of their cumulative spending over a period of time (e.g. customers with relatively high level of spending with Casino/OGSPs accountholder relationships). Similarly, casual customers who gamble a relatively large amount of*

[10] Casinos should take into account the relative value of the monies in the country where the customer obtained their wealth. Land-based casinos should also take into account the relative value in the country where the customer is spending their money.

money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders. Some Casinos and OGSPs offer special facilities to high spending customers, e.g. the use of VIP rooms to gamble away from the general public areas of casinos. Casinos and OGSPs need to ensure that AML/CFT policies, procedures and internal controls are applied consistently to customers in VIP rooms (particularly for casino due diligence, recordkeeping, suspicious activity reporting, and where required, currency transaction reporting).

c. ***Disproportionate spenders:*** *Casinos and OGSPs should devise policies relative to obtaining information about customers' financial resources, when feasible and available, to determine if customers fall into this category. These policies should be based on risk-based considerations on the part of the operator. One issue to consider is if and how Casinos/OGSPs can gain an understanding of their customers' sources of income or wealth. This information could provide some insight as to the likely level of disposable assets which customers have available to gamble, (though this may only be feasible in practice when a customer makes a credit application).*[11]

   In addition, Casinos and OGSPs should be alert to customers engaged in high value gambling that is inconsistent with an operator's information about customers' known levels or sources of assets (e.g. a customer's bank account) and/or income, or understanding of customers' occupations evidenced in Casino/OGSPs credit account records (i.e. credit application), as well as any other information on file including established play at other Casinos/OGSPs. If, and when this information is obtained, it may assist in assessing whether a customer's level of gambling is commensurate to her/his assets or level of legitimate income. For example, it may be advisable to scrutinise a customer with relatively modest assets or income, who suddenly becomes a high spending customer;

d. ***Understanding the types of customers:*** *While casual customers can pose a heightened money laundering risk in some situations, it may be difficult to identify their*

[11] For example, the level of available assets is important in situations in which customers gamble on "credit".

associated spending patterns. This category would include tourists, although not all passing tourist trade will fall within this definition. Land-based Casinos may host tourists on organised gambling tours (known as junkets), which are discussed below. However, even regular customers may pose a risk, particularly if their spending pattern changes, e.g it dramatically increases or their rated play does not fit their playing profile e.g. minimal play. In considering an overall appreciation to the nature of controls to implement, the Casino or OGSPs needs to assess whether:

- *the majority of customers are regular customers, including members; or*
- *Passing trade, including casual tourists or organised casino tours (known as junkets).*

e. ***Ultimate Beneficial Owners (UBOs):*** *while the sector does not deal with clients who are legal persons, it is worth noting that Close Corporations (CCs) are the most abused vehicles to advance ML, as per the 2023 National Risk Assessment (NRA) update. Caution needs to be had when clients known or identified as UBOs or representatives of CCs are making use of Casino services;*

f. ***Improper use of third parties:*** *Similar to Junket services, criminals may use third parties, or anonymous or identified agents to avoid CDD undertaken at a threshold. They may also be used to gamble, e.g. to break up large amounts of cash. Third parties may be used to buy chips, or to gamble on behalf of others with minimal play (which may include early or high cash outs), or cash out/redeem chips for larger denomination currency, casino checks, etc. It is a lot easier to use third parties with online services as there is no face-to-face engagement between the operator's personnel and online customer;*

g. ***Junkets:*** *Over-reliance on tour operators can pose a heightened money laundering risk especially in a market such as Namibia, with a resident population too small to normally support Casinos. In these instances, Casinos can become overly dependent on junket representatives for business, a potential misuse of these services. In large markets, junket representatives are sources of premium players for Casinos. In some instances, a*

Casino may enter into a contractual agreement with a junket operator to rent a private room within a Casino and in some situations, it is the junket operator, not the Casino, which monitors player activity and issues and collects credit.

Junket operators that provide premium players may exert commercial pressures on Casinos which may result in reducing scrutiny of individual spending patterns or may try to unduly influence or exercise control over licensed Casino operations. Further, junket organisers may engage in lending or the facilitation of lending to players outside the Casinos' knowledge. In most instances, junket organisers 'pool' resources and therefore obscure the spending of individual customers, thus preventing casinos from making any assessment of customers' spending patterns vs financial capacity/profile. Casinos need to devise measures to identify and prevent junket organisers from engaging in informal arrangements that are inconsistent with risk-based AML/CTF policies, procedures and internal controls;

h. ***Multiple casino player rating accounts:*** *Some players will open up multiple player rating accounts with different names at the same Casino or OGSPs and will provide different rating account numbers to Casino or OGSPs raters at different times to hinder an operator's ability to track their gambling activities under the same customer name. Casinos and OGSPs will need to identify such accounts with similar players' names and the same physical descriptions (e.g. age, male or female, eye colour, hair colour, height, weight) to be able to monitor customers' aggregate gambling across their Casino or OGSPs operations. Casinos and OGSPs should implement policies, procedures and systems to assist in the identification of customers opening multiple-player rating accounts for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid government reporting thresholds.*

Practical tip:

In practice, the overall risk is assessed periodically and client profile types are identified, which can for example be: Foreign PEP, Domestic PEP, Self-Employed businessman, Government Employee, teacher, Bank Employee etc. Inherent risk levels (high, medium, low) are then assigned to each such group/profile. When a client is onboarded, he or she is placed in one of such profiles and then subjected to due diligence relevant for such profile. Such due diligence must then include reviewing information which may be specific to such individual client.

3.4.1.2 Vulnerability of Products and Services

The 2020 NRA found that Table Betting services carry a slightly higher ML risk than Slot Machines. Casinos and OGSPs have to conduct their internal product vulnerability assessments. The following are a few examples of service vulnerabilities:

a. ***Proceeds of crime:*** *whichever way money is transferred to a Casino and OGSPs, there is a risk that such money could have arisen from illegal activities such as fraud, narcotics trafficking, theft from employer. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk;*

b. ***Cash:*** *Customers may use a land-based Casinos to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport. Also, certain cash deposits by a customer, especially cash deposits which are considered relatively large either in relation to i) a particular Casino's average receipts, or ii) what is known about a customer's financial status. The majority of payments to Online Operators are made directly from financial institution accounts. However, Online Operators can operate as part of mixed gambling chains which also include betting shops and/or land-based casinos. It may be possible for customers to provide land-based outlets with cash*

which can then be credited to Online Operator accounts. Online Operators should work closely with their land-based counterparts that initially receive the cash to ensure that CDD measures are applied, including verifying that the depositor is the account holder, and when appropriate, benefit is secured from the personal contact between land-based Casino staff and customers;

The Gaming and Entertainment Control Act, 2018 in its current form does not make provision for online Casino activities, although it is unclear whether such position renders same illegal. There are no enforcements observed for domestic Gambling Houses (Not licensed Casinos) already availing such online gambling services. In February 2023, the Gambling Board confirmed that is has received industry requests from Land-based Casinos to amend the law to provide for such or issue guidelines in such regard;

c. ***Transfers between customers:*** *If Online Operators wish to allow inter-account transfers between their customers they should devise careful policies and procedures which monitor the amount of the transfer(s). Online Operators may also be aware of customers transferring money between themselves more informally without using their operator accounts, which should be taken into consideration in the operator's risk assessments. Land-based Casinos may also be aware of customers borrowing money from non-conventional sources, including other customers. Informal money lending can be illegal, and it can also offer criminals an opportunity to introduce proceeds of crime, usually cash, into the legitimate financial system through the Casino. Again, this can pose a heightened risk;*

d. ***Use of Casino and OGSPs deposit accounts:*** *Casinos and OGSPs will wish to encourage their customers to only use their deposit accounts for gambling purposes. Casinos need to consider what constitutes an abuse of such an account and should have policies, procedures, and internal controls, to prevent customers from using such accounts to deposit and withdraw without gambling or minimal play;*

e. ***Redemption of Chips, Tickets or Tokens for Currency:*** *Casinos and OGSPs are not required to identify clients transacting at, or below NAD 24,999.99. Therefore, customers are not required to provide identification for the redemption of chips, tickets or tokens unless transaction is above the said threshold. For a customer that has an established Casino/OGSP account number[12], a Casino/OGSP, which is not required to record such transactions at the cage (or such similar virtual/online arrangement), nonetheless should have policies, procedures, and internal controls to identify large redemptions[13] to such a customer that were paid with currency (including any large cash outs without gambling for large denomination bills). Casinos and OGSPs should also have procedures in place to identify clients (including non-account holders) who could be structuring their transactions below the identification thresholds; and*

f. ***EFTs and direct payments to client accounts:*** *This speaks to the delivery chanel of pay-outs. Clients who request or insist on pay-outs, winnings or redemptions to be paid directly to their bank accounts present higher risk of ML/TF/PF. For this reason, such should be minimal and due diligence duly executed if permitted. It is however pleasing to note that redemptions and winnings/pay-outs are paid in cash to clients, over 99% of the time. Unlike in other countries, local Casinos rarely make payments directly from their bank accounts to client accounts. The sector is cash intensive in that clients introduce cash and receive payments in cash.*

3.4.1.3 Evaluate Product Delivery Channels

Delivery channels speak to the means or channels through which Casinos provide their services. For example, face-to-face or online services or through intermediaries such as Junkers. Conventionally, online Casino operations are exposed to higher ML/TF risks than land-based

[12] Types of casino accounts that a customer could have include deposit (i.e. safekeeping, front money or wagering), credit, check cashing, player rating or tracking, and slot club accounts.

[13] As part of a casino's risk-based prevention program, when a customer presents at a cage a large chip or token redemption, a cashier confirms it typically by a telephone call to a pit boss, floor person, card room supervisor, or other casino employee to determine if the chips were put at risk, or won at a table game as "verified winnings" or purchased at a table (e.g. when a customer is "walking with" chips at the end of table game play) to identify: i) potential counterfeit chips or tokens, ii) stolen chips or tokens, or iii) any temporary advance of chips to a customer (i.e. rim credit). Also, a cage cashier will query a casino's credit system for credit issuance (i.e. marker) and credit payment (i.e. marker redemption) activities for a customer with large chip or token redemptions.

Casinos. Below are various considerations which apply to and OGSPs and such online casino operations:

a. ***Payment methods:*** *This refers to the types of payment, and payment methods, accepted from customers. Payments via speed points or using debit and credit cards may present reduced ML/TF risks than cash payments;*

b. ***Multiple casino accounts or casino wallets:*** *An online operator may own and control multiple web sites. Single web sites can also offer a range of different types of gambling. Operators will need to monitor customers' aggregate position across the whole of their online gambling service businesses. Customers may wish to separate the different types of gambling they are conducting with the same operator, or through the same website, for legitimate reasons, e.g to monitor their performance in different areas. Operators should implement procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level;*

c. ***Changes to banking/financial institution accounts:*** *Online Operators' customers commonly use their accounts with financial institutions to gamble online. Customers may hold a number of financial institution accounts, and they may wish to change which of these accounts they use in certain operations/casinos. Operators may wish to consider updating customer due diligence following such changes in banking details for example;*

d. ***Identity fraud:*** *Details of financial institution accounts may be stolen and used on websites. Stolen identities may also be successfully used to open financial institutions accounts, and such accounts may also be used on websites. Internet Provider (IP) address/number checks are useful in preventing criminals from opening multiple online (or land-based gambling) accounts using stolen identities, using the same computer. Operators will be aware of these risks because of the 'charge back' system. Online*

Operators also have a responsibility to protect their customers from having their identities stolen when using their websites, and will therefore need to provide adequate security;

e. ***Pre-paid cards:*** *Using cash to fund a pre-paid card poses similar risks as cash. Operators cannot make the same level of cross reference checks on some types of pre-paid cards as they are able to perform on financial institution accounts;*

f. ***Games involving multiple operators:*** *Poker games often take place on platforms (i.e a central computer system that links electronic gambling devices for purposes of game selection, operation, monitoring, security, and auditing) shared by a number of different Online Operators. The platform is likely to play a key role in monitoring the pattern and value of play for potential ML activities, e.g. chip dumping. The operator and the platform should have clear policies in respect to respective roles, alerts, enquiries and subsequent actions, for AML/CFT purposes.*

3.5 Role of Key Partners/Stakeholders

The provision of some services in the sector require inputs or responsibilities undertaken by partners or stakeholders. Casinos and OGSPs should duly understand the nature and effectiveness of AML/CFT/CPF controls that are implemented by such partners or stakeholders in the value chain, if any. Ensure that such partners or stakeholders have capacity and are willing to play their part in ensuring effective risk mitigation as per the FIA. Controls such as availability of records[14], as and when required by the institution (for timely and effective due diligence) or competent authorities[15] are worth considering;

[14] As per FIA record keeping obligations.
[15] As defined by the FIA.

3.6 Type, Nature and Extent of Controls

To reduce inherent[16] risks to tolerable or acceptable residual[17] levels. Casinos and OGSPs have a responsibility to implement such controls and duly demonstrate their effectiveness to authorities such as the FIC. The FIC must be satisfied, upon such presentation, that such residual risk levels are tolerable or acceptable to the national AML/CFT/CPF framework. The following considerations are essential in designing controls that respond to risk exposure:

a. *Type and effectiveness of existing supervision mechanisms:* For example, electronic and/or physical, loyalty clubs which monitor gaming activities. The speed and volume of business can be used as a guideline to the extent of controls;
b. *Staffing numbers, turnover rate and experience levels:* Experienced staff members who understand FIA obligations are helpful in implementing effective controls;
c. *Honesty and integrity of staff:* Special care should be taken to ensure that all staff members are aware of their operational policies and procedures relating to assisting or facilitating customers to advance ML/TF; and
d. Whether the Casino or OGSPs' business model centres upon either of the following options, or both:
    - Attracting a large number of customers who gamble relatively small amounts of money, or
    - Attracting a small number of customers who gamble relatively large amounts of money.

The entirety of controls, aligned to risks, should be documented in an AML/CFT/CPF Program or Policy document which needs management approval.

[16] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.
[17] The remaining risk level after due controls have been implemented.

3.7 New Innovations, Products and Services

New innovations can often change existing control effectiveness or introduce new areas of risk exposure. For institutions already operating in the AML/CFT/CPF framework and are launching or introducing new products, it is essential to ensure aligning the approved AML/CFT/CPF Program or Policies to speak to the new products or innovations. The existing program may be amended if introduction of new innovations or proposed amendments so require. FIC Directive 01 of 2021 explains considerations around introducing new products and services to the AML/CFTCPF space.

3.8 Segregation of Duties

Although not explicitly stated in the FIA, the nature of risk exposure as stated herein warrants that Casinos implement segregation of duties to prevent collusion between employees and customers. This may include separating the functions of cash handling, gaming operations, and customer service.

3.9 External Risk Assessments

The considerations and indicators herein are not extensive. Casinos are required to consider observations from Sectoral Risk Assessment Reports and National Risk Assessments issued by the FIC. Local[18] and international trends and typology reports issued by bodies such as ESAAMLG[19] and FATF[20] (available on their websites) equally help highlight changing risks broadly and related to the sector. To the extent possible, this guidance has incorporated lessons and best practices from such local and international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard.

[18] Published on the FIC website under Risk Assessments folder while trends and typology reports are under Publications folder.
[19] https://www.esaamlg.org/index.php/methods_trends
[20] https://www.fatf-gafi.org/en/publications.html

3.10 Risk Assessment/Management Reports

All identified risks as far as products, services, delivery channels, types of clients etc., should be documented in Risk Management Reports. Such report(s) should be periodically updated when material changes arise in risks and controls.

PART B

IMPLEMENTING A RISK-BASED PREVENTATIVE FRAMEWORK

4. RISK BASED APPROACH

Part A above dealt with evaluation of risks presented by customers/clients and the vulnerability of services or transactions such customers make use of. This part builds on CDD measures to mitigate such risks in a Casino and OGSP. The strategies to mitigate risks should be designed to identify or prevent the activity from occurring through a combination of deterrence measures such as: on-going and enhanced due diligence of client behaviour[21], effecting appropriate CDD[22] measures for customers (e.g especially for deposit); record keeping[23] to assist criminal investigations; monitoring[24] to detect suspicions for and reporting[25].

The FIC website contains Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA.

4.1 Extent of Customer Due Diligence Measures

The nature and extent of CDD measures depends on the degree of risk a client, in view of the service/transaction, they wish to access, presents to the Casino or OGSP.

CDD goes beyond simply carrying out identity checks to understanding who one is dealing with. This is important because even people known to the Casino or OGSP may become involved in illegal activities at some time, for example if their personal circumstances change or they face new financial pressures. A Casino or OGSPs' due diligence measures should reduce this inherent risk and the opportunities for staff to be corrupted. The Casino or and OGSPs should be able to demonstrate that the extent of the CDD measures applied for each client are appropriate to mitigate risk exposure.

[21] FIA Sections 23 and 24
[22] FIA Sections 21 and 22
[23] FIA Sections 26 and 27
[24] FIA Section 24
[25] FIA Section 33

4.2 Simplified Due Diligence

4.2.1 Extent of Simplified CDD

The extent to which simplified due diligence should be applied is essential to financial inclusion objectives. For this reason, identification in terms of the FIA should only be applied when so required. Given this, it is important to note that identification of clients is required when a business relationship (gambling account opened) is established or when a single transaction (walk-in client) that exceeds the following thresholds is entered into:

CDD Threshold	Extend of CDD
Less than or equal to NAD 24,999.99	Below simplified CDD threshold. The normal Casino identification for general operational purposes should suffice. Only apply EDD if risk is assessed as high, e.g structuring in small amounts below threshold.
Above NAD 24,999.99	Simplified CDD as a minimum, and escalation to EDD if risk is high.

A Casino or OGSP may apply simplified due diligence measures where the business relationship or transaction is considered low risk in terms of ML, TF or PF. In practice, simplified due diligence only applies to a client when the Casino assess such as being low risk. Transactional risk exposure such as destination of or origin of funds should be equally considered and if risk is higher, EDD should be considered. FIA Regulations 6 to 11 provide guidance on the minimum identification procedures that should be followed for the various types of clients.

4.2.2 Ascertainment and Verification of Information

When simplified due diligence is applicable, Casinos and OGSPs are still required to identify and verify or ascertain customers' identification information. Below is a list of the type of

information which needs to be ascertained/verified and that which needs to be obtained (from client):

a. Verification: full names;
b. Verification: nationality;
c. Verification: If citizen – national ID no./ passport no./date of birth;
d. Verification: Non-citizen – passport no./national ID no./date of birth;
e. Obtain: Namibia residential address for citizens OR if non-citizen, residential address in his/her country or physical address in Namibia, if any; and
f. Contact particulars.

4.2.3 Tips on simplified CDD

Casinos and OGSPs may:

a. use information already at hand such as client profile, without unduly requesting for me. For example, if you identified your customer as a student or pensioner, you can assume what the source of funds is, unless other factors exist, such as higher financial values or too frequent transactions which may be beyond reasonable student or pensioner earnings; and
b. adjust the frequency of CDD reviews when necessary, for example, when a change occurs which may suggest escalation of the low-risk behaviour.

4.2.4 Pre-requisites for Simplified Due Diligence

To apply simplified due diligence, a Casino or OGSP must ensure:

a. it is supported by internal customer risk assessment;
b. enhanced due diligence does not apply (there is no high risk in terms of client or service);
c. there is no structuring of transactions to reduce amounts and reduce or avoid EDD measures;
d. monitoring the business relationship or transactions (e.g with frequent transactions of similar client) to ensure that there is nothing unusual or suspicious from the outset;

e. customer is not from, nor associated with a high risk country;
f. the customer is not a PEP, a family member, or a known close associate of a PEP;
g. the real customer is seen face-to-face (and not having others transact on his/her behalf. This may be necessary at least when creating account for Online Operators);
h. the source of funds or wealth are transparent and understood; and
i. the transaction is not complex or unusually large.

4.2.5 When to cease Simplified Due Diligence and commence EDD:

a. If suspicions of ML, TF or PF arise;
b. doubt whether documents obtained for identification are genuine;
c. doubt whether the customer is indeed the one demonstrated in the documentation;
d. indications that client may be transacting on behalf of another unduly;
e. suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired. Impact of identity theft is rife with online services;
f. circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk; and
g. Any other considerations that do not maintain the low risk of client or specific transaction(s).

5. Enhanced Due Diligence (EDD)

5.1 Nature and Type of EDD Measures

It is critical that an ADLA has measures that can identify when to escalate from simplified due diligence to EDD, e.g identifying that a client meets the definition of a PEP. EDD applies when a client's risk profile or transaction is not low. It includes taking additional measures to identify and verify customer identity, creating a client's financial profile including the source of funds and conducting additional ongoing monitoring.

It is essential to keep in mind that identification procedures as per FIA Regulations 6 to 11 regulate obtaining the minimum identification information (as per 4.2.1 and 4.2.2 above) while Regulation 12 provides for EDD or obtaining additional information[26]. For non-account holders who would access Casino and OGSPs services, it is necessary to ensure obtaining all relevant information before availing services. If clients, by virtue of the type of membership that they are applying for would result in them transacting in higher values, it is essential to already subject them to EDD. If a client was admitted to a membership type wherein he or she transacts in lower values and at some point choses to migrate to other memberships wherein he/she can transact in higher values, the inherent risk naturally escalates and it is prudent to subject such to EDD upon changing such membership.

EDD means building onto the basic identification information obtained as per simplified due diligence measures in parts 4.2.1 and 4.2.2 above. Such EDD information primarily includes the following and is useful in monitoring transactional behaviour:

Type of EDD Information	**Usefulness of Such**
Nature & location of business activities	Creating client financial profile: Helps Casino create context around magnitude of clients' earning levels, especially for self-employed or business people.
Occupation or source of income	
Source of funds involved in transaction	Enables a comparison of transacting behaviour through funds being introduced or moved and the financial profile of client

Junket Operators, as described in the risk assessment section above presents a higher risk as Casinos will mostly not know whether clients are gambling their own funds or funds pooled from other sources. Casinos need to devise measures to identify and prevent junket organisers from engaging in informal arrangements that are inconsistent with risk-based AML/CTF policies, procedures and internal controls. There has to be deliberate efforts to identify such junket operations, especially amongst a group of gamblers, especially tourists.

[26] the extent of which is dependent on the risk the client/transaction may pose to the ADLA.

5.2 When to undertake EDD

a. As per internal risk assessment, Casino has determined that there is a high risk of ML, TF or PF associated with the client or transaction;
b. FIC or another supervisory or law enforcement authority provide information that a particular situation or client is high risk;
c. a customer originates from or has ties to a high risk country;
d. client has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious transaction/activity);
e. a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person;
f. the transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose;
g. client deposits or introduces funds into the Casino and soon thereafter, without logical explanation, chooses to withdraw same and asks for a transfer/payout; and
h. Any other considerations enhancing client or transaction risk.

5.3 Factors which escalate risks

Casinos and OGSPs should consider several factors in risk assessments when deciding if EDD needs to be applied. The following are some factors to consider.

5.3.1 Customer related factors based on information the Casino or OGSP has or behaviours indicating higher risk:

a. unusual aspects of the business relationship with client;
b. a client/person is resident in a high-risk area/country;
c. a client with an abundance of cash, without reasonable explanation;
d. too frequent or unusual transactions without reasonable explanations;

e. searches on a person or associates show, for example, adverse media reports/attention, disqualification as a director or convictions for dishonesty;
f. structuring or smurfing; and
g. any other relevant considerations.

5.3.2 Geographical factors indicating higher country risk

Customers from high risk countries are inherently high risk. The following are indications, based on credible sources, which may escalate the risk of a country:

a. has been assessed by organisations such as FATF, World Bank, Organisation for Economic Cooperation and Development and the International Monetary Fund as having in place *ineffective* AML/CFT/CPF measures;
b. not subject to equivalent AML/CFT/CPF measures;
c. with a significant level of corruption, terrorism, or supply of illicit drugs;
d. subject to sanctions or embargoes issued by UN, OFAC, EU etc;
e. providing funding or support for terrorism; and
f. having terrorist organisations designated by the UN, US, EU, other countries, and international organisations

In addition to the above, when the client (as per information at hand or in the media) can be linked to or is related to any of the following, a Casino or OGSP must consider EDD:

a. oil;
b. arms and weapons;
c. precious metals and stones;
d. tobacco products;
e. cultural artefacts; and
f. ivory and other items related to protected species

5.3.3 Understanding the concept of additional measures

For EDD to be undertaken duly, the Casino or OGSP must do more to verify, identify and scrutinise the background and nature of clients and their conduct relating to services. This is usually more extensive than simplified due diligence measures. The extent to which EDD goes beyond simplified due diligence must be clearly stated in the Casino or OGSPs' AML/CFT/CPF control procedures. For example, the Casino or OGSPs should:

a. obtain additional information or evidence to establish the identity from independent sources, such as supporting documentation on identity or address or electronic verification alongside manual checks;
b. take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who is competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust;
c. when receiving funds for gambling activities, ensure such funds are being introduced by the client and not another person merely using a client to introduce funds in the Casino or OGSP;
d. the following measures must be taken when the transaction relates to a PEP, a family member or known close associate of a PEP (See Guidance Note 01 of 2019 on PEPs for detailed guidance on PEPs):
    - obtain senior management approval before establishing a business relationship with that person;
    - take adequate steps to establish their nature of business activities, source of wealth and actual source of funds to be used in gambling activities; and
    - conduct enhanced ongoing monitoring if transactions are frequent or appear structured.
e. carry out more scrutiny of the client's transactions/conduct in the Casino or OGSP and satisfy yourself that it is consistent the client profile;

f. measures which must be taken when a client originates from, or has ties to a high-risk main or third country[27]:
   - Obtain additional information on the customer and the customer's beneficial owner(s), if they identify themselves as associated with a high risk entity;
   - Obtain the approval of senior management for establishing or continuing the business relationship; and
   - Enhance monitoring of the business relationship by increasing the number and timing of controls applied and select patterns of transactions which require further examination.

6. SUSPICIOUS TRANSACTION OR ACTIVITY REPORTS ("STRs/SARs")

The primary reason for monitoring transactions carried out by clients is to ensure that such transactions are consistent with the Casino or OGSP's knowledge of the client, the client's commercial or personal activities and risk profile. Suspicions are often detected from client behaviour or activities outside the known client profile. Thus, understanding client profile is essential as it places Casinos or OGSPs in positions to effectively detect and report suspicions when they arise. Indicators, especially such listed in Annexure A of this Guidance, are helpful in identifying potential suspicious activities or transactions.

New report types have been introduced to enhance effectiveness. With effect from 17 April 2023, TF and PF suspicions, as well as sanctions screening name matches shall no longer be reported through STRs and SARs on goAML. TF and PF suspicions shall only be reported through TPFA and TPFT reports, as explained in section 8 herein below. Similarly, sanctions screening name matches shall only be reported through Sanctions Name Match Activity reports (SNMAs). Only ML suspicions shall be reported through STRs and SARs.

[27] (a business is established in a country if they are incorporated there, is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there)

STRs are reports that explain suspicious transactions for ML. The term suspicion is meant to be applied in its everyday, normal sense. The suspicion, as an example, could be the funds involved in the transaction are the proceeds of any crime or linked to terrorist activity. The Casino or OGSP does not need to know what sort of crime may have been committed, but one or more red flags or warning signs of ML, which cannot be reasonably explained by the customer, should be adequate to reach the standard of what constitutes a suspicion worth reporting to the FIC.

SARs are reports which, under normal circumstances explain potential suspicious activity related to clients but may not necessarily be transactions whereas STRs refer to actual suspicious transactions. For example, if a client attempts to transact and after EDD enquiries does not proceed with finalizing the transaction, and the activities or his/her behaviour around such is suspicious, then the appropriate report to file with the FIC is a SAR and not a STR.

6.1 Reporting Behaviour of Casinos

Nationally, the FIC has received about 9,000 STRs from inception to date. Casinos only reported 39 STRs. When reports are received, such undergo a cleansing process which primarily results in categorization of same to determine how such reports would be treated (including setting aside or escalation to case files for further investigation). The table below shows record of STRs and SARs filed by the Casino sector.

Year	STRs	SARs
2023	12	0
2022	5	0
2021	0	2
2020	0	1
2019	5	0
2018	2	0
2017	9	1
2016	3	0
2015	0	0
2014	1	0
2013	1	0
2012	0	0
2011	1	0

Total	**39**	**4**

The above table suggests only 4 SARs were filed since inception, and they were all accorded a "Low Priority Status". Enhanced reporting in terms of quantity and STR quality remains essential to the combatting framework. The notable improvement in STRs reported in early 2023 by the sector is therefore encouraged. The table below speaks to the categorization of the 39 STRs received from the sector.

Case File Opened	Low Priority	Under Cleansing	Set-Aside
4	25	9	1

As per above table, most STRs from the sector were categorised as Low Priority. This does not however suggest poor reporting as the only reason for such categorisation, although such was observed in some STRs. Several factors including limited FIC investigation personnel and low financial values within certain STRs (when compared to other STRs nationally), amongst others, contribute to STRs being categorized as Low Priority.

6.2 Improving Report Quality

Below are some areas noted from the sector's STRs/SARs which can been enhanced on to improve STR/SAR quality.

a. **Lack of ML/TF and/or PF indicators in the reports:** It is helpful that upon reporting, such information is availed. If the internal risk assessment, CDD and ongoing monitoring measures are effective, such should yield indicators which may inform the suspicion. AML Compliance Officers are encouraged to reach out to the FIC when uncertain of suspicions;

b. **Poorly articulated "Reasons for Suspicion" in STRs:** usually, when adequate CDD has been undertaken, it is easier to explain grounds for suspicion when making analysis of flagged transactions. Regardless, attempts should be made to adequately explain why we find transactions or activities suspicious as such helps with FIC analysis of reports;

c. **Duplicate and erroneous filing of reports:** More care needs to be taken, especially by AML Compliance Officers to reduce erroneous and duplicate reporting. The initial cleansing processes take from the valuable time that FIC analysis resources could deploy to other activities; and

d. **Filing of incomplete STRs/SARs:** more could be done to ensure completeness of information shared in STRs. It helps with value addition from such reports. If the internal risk assessment, CDD and ongoing monitoring measures are effective, such should yield indicators which inform the suspicion. The draft Sectoral Guidance Doc lists indicators within Part A (risk assessment). Such can further assist in this regard. AML Compliance Officers are encouraged to reach out to the FIC when uncertain.

6.3 Practical Controls

Operating frameworks or controls in the Casino/OGSP must enable the following:

a. Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in ML, TF or PF;
b. The Casino or OGSP's AML Compliance Officer, or their appointed alternative, must consider all such internal reports. The Compliance Officer must submit relevant reports to the FIC via GoAML;
c. Such reports should be reported promptly and without delay to enhance the effectiveness of combatting activities;
d. After filing such report, the Casino or OGSP should consider all risk exposure and whether it is prudent to continue availing services to such client;
e. It is a criminal offence for anyone, following a disclosure to a Compliance Officer or to the FIC, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation;
f. Important actions required:

- enquiries made in respect of internal reports (red flags) must be recorded;
- the reasons why a report was, or was not, submitted should be recorded
- keep a record of any communications to or from the FIC about a suspicious transaction or activity report.

7. RECORD KEEPING

7.1 What Records must be kept?

a. the identity, address and all such client identification records as stated in part 4 herein;
b. the date, time and amounts of client's gambling activities/transactions;
c. information relating to all relevant reports filed with the FIC; and
d. any other information which the FIC may specify in writing.

OGSPs or Online Operators should satisfy themselves that the records they obtain would meet the required standard as per the FIA and summarised herein.

7.2 Who must keep records?

The Casino or OGSPs (as Accountable or Reporting Institution) ought to keep records as per the FIA. A third party may keep records on behalf of a Casino or OGSP but the institution remains ultimately accountable for ensuring such records are kept as per the FIA. Casinos or OGSPs must engage the FIC when proposing to outsource record keeping responsibilities. Further, the records of two or more Accountable or Reporting Institutions that are supervised by the same supervisory body can be centralised.

7.3 Manner of Record Keeping

The records must be kept:

a. in a manner that protects the confidentiality of such copy, record or document;

b. in a manner which permits reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity or civil or criminal asset forfeiture procedures.

Further, records can be kept in hard copy or electronic format as long as a paper copy can be readily produced. Casinos and OGSPs should maintain effective record-keeping systems to enable the FIC and other relevant authorities to access such records in a timely fashion. The Golden Rule with record keeping is enabling an effective reconstruction of identification or transacting activities by competent authorities.

7.4 Period for which records must be kept

Records that relate to the establishment of a business relationship must be kept as long as the business relationship exists and for at least five years from the date on which the business relationship is terminated. Records that relate to single transactions must be kept for five years from the date on which the transaction was concluded. Records that relate to copies of reports submitted to the FIC must be kept for a period of not less than five years from date of filing such report. However, records must be kept for longer than the 5-year period if the Casino or OGSP is requested to do so by the FIC, the Office of the Prosecutor-General or by any other law enforcement agency.

8. UNSC[28] SANCTIONS SCREENING

The object of sanctions screening is to implement Targeted Financial Sanctions (TFS) against anyone listed (or designated) by the UNSC.

Casinos and OGSPs are expected in terms of section 24 and Regulation 15(5)[29] of the FIA to screen clients or potential clients involved in transactions against the relevant sanctions lists

[28] United Nations Security Council

[29] Accountable institution to conduct on-going and enhanced customer due diligence: (5) An accountable institution must also, in the process of monitoring, screen - (a) names of prospective clients, before acceptance of such a client; (b) names of existing clients, during the course of the business relationship; and (c) all the names involved in any transaction, against the sanctions

issued by the United Nations Security Council (UNSC). Such screening should take place before accounts are opened or client is granted access to services, regardless of whether the client transacts below or above the CDD threshold. If making use of agents, in any way, Casinos and OGSPs need to ensure that their agent(s) or such other stakeholders duly attend to their responsibilities in this regard. This is essential to combat TF and PF activities by ensuring designated persons, organisations or countries are identified and prohibited from accessing any designated services while their assets are frozen without delay. The term Targeted Financial Sanctions (TFS) includes asset freezing without delay and prohibition from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

Screening against other designations lists such as OFAC, though not mandatorily required by domestic laws is very helpful in the overall risk management effectiveness. For any transactions or currency exchanges in USD for example, there is an inherent requirement to screen involved parties against the OFAC list. Similarly, when dealing in British Pounds or the Euro, screening against lists issued by such relevant authorities is an inherent requirement.

This section avails basic guidance on TFS. Casinos are required to further consider the detailed guidance around sanctions screening and TFS contained in Guidance Note 07 of 2023.

8.1 Effective Client Screening

In order to effectively implement TFS, Casinos must ensure:

a. sanction screening is performed on all clients before availing them services; and
b. no services are availed to clients before the sanction screening is completed and evidence of same has been documented. Screening should **not be undertaken after** availing services or facilitating transactions. Prior screening **enables proactive detection of sanctioned persons**. If such sanctioned persons are detected, such

lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter for purposes of combating the financing of terrorism and the funding of proliferation activities.

should not be granted access to any services at all and their attempted transactions should be reported to the FIC promptly and without delay, while the assets (or funds) involved are frozen or further transactions prohibited, as per the FIA and PACOTPAA. **In practice, policies and operating procedures therefore need to ensure clients are allowed to at least attempt the transaction to ensure due identification, which will enable effective screening and, if client is listed, eventual freezing of the funds which the client attempted to transact with, followed by complete prohibition to transact any further.**

The following databases of a Casino must be included in the screening process:

a. Existing customer databases. All systems (if any) containing customer data and transactions need to be mapped to the screening system to ensure full compliance;
b. Potential customers before conducting any transactions or entering a business relationship with any person;
c. Names of parties to any transactions (e.g., existing Casino client and new clients screened before account opening etc.[30]);
d. If known, names of individuals with direct or indirect relationships with them; and
e. If known, persons acting on behalf of customers (including those who may have pooled funds or availed funding to others who gamble on their behalf).

Casinos and OGSPs may consider using the screening tool availed by the FIC. It is important to first evaluate same and gain reasonable assurance that the screening mechanism to be employed would address its risk exposure, if not, employ other alternative screening measures to effectively mitigate this risk. Both ad-hoc and batch screening are permitted, depending on the risk. The FIC notes that screening is at times undertaken by the operational system as availed by the Casino or OGSP's partner/agent. The need to gain assurance that such screening tool is effective rests on the Casino and OGSP as Accountable and Reporting Institution.

[30] Other sectors such as Banks need to include agents, freight forwarders, vessels etc.

8.2 Where to find the updated Sanctions Lists?

Casinos, like all other Accountable and Reporting Institutions are required to access lists of sanctioned persons and screen their clients against such lists before establishing a business relationship and whenever the sanctions lists are updated. Domestically, at the time of issuing this Guidance, the NSC has not designated or listed any persons yet. At an international level however, the information on designated individuals, entities or groups in the Sanctions Lists is subject to change. The most recently updated sanctions list of the UNSC[31] can be found on the UNSC website or via the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

8.3 Targeted Financial Sanctions (TFS)

As mentioned above, the term Targeted Financial Sanctions includes **asset freezing without delay** and **prohibition** from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

8.3.1 Asset freezing without delay

In terms of international standards, without delay means **within a matter of hours[32]**. Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes:

a. The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access; and
b. The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

[31] The UNSC has a UN Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC.
[32] See findings on Namibia's 2022 Mutual Evaluation Report.

Examples of freezing:

i. ***Financial Institutions:*** *a freezing measure can be suspending listed client's access to bank accounts which have funds or blocking transactions which can deplete such;*

ii. ***DNFBPs like Casinos and OGSPs:*** *a freezing measure can be denial of further access to funds on client's Casino membership account or funds introduced in Casino one way or the other for the benefit of the client; and*

iii. ***VASPs[33]:*** *a freezing measure can be holding onto the funds/value from client (e.g in VASP's custody) to trade and transfer virtual assets, despite client having asked for same.*

8.3.2 Prohibition

Prohibition from making funds or other assets or services available: This means the prohibition to provide funds or other assets to or render financial or other services to, any designated individual, entity, or group.

Examples of prohibition:

i. ***Financial institutions:*** *prohibition from offering banking or transactional services which may undermine TFS objects;*

ii. ***DNFBPs, like Casinos and OGSPs:*** *prohibition from accessing or the provision of any Casino or gambling services etc., which can undermine TFS objects;*

iii. ***VASPs:*** *prohibition from the provision of any services, including but not limited to trading and transferring virtual assets.*

8.3.3 Object of freezing and prohibition

Note however that even when freezing measures are taken or implemented, there should be no restrictions on client introducing or depositing more funds with the Casino, provided they do not further gamble or deplete such. As long as the service which the listed client so desires cannot be finalised for them, prohibition and asset freezing requirements will be met on condition

[33] Virtual Asset Service Providers such as those dealing in Bitcoin etc.

whatever has already been frozen is not further depleted. The object remains to deprive listed/designated/proscribed persons from as much funds/assets as possible so they can be denied access to resources which may be used to fund terrorist or proliferation activities. This is the essence or primary goal of TFS measures. Casinos need to consider appropriate implementation given the circumstances they may find themselves in, with each transaction/client.

8.4 Reporting Possible Matches

As mentioned above, institutions should no longer report sanctions screening matches, TF or PF suspicions via STRs or SARs. New report types have been created to enhance effectiveness, especially around TFS measures. From 17 April 2023, sanctions screening matches as well as TF and PF suspicions or transactions should be reported as per below:

Reportable Activity or Transaction	Type of Report
Detection of a possible **sanctions screening match.**	SNMA - Sanction Name Match Activity report
Reporting any other **Activity** (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF.	TPFA - Terrorist & Proliferation Financing Activity report
Reporting any other **Transaction** (actual or completed transaction) which may point to, or be linked to potential terrorism, TF or PF.	TPFT- Terrorist & Proliferation Financing Transaction report

The mechanism to report any freezing or prohibition measures taken upon identifying confirmed or potential matches is through the goAML platform. The use of the goAML platform for TFS reporting purposes eases the burden of reporting and avails the necessary confidentiality required for this process. The following information must be shared when submitting a SNMA report:

a. The full name of the ‘confirmed match’. Attach identification documents of the ‘confirmed match’, such as passport or other ID documents for individual; and

b. Amount of funds or other assets frozen (e.g., value of funds wanted to transact with etc.). Attach proof documents such as internal Casino record showing the frozen funds, transaction receipts, etc., if such are at hand.

The mechanism to report any freezing or prohibition measures taken upon identifying confirmed or potential matches is through the goAML platform. The use of the goAML platform for TFS reporting purposes eases the burden of reporting and avails the necessary confidentiality required for this process.

Example:

A Casino identifies a confirmed match when screening clients upon account opening.

Person A is listed and is a prospective Casino client or approaches the Casino to access their services. The Casino must block the transaction immediately, refrain from offering any services to Person A, and submit a SNMA via goAML. The SNMA must include attachments that clarify:

a. *The value and location/placement of the funds client want to make use of (e.g in Cash brought to the Casino). Such cash should be seized, counted and placed beyond the reach of the client. Membership holders should be denied further access to funds on their membership accounts. For OGSPs, ensure to receive the funds in whatever format (account/online) and seize same or deny listed client access to such. When reporting, include supporting documents which indicates what was seized, who much and how or where it is kept;*
b. *ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.*

When a possible match is reported to the FIC, the FIC or such relevant competent authorities will direct all activities related to the frozen assets or funds. The Casino or OGSP may not release frozen assets or do anything related to such assets without being instructed to do so.

9. ROLE OF AML COMPLIANCE OFFICER

The effectiveness of the Compliance Officer[34] usually impacts an Accountable Institution's overall risk management level. The AML/CFT/CPF controls within a Casino or OGSP should therefore ensure the Compliance Officer is placed in a position to execute his/her FIA responsibilities as required. Such responsibilities primarily include ensuring that:

a. internal ML/TF/PF risk assessments are undertaken and results thereof duly implemented. Periodically, such risk assessments are duly revised or updated;
b. the AML/CFT/CPF Controls (policies, procedures etc) are at all times aligned to risk levels;
c. front-line staff (staff members who directly deal with customers) are duly trained on CDD measures as per the FIA;
d. he/she undertakes monitoring transactions, e.g. routine or spot checks;
e. measures to internally detect and escalate[35] potential ML/TF/PF indicators or red flags are prudent and enable the required level of confidentiality;
f. he/she files relevant reports with the FIC, without delay;
g. he/she regularly reports to senior management about AML/CFT performance; and
h. he/she attends to any other activities necessary to enhance FIA compliance.

Compliance Officers ought to have adequate managerial authority and capacity within an Accountable Institution to lead compliance activities, as per the FIA. Depending on the size of the Casino, volume of transactions etc., Management has a responsibility to ensure the Compliance function is able to duly execute on the FIA mandate.

[34] Appointed as per Section 39 of the FIA.
[35] To the Compliance Officer for analysis and decision on whether to report same to the FIC.

10. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of Casinos and OGSPs. Should an institution fail to adhere to the guidance provided herein, it will be such institution's responsibility to demonstrate alternative risk management controls implemented which are effective.

11. GENERAL

This document may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. This Guidance is issued without prejudice to the FIA and its complementing Regulations. The information contained in this document is intended to only provide a summary on these matters and is not intended to be comprehensive.

The Guidance Note can be accessed at www.fic.na

DATE ISSUED: 14 APRIL 2023
DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

FIC CONTACT DETAILS

All correspondence and enquiries must be directed to:
The Director, Financial Intelligence Centre
P.O. Box 2882
No. 71 Robert Mugabe Avenue, Windhoek
helpdesk@fic.na

ANNEXURE A: IDENTIFYING PEPs

Below is a list of persons who meet the description of a PEP[36], amongst others:

a) heads of state, heads of government, ministers and deputies, assistant ministers or senior politicians;
b) members of parliament or of similar legislative bodies;
c) secretary to cabinet or those holding such similar position;
d) members of the governing bodies of political parties;
e) significant, senior or important political party officials;
f) executive directors and their deputies (former Permanent Secretaries);
g) directors and their deputies in line ministries;
h) regional authority councillors as well as directors and their deputies;
i) local authority councillors as well as the executive management of local authorities;
j) senior executives of state-owned entities;
k) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
l) members of the boards of domestic or international banks and central banks;
m) ambassadors and members of management of embassies or similar bodies;
n) high-ranking officers in the armed forces and law enforcement, including prosecutorial services;
o) members of the management of supervisory bodies; and
p) directors, deputy directors and members of boards or equivalent function of an international organisation.

In particular, the following definitions, which do not cover middle ranking or junior staff in public functions, applies to the scope of people who meet the definition of PEPs:

[36] See Revised Guidance Note 01 of 2019.

i. **Foreign PEPs:** individuals who are or have been entrusted with prominent public functions by a foreign country;

ii. **Domestic PEPs:** individuals who are or have been entrusted domestically with prominent public functions;

iii. **International organisation PEPs:** persons who are or have been entrusted with a prominent function by an international organisation;

iv. **Family members:** individuals who are related to a PEP either directly or through marriage or similar (civil) forms of partnership; and

v. **Close associates:** individuals who are closely connected to a PEP, either socially or professionally. Close associates of PEPs means individuals who are closely connected to a PEP, either socially or professionally, and include but not limited to: individuals known to have any close business relationships with a PEP, such as the PEP's business partners or identified as the owners and/or beneficial owners of a legal person or legal arrangement which is associated with a PEP.