FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

PROVISIONS & GUIDELINES FOR GAMING SERVICE PROVIDERS (CASINOS AND LOTTERIES)

For implementation and interpretation of the National Ordinance Combatting Money Laundering and Financing of Terrorism

November 2024
Financial Intelligence Unit
Ministry of Justice
Sint Maarten

Contents

1 INTRODUCTION

1.1. Introduction

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the Ministers of its Member jurisdictions. These Member jurisdictions have committed themselves to endorse and fully implement the 40 Recommendations of the FATF for combating money laundering and the financing of terrorism and proliferation, using guidance and other policy endorsed by the FATF where appropriate.

The Caribbean Financial Action Task Force (CFATF) is designated by the FATF as a so-called FATF-style regional body (FSRB)[1], and is an Associate Member of the FATF. Country Sint Maarten is a member of the CFATF since May 2011.[2]

All CFATF members adhere to the FATF 40 Recommendations, which are internationally recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.[3] These standards cover all the measures that national systems should have in place within their criminal and regulatory systems. They further lay down the preventive measures to be taken by financial institutions and so-called Designated Non-Financial Businesses and Professions (DNFBPs).

The Financial Intelligence Unit-Sint Maarten (FIU Sint Maarten) has the legal authority to issue Provisions and Guidelines (P&G) for the DNFBPs comprising binding guidance on implementing the legal requirements for measures designed to deter, detect and disrupt money laundering and terrorism financing.

The FIU Sint Maarten is currently supervising the following DNFBPs:

> *Lawyers, (Candidate-)Notaries, Accountants; Tax Advisors; Administration Offices; Car Dealerships; Dealers in precious metals and jewels; Pawn-shops; Casinos and Lotteries, Real Estate Agencies; Appraisers; Project Developers, and all other persons and companies that provide the services pursuant to article 2, paragraph 1, under b of the National Ordinance Combatting Money Laundering and the Financing of Terrorism.* (*AB 2019, GT no. 25*)

This particular P&G applies to gaming service providers: casinos and lotteries. Casinos are divided in land based casinos and on-line casinos. For the services relevant to these providers, please be referred to paragraph 1.6.

Gaming service providers are by definition non-financial institutions. As part of the operation, gaming service providers offer gaming for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering and terrorist financing. Gaming service providers conduct financial activities similar to financial institutions including but not limited to accepting funds on account; debit card cashing facilities, safety deposit boxes. It is this routine exchange of cash for casino chips or plaques, as well as the provision of electronic transactions to and from casino deposit accounts and the movement of funds in and out of the financial sector, which makes gaming service providers an attractive target for those attempting to launder money and financing terrorism.

The Anti-Money Laundering (AML) legislation for Sint Maarten is laid down in the National

1 As the result of meetings of Member jurisdictions convened in Aruba in May 1990 and Jamaica in November 1992.
[2] www.cfatf-gafic.org
[3] See www.fatf-gafi.org

Ordinance Combatting Money Laundering and the Financing of Terrorism (NOCMLTF).

The NOCMLTF regards both financial as non-financial services. In order to prevent the gaming service providers from being abused for money laundering activities or the financing of terrorism, the NOCMLTF specifies that the gaming service providers must identify their customer and the 'Ultimate Beneficial Owner' (UBO) before providing a service to the customer or UBO. After the gaming service providers have entered into a business relationship, the gaming service providers will continue applying Customer Due Diligence (CDD) to their customers. Furthermore, pursuant to the NOCMLTF, the gaming service providers are obliged to report unusual transactions to the Financial Intelligence Unit-Sint Maarten (FIU Sint Maarten).

Apart from the identification of the customer and UBO and reporting unusual transactions, the gaming service providers must take a risk based approach (RBA) when providing services. Furthermore, the gaming service providers must keep records for the period of ten (10) years after terminiation of the relationship with their customers.

As supervisor of the designated DNFBPs, the FIU Sint Maarten pays utmost attention to the reliability and timeliness of the information provided in this document. However, please note that the contents of this P&G are subject to change, based on the dynamic FATF recommendations and the policies applied by the FIU Sint Maarten. It is also advisable to regularly visit the website of the Sint Maarten FIU (http://www.fiu-sxm.net) to keep abreast of the latest developments or amendments to this P&G, as well as other documents in the field of combatting money laundering and the financing of terrorism.

1.2 Money laundering

Money laundering is rendered a criminal offence pursuant to the Criminal Code of Sint Maarten (AB 2019, no. 41) in articles 2:404 (intentional money laundering), 2:405 (habitual money laundering) and 2:406 (money laundering through default).

Money laundering is the attempt to conceal or disguise the source of illegally obtained money, thus integrating it into the legal economy in order to create a legal status for the criminal assets. This way the origin of the illegal money becomes seemingly legitimate. Generally, the process of money laundering comprises three (3) stages:

(1) Placement

During the first stage of money laundering the launderer introduces the illegal monies into the financial system. This might be done for example by breaking up large amounts of cash into less conspicuous smaller amounts that are then deposited directly into a bank account or by purchasing a series of monetary instruments (money orders, etc.).

(2) Layering

After the funds have entered the financial system, the second – or layering – stage takes place. The illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the origin of the money. The intention of this phase is to break the 'paper trail'. The launderer engages for example in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is prevalent in most countries and not only in those jurisdictions that do not follow the FATF 40 Recommendations.

(3) Integration

Integration is the provision of apparent legitimacy to benefits of criminal conduct. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. The launderer might choose to invest the funds into real estate, luxury assets (cars, yachts, art or jewellery) or business ventures.

1.3 Financing of terrorism

Pursuant to Art. 2:408 of the Criminal Code of Sint Maarten (AB 2019, no. 41) terrorism financing constitutes a criminal offense on Sint Maarten. Terrorism financing is a means of providing funding for terrorist activities. It may involve funds raised from criminal or even legitimate sources. Terrorism financing is used to support terrorist movements financially in the broadest sense of the word.

Terrorism can be defined as the use or threat of action designed to influence government or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

International experience shows that terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the UBOs of the funds.

Financial transactions associated with terrorist financing tend to be in smaller amounts. When terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

International experience also shows that that to move their funds, terrorists for example use the formal banking system, informal value-transfer systems (e.g. Hawalas and Hundis) and, the oldest method of asset-transfer, the physical transportation of cash, gold and other valuables through smuggling routes.

1.4 Risk-Based approach (RBA)

The AML/CFT framework creates an obligation for the gaming service providers to apply a risk-based approach (RBA) when establishing and continuing a service relationship with a customer. The gaming service providers bear the responsibility and legal obligation to undertake this risk assessment before establishing and when continuing a service relation with their customer. The risk assessment is formalized in a Customer Due Diligence (CDD) which, depending on the risk (e.g. type of customer, product, transaction, geographical region, business relation) must be carried out in a standard, simplified or enhanced form.

The FIU Sint Maarten has the legal authority to supervise compliance with the risk assessment by the gaming service providers. This P&G offers guidance, among other things, on how to apply the RBA approach. It is up to the gaming service providers to develop internal compliance policies and procedures in order to be able to fulfil their legal obligations.

1.5 Provisions and Guidelines (P&G)

The AML/CFT framework for the financial sector constitutes the National Ordinances and executive decrees, regulations, provisions and guidelines (P&Gs).

Pursuant to Art. 31 (2) of the NOCMLTF, and Art. 2 (5) of the National Ordinance Financial Intelligence Unit (NOFIU), the FIU Sint Maarten has the legal authority to issue binding guidelines. The purpose of this P&G is to provide all DNFBPs that are supervised by the FIU Sint Maarten with

comprehensive guidance on implementing the legal requirements for measures designed to deter, detect and disrupt money laundering and terrorism financing.

The P&G gives guidance on:

- outlining and explaining the legislation on anti-money laundering (AML) and combatting terrorist financing (CFT) measures, relevant for the supervisory task of the FIU Sint Maarten.
- Risk assessment and Customer Due Diligence.
- Reporting of unusual transactions.
- Recordkeeping.
- Setting up a compliance regime.
- Outlining the enforcement and supervisory measures.

Failure to comply with the AML/CFT framework may result in administrative sanctions (e.g. penalty payments or fines)[4] being imposed on the gaming service providers. Furthermore, an intentional or unintentional breach of the AML/CFT framework is considered an offence respectively a misdemeanor which can result in criminal sanctions (imprisonment or a fine) being imposed on the gaming service providers. Information on the legal procedure and enforcement of the legislation and this P&G will be given in Chapter 6.

1.6 Who need to comply with the P&G?

The duty to perform CDD and the reporting obligation is applicable to the gaming service providers who, in or from Sint Maarten, renders a service as a profession or as a trade, as mentioned in Art. 2 (1), under b, sub 4° of the NOCMLTF.

The services comprise the provision of the opportunity to participate in:

a. games of chance as referred to in the National Ordinance Games of Chance;
b. games of chance as referred to in the National Ordinance Offshore Games of Chance; or,
c. a lottery as referred to in the Lottery Ordinance.

1.7 Duty to register

Gaming service providers have a duty to register at the FIU Sint Maarten pursuant to Art. 26 (1) of the NOCMLTF. The registration at the FIU Sint Maarten must be carried out immediately after the gaming service providers have registered their company at the Chamber of Commerce & Industry, based on the services as mentioned in Art. 2 of the NOCMLTF.

1.8 Organizational changes

The registration entails the record of the details of the organization such as the legal name of the company, the organizational structure, the address, phone numbers, and the names of the company representatives. If at any point in time, there are changes made in the organizational structure or within the organization, then this amendment must be communicated to the FIU Sint Maarten by filling out the Organizational Change Form. Please be referred to Template 1.

[4] See Art. 31 (3) of the National Ordinance Combatting Money Laundering and the Financing of Terrorism, and Art. 19 of the National Ordinance Financial Intelligence Unit.

2 CUSTOMER DUE DILLIGENCE

2.1 Introduction

Pursuant to Art. 20 of the NOCMLTF, gaming service providers are obliged to identify and assess their vulnerability to money laundering and, using a risk-based approach, to mitigate this vulnerability effectively. Gaming service providers shall implement an adequate policy as well as compile written procedures and measures, which focus on preventing combating money laundering and the financing of terrorism. If higher risk is identified, the gaming service providers and their employees should take enhanced measures to manage and mitigate the risks. Furthermore, Art. 20 (3) of the NOCMLTF indicates that gaming service providers shall implement an adequate policy and have adequate procedures which focus on preventing the abuse of new technological developments, new products, new business practices and instruments for the benefit of money laundering and the financing of terrorism. The procedures referred to in the first complete sentence, also relate to risk assessment prior to launch of the new products and business.

The senior management of the gaming service providers shall approve the policies, controls and procedures that is put in place and monitor this and, where appropriate, enhance the measures taken. Senior management refers to individuals at the highest level of organizational management within the company who have the day-to-day responsibilities of managing the business.

Periodically, gaming service providers shall have an independent evaluation performed of the procedures and measures in order to be able to assess whether, and to what extent, they are vulnerable to money laundering and the financing of terrorism. It is assumed that the independent evaluation will be conducted by a qualified assessor. The findings of the periodic evaluations, referred to in paragraph 5, shall be recorded in writing and a copy sent to the FIU Sint Maarten.

2.2 The scope of Customer Due Diligence (CDD)

Pursuant to Art. 3 (2) of the NOCMLTF, in the following situations, gaming service providers conduct CDD, when:

a. in or from Sint Maarten, it enters into a business relationship;
(…)
c. it relates to games of chance as referred to in the National Ordinance Games of Chance, the National Ordinance Offshore Games of Chance or the Lottery Ordinance whereby transactions in excess of an amount of NAf 5,000. -- are paid for using cash, electronically or by means or other payment systems;
(…)
f. there is any suspicion that the customer is involved in money laundering or the financing of terrorism;
g. there are any doubts about the validity or reliability of data previously obtained from the customer; or
h. there is any risk of an existing customer being involved in money laundering or the financing of terrorism.

Art. 3 (3) of the NOCMLTF states that taking account of Arts. 3, 6 and 10 of the NOCMFT, gaming service providers shall match their CDD to the risk sensitivity of money laundering and the financing of terrorism. To this end they shall compile a risk profile of the customer and the UBO.

Art. 3 (4) of the NOCMLTF states that by means of a ministerial regulation, rules can be drawn up concerning the execution of monetary transfers specifically including the data and information that

has to be recorded in respect of the party that has made the funds or monetary instruments available to the gaming service providers within the context of a monetary transfer as well as that of the beneficiary of the transaction.

2.3 The moment of performance of the Customer Due Diligence (CDD)

Pursuant to Art. 4 (1) of the NOCMLTF, gaming service providers perform CDD:

a. before commencing the procedure for entering into a business relationship; and,
b. each time before an incidental transaction as referred to in Art. 3 (1), under b or c, or a transaction as referred to in Art. 3 (2), under b to f, is carried out if there is a suspicion of money laundering or terrorist financing.

Art. 4 (2) of the NOCMLTF states that, notwithstanding the first paragraph:

a. gaming service providers verify the identity of the customer and the beneficial owner during the procedure for establishing the business relationship, if this is necessary in order not to disrupt the service provision and there is little risk of money laundering or terrorist financing. In that case, the gaming service providers verify the identity as soon as possible after the establishment of the business relationship with the customer;

Pursuant to Art. 5 (1) of the NOCMLTF gaming service providers are prohibited from having anonymous accounts or accounts in unmistakably fictitious names.

Pursuant to Art. 5 (2) of the NOCMLTF without prejudice to Art. 4 (2) of the NOCMLTF gaming service providers are prohibited from entering into a business relationship or executing a transaction if they have not conducted CDD, or are unable to conduct CDD, until the result envisaged in Arts. 3, 7 and 8 of the NOCMFT.

Pursuant to Art. 5 (3) of the NOCMLTF gaming service providers collect sufficient data and conduct periodic investigations, based on relative importance and risks in order to determine whether the risk profile of their customer needs to be changed.

Pursuant to Art. 5 (4) of the NOCMLTF, if gaming service providers after entering into a business relationship can no longer comply with Arts. 3, 7 and 8 of the NOCMFT, they will terminate without delay this business relationship.

2.4 Special regulations regarding the scope of CDD

Pursuant to Art. 6 (1) of the NOCMLTF:
By way of derogation from Art. 4 (1), gaming service providers may apply a simplified CDD with regard to the requirements set out in Arts. 3, 7 and 8:

(…)
b. if a gaming service provider executes a transaction or enters into a business relationship with regard to:
    (…)
    3º. beneficial owners in accounts held by a gaming service providers that are used exclusively for holding third party funds, provided that such service provider is subject to anti-money laundering and anti-terrorist financing regulations that meet internationally accepted standards for the prevention and money laundering and terrorist financing and be

under effective supervision of compliance with those standards;

Pursuant to Art. 6 (2) of the NOCMLTF a simplified CDD shall in any case include identification and determination as referred to in Art. 7 (1), under a, b, c and e.

Pursuant to Art. 6 (3) of the NOCMLTF gaming service providers collect sufficient data and carries out periodic surveys to determine whether the first paragraph applies to a customer.

Pursuant to Art. 6 (4) of the NOCMLTF the first paragraph does not apply if the customer, business relationship or transaction entails a higher risk of money laundering or terrorist financing, or if there are indications that the customer is involved in money laundering or terrorist financing.

2.4.1 Standard Customer Due Diligence (CDD)

Pursuant to Art. 7 (1) of the NOCMLTF, to prevent and combat money laundering or the financing of terrorism, gaming service providers shall conduct standard CDD which shall, at least, include the following:

a. the identification of the customer and the verification of the customer's identity;
b. the identification of the ultimate beneficiary and taking reasonable measures to verify the identity of the ultimate beneficiary in such a way that the gaming service provider is convinced of the identity of the ultimate beneficiary;
c. measures to establish the objective and the envisaged nature of the business relationship;
d. conducting ongoing checks of the business relationship and the transactions carried out during this relationship, in order to ensure these correspond to the knowledge the gaming service provider has of the customer, his/her/its business and the ultimate beneficiary, as well as their risk profiles, including, if necessary, the origin of the financial resources; and,
e. measures to establish whether a customer is acting for him/her/itself or on behalf of a third party and taking measures to establish and verify the identity of the third party.

Identification natural person:
Art. 7 (3) of the NOCMLTF states that the data and information, referred to in paragraphs 1 and 2, which form part of CDD, shall at least include the following:

a. in respect of natural persons:
    1°. the surnames, the first names, the place and date of birth, the address of the place of residence or domicile of the customer and the ultimate beneficiary, as well as anyone who acts on behalf of these natural persons or a copy of the document containing a personal identification number on the basis of which their identification was confirmed;
    2°. the nature, number, date and place of issue of the document used to verify the identity;
    3°. the nature and date of the transaction;
    4°. the type of currency and the amount involved in the transaction;
    5°. the type and number of the bank account used in the transaction; and,
    6°. all the bank statements and business-related correspondence.

Identification legal entities:
Art. 7 (3), under b of the NOCMLTF states in respect of legal entities:

1°. the legal form, the deed of incorporation, the Articles of Association, the trade name, the address and, if the legal entity is registered with the Chamber of Commerce & Industry, its registration number at the Chamber of Commerce & Industry, as well as the way in which its identity has been verified by a reliable and independent source;

2°. the surnames, first names, places and dates of birth of those who hold executive positions, those who act on behalf of the legal entity, the ultimate beneficiary, or those who have effective control of the legal entity, as well as the way in which these identities have been verified by a reliable and independent source; and,

3°. the data referred to under a, parts 3° to 6°.

Pursuant to Art. 7 (4) of the NOCMLTF if the customer or the owner of the controlling interest is a listed company and is subject to rules concerning the publication of information which guarantees transparency in respect of the economic ownership, or is a subsidiary of such a company, the provisions of this article in respect of establishing and verifying identity are not applicable to the shareholders or ultimate beneficiaries of such a company.

Pursuant to Art. 7 (5) of the NOCMLTF the provisions in paragraphs 2, 3 and 4 apply accordingly to any party claiming to act on behalf of the customer.

2.4.2 Third party

Gaming service providers are obliged to inquire whether the natural person is acting on his own behalf or is acting as an (duly authorized) agent on behalf of a third party. In terms of Art. 7 (1), under e and Art. 8 of the NOCMLTF, the gaming service providers must take reasonable steps to confirm the identity of the third party:

1. If a customer is a legal entity or a legal construct, the gaming service providers shall check whether the natural person who proposes to act on behalf of the customer is authorized to do so; furthermore, the gaming service providers shall establish the identity of the natural person and verify this identity before it provides the service; the gaming service providers shall also record details pertaining to the customer's legal form and representation.
2. In respect of a customer, as referred to in paragraph 1, gaming service providers shall take reasonable measures which, at a minimum, result in the service provider gaining insight into the ownership and actual control structure of that customer.

2.4.3 Data collected

Pursuant to Art. 9 of the NOCMLTF:

1. Gaming service providers are responsible for ensuring that the data and information which is obtained in the context of CDD, in particular data and information related to customers, ultimate beneficiaries or business relationships which pose a higher risk of money laundering and the financing of terrorism are updated and relevant.
2. If gaming service providers reasonably take the view that the CDD process may warn a customer or prospective customer then, having collected data from which the identity of the

customer or prospective customer can reasonably be deduced, the gaming service providers may decide not to pursue the due diligence inquiries any further but to submit a report of a suspicious transaction.

3. Gaming service providers are responsible for ensuring its employees are familiar with, and sensitive to, the risk that a customer or prospective customer could be warned by or during the CDD process.

2.4.4 Enhanced Customer Due Diligence (CDD)

Pursuant to Art. 10 of the NOCMLTF, if there is an increased risk of money laundering or terrorism financing, gaming service providers are obliged to perform an enhanced CDD:

1. Gaming service providers shall conduct if, and depending on whether, the nature of a business relationship or transaction carries a higher risk of money laundering and the financing of terrorism.
2. Enhanced CDD, as referred to in paragraph 1, should be carried out before the business relationship is entered into or the transaction executed, as well as during the business relationship, if it relates to:
    a. a customer that is not a resident of Sint Maarten, respectively not based in Sint Maarten;
    b. a customer that is not physically available to be identified;
    c. a complex, unusually large transaction;
    d. a transaction without a clear economic or legal purpose;
    e. private asset management for the benefit of high-net-worth natural persons;
    f. legal entities, trusts or comparable entities which are intended for the placement of personal assets;
    g. companies and comparable entities in which the shares have been converted into bearer shares or are registered shares held for the benefit of a third party;
    h. natural persons, legal entities, trusts and comparable entities which are registered or based in a country or jurisdiction which does not, or does not sufficiently, comply with internationally accepted standards for the prevention and combatting of money laundering and the financing of terrorism;
    i. Politically Exposed Persons;
    j. entering into correspondent bank relationships;
    k. a customer or transaction which is subject to a restriction on the basis of the National sanction ordinance;
    l. if one or more of the details referred to in Art. 22 (1) are missing.

(...)

4. At a minimum, enhanced CDD shall consist of standard CDD, as referred to in Art. 7 (1), supplemented with:
    a. additional information about the customer and the ultimate beneficiary;
    b. additional information about the intended nature of the business relationship;
    c. information about the source of the customer's funds or assets;
    d. information about the reasons for transactions, both intended and completed;
    e. approval from the board for entering into or continuing the business

relationship;

f. enhanced supervision of the business relationship by revising the number and timing of the checks, and selecting transaction patterns which require more extensive investigation;

g. the requirement that the first payment is executed through an account in the customer's name at a bank which has conducted the same level of CDD.

2.4.5 Politically Exposed Persons (PEP)

Pursuant to Art. 11 of the NOCMLTF:

1. Gaming service providers shall conduct an adequate policy and have risk assessment procedures to establish whether a customer, a prospective customer, an ultimate beneficiary or a beneficiary of a life insurance policy is a Politically Exposed Person. Moreover, gaming service providers shall have procedures to enable them to establish the origins of the assets and bank balances of their customers and the ultimate beneficiaries who, on the basis of the first complete sentence, are designated Politically Exposed Persons.
2. Without prejudice to the provision in paragraph 3, gaming service providers which enter into a business relationship with, or executes a transaction for, a Politically Exposed Persons is responsible for ensuring that:
   a. the decision to enter into the business relationship, or execute an individual transaction, is only taken or approved by persons who are in overall charge of the gaming service providers;
   b. there is ongoing supervision of the business relationship.
3. If, after a business relationship has been entered into, a customer or ultimate beneficiary is designated a Politically Exposed Persons, the business relationship shall only be maintained after it has been approved by persons who are in overall charge of the gaming service providers.
4. For two years after a customer, prospective customer or ultimate beneficiary has ceased to hold a prominent public office, he/she shall still be designated a Politically Exposed Persons. The first complete sentence applies accordingly to family members and relations.

2.4.6 National/geographical indicators

Pursuant to Art. 12 of the NOCMLTF, gaming service providers shall pay specific attention to the national/geographical risk analysis as follow:

1. Gaming service providers shall pay specific attention to:
   a. business relationships and transactions with natural persons, legal entities and trusts which are registered or based in a country or jurisdiction which does not, or does not sufficiently, comply with internationally accepted standards for the prevention and combatting of money laundering and the financing of terrorism; and
   b. all complex and unusual transactions and all unusual features of transactions which have no explicable economic or legal purpose.
2. If gaming service providers have reasonable suspicions that a transaction with a natural person, legal entity or a trust, registered or based in a country or jurisdiction as referred to in paragraph 1, under a, has no explicable

economic or legal purpose, or if it relates to a transaction as referred to in paragraph 1, under b, the gaming service providers should investigate the background and purpose of the transaction and record the findings in writing.

3. The findings referred to in paragraph 2 should be retained for at least ten years.

Other reliable sources that can be consulted in this regard are the Office of Foreign Asset Control (OFAC) www.treas.gov/ofac for information relating to the extraterritorial effect of targeted financial sanctions of the United States (in case of a nexus). The IMF, the World Bank and the Organisation for Economic Cooperation and Development (OECD) can also be classified as being reliable sources.

2.5 The introduction of customers

Pursuant to Art. 13 of the NOCMLTF, without prejudice to their own responsibility as referred to in Art. 7 (1), under a, b and c, gaming service providers may, by way of derogation from Art. 5 (2), approach a customer who is introduced by a service provider established in Sint Maarten. On the CDD performed by that service provider, insofar as this examination comprises the elements described in Art. 7 (1), under a, b and c, provided that:

a. the gaming service providers ascertain that copies of all data and information relating to the CDD performed by the third party as referred to in the opening lines can be made available to him by the third party without delay at the request of the gaming service provider; and,
b. the gaming service providers ascertain that the third party has procedures and measures that enable the third party to perform a CDD and to keep the data and information obtained as a result of that CDD in the manner referred to in Chapter IV.

Pursuant to Art. 14 of the NOCMLTF:

1. Art. 13 does not apply to customers introduced by service providers established outside Sint Maarten who are established in a country or jurisdiction that does not or insufficiently complies with internationally accepted standards in the field of preventing and combatting money laundering and terrorist financing.
2. In the application of Arts. 10 (2), under h, 12 (1), under a, and second paragraph, 14 (1), and 19, second and third paragraphs, a country or jurisdiction shall be deemed in any case not or fail to meet internationally accepted standards for the prevention and combatting of money laundering and terrorist financing if the country or jurisdiction is on the list of High Risk and non-cooperative jurisdictions published on the FATF-website.

2.6 Verification of documents, data and information

Pursuant to Art. 17 of the NOCMLTF:

1. If a customer is a natural person, his/her identity shall be verified on the basis of reliable and independent documents, data or information.
2. If a customer is a legal entity under the laws of Sint Maarten and its registered office is in Sint Maarten or it is a foreign legal entity based in Sint Maarten, its identity shall be verified on the basis of documents, data or information from a reliable and independent source.
3. If a customer is a foreign legal entity not based in Sint Maarten, its identity shall

be verified on the basis of reliable and internationally accepted documents, data or information or on the basis of documents, data or information which, by statutory provision, are recognized as a valid means of identification in the customer's country of origin.

4. (…)
5. gaming service providers shall verify the identity of the ultimate beneficiary on the basis of reliable and internationally accepted documents, data or information or on the basis of documents, data or information which, by statutory provision, are recognized as a valid means of identification in the ultimate beneficiary's country of origin, and in such a way that the gaming service providers are convinced of the identity of the ultimate beneficiary.
6. The gaming service providers shall copy all the documents referred to in the paragraphs 1 to 5.
7. If gaming service providers reasonably take the view that making a copy, as referred to in paragraph 6, may warn a customer or prospective customer then, instead of making copies, the gaming service providers may decide that it is sufficient to gather data from which the identity of the customer or prospective customer can reasonably be deduced.

2.7 Procedures and measures to prevent and control ML/TF

Pursuant to Art. 18 (3) of the NOCMLTF:

1. The Minister shall establish a national policy to promote transparency, integrity and public trust in the governance and management of all non-profit organizations, as well as national policies to prevent or reduce money laundering and terrorist financing, based on the identified risks.
2. The policy is aimed at, among other things, that policymakers, the FIU Sint Maarten, the investigative authorities, supervisors and other relevant competent authorities at the level of policy-making and operational implementation have effective mechanisms that enable them to cooperate, money laundering and terrorist financing of various types of organizations established in Sint Maarten assess legal entities and coordinate the development and implementation of policies and activities against money laundering, terrorist financing and the proliferation of weapons of mass destruction where appropriate.
3. The policy is reassessed every ten (10) years, adjusted if necessary, and re-adopted.
4. The Minister of Justice takes into account the advice referred to in Art. 3 (2), under k and l, of the NOFIU.

2.7.1 Risk Based Approach (RBA) Customer Due Diligence (CDD)

The purpose of the risk based CDD is to recognize and manage the risks of money laundering and terrorism financing when providing services. Executing a risk based CDD should give the gaming service providers a profounder understanding of the identity of the customer or the UBO[5] with

[5] UBO is described as follows in terms of Art. 1, under ee, of the National Ordinance Combatting Money Laundering and the Financing of Terrorism. The UBO is a natural person has interest of more than 25% of capital, or can exercise more than 25% of the customer's voting rights at a shareholder's meeting, or in some other way can exercise effective control in or on behalf of the customer; is the beneficiary of 25% or more of the capital in a legal construction, including a foundation or a trust, or can exercise effective control in the legal construction; or has control over 25% or more of a customer's capital.

whom they are doing business. The CDD includes identifying and verifying the customer or the UBO, if applicable, as well as taking other appropriate measures. The CDD measures are based on FATF Rec. 22 in conjunction with FATF Rec. 10.

This is included in Art. 3 of the NOCMLTF (see paragraph 2.4 CDD).

The CDD does not only apply to new customers but also to existing customers. The application of the CDD to existing customers should also be risk based. The CDD requirements are on the basis of materiality (for example if the gaming service providers already dispose of relevant and valid CDD information there is no need to request this information once again) and should be conducted at appropriate times.

2.7.2 Risk Assessment

A risk based approach (RBA) starts with the identification of the customer and an assessment of risks that have to be managed. Risk should be assessed in relation to customers, products and services, delivery channels and geographic areas of operation. Template 2 and 3 provide a template for a risk assessment that gaming service providers may find useful.

2.7.3 Moment of risk assessment

Risk assessments have to be performed throughout the course of business with the customer and vendors but in any case, a risk assessment should be performed at least once a year.

For High Risk 1 year, Medium Risk 2 years and Low Risk 3 years.

The gaming service providers must keep records.

Please be referred to Annex 1 and Annex 2 for specific Risk categories and Risk factors.

2.7.4 Specific Money Laundering/Terrorist Financing red flags for the Gaming service providers

There are numerous red flags, which may assist you to identify potential money laundering or terrorism financing activities. Although the existence of a single indicator does not necessarily indicate illicit activity, it should encourage further monitoring and examination. In most cases, it is the existence of multiple red flags, which raises a reporting entity's suspicion of potential criminal activity, and triggers their response to the situation. Directors and Senior Management of gaming service providers should include these money laundering/terrorism financing red flags in staff training and encourage their staff to use these red flags when describing suspicious behaviors for inclusion in suspicious matter reports submitted to the FIU Sint Maarten.

ML/TF red flags for the Gaming service providers

The list below features some of the major red flags of money laundering and terrorist financing for the gaming service providers and should be treated as a non-exhaustive guide:

i. Any gaming service provider transaction where an individual receives payment made out to third parties or without a specified payee;
ii. Customer requests a winnings voucher in a third party's name;
iii. Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party;
iv. Multiple vouchers being requested or drawn on account;
v. High volume of transactions within a short period;
vi. Multiple chip cash outs on the same day;
vii. Chip cash out is same/similar to chip purchase;
viii. Requests for credit transfers to other gaming service providers;
ix. Customer attempts to avoid the filing of a report for cash transactions by breaking up the transaction;
x. Customer requests vouchers that are not for gaming winnings;
xi. Customer enquiries about opening an account with the gaming service providers and the ability to transfer the funds to other locations when you do not know the customer as a regular, frequent or large volume player;
xii. Customers claiming a high level of gaming machine payouts;
xiii. Supposed winnings do not correspond with recorded winnings;
xiv. Dramatic or rapid increase in size and frequency of transactions for regular account holder;
xv. Detection of chips brought into the casino;
xvi. Customer purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a gaming service provider voucher;
xvii. Customer in possession of large amounts of currency or bills;
xviii. Customer be friending/attempting to befriend casino employees;
xix. Customer puts money into slot machines and claims accumulated credits as a jackpot win;
xx. Customer exchanges small denomination bank notes for large denomination bank notes, or chip purchase vouchers;
xxi. Customer is known to use multiple names to conduct an activity;
xxii. Customer requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is no effective anti-money-laundering system;
xxiii. Inserting funds into gaming machines and immediately claiming those funds as credits;
xxiv. Customer claiming gaming machine credits/payouts with no jackpot;
xxv. Accumulating gaming credits with minimal play;
xxvi. Customer's intention to win is absent or secondary;
xxvii. Two or more customers frequently wagering against one another on even-money games;

xxviii. Purchasing and cashing out casino chips with little or no gaming activity;
xxix. Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single voucher;
xxx. Use of third parties to purchase casino chips;
xxxi. Use of credit cards to purchase casino chips;
xxxii. Customer due diligence challenges, e.g. refusals, false documents;
xxxiii. Customer purchases chips and leaves casino shortly after;
xxxiv. Large chip purchases;
xxxv. Frequent purchase of gaming service provider gift certificates;
xxxvi. Unexplained income inconsistent with financial situation/customer profile.

2.8 Foreign branches, or subsidiaries and compliance with legislation in host states

Pursuant to Art. 19 (1) of the NOCMLTF, gaming service providers with a branch or subsidiary outside Sint Maarten shall be responsible for ensuring that, at a minimum, the branch, respectively the subsidiary, applies internationally accepted standards (FATF Recommendations) for the prevention and combatting of money laundering and the financing of terrorism. Gaming service providers are required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations.

Gaming service providers are required to inform the FIU Sint Maarten when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (i.e., host country) laws, regulations, or other measures. Group-level compliance, audit or AML/CFT functions should be provided with customer, account and transaction information from branches and subsidiaries when necessary for the AML/CFT purposes. This means that in case of a group of branches the relevant AML/CFT information should be exchanged between the central compliance office and the branches.

3 COMPLIANCE REGIME

Pursuant to Art. 20 (1) of the NOCMLTF, gaming service providers are obligated to identify and assess its vulnerability to money laundering and terrorist financing, and to combat it effectively using a risk-based approach.

Pursuant to Art. 20 (2) of the NOCMLTF, gaming service providers pursue an adequate policy and have documented procedures and measures aimed at preventing and combatting money laundering and terrorist financing, in particular the application of Chapters II, III, IV, V and VI of this national ordinance. An adequate policy as referred to in the first sentence means, among other things, that if higher risks are recognized, the gaming service providers and their staff take stricter measures to control and limit the risks.

The senior management shall approve the Compliance regime, which consist of policies, controls and procedures that is put in place and monitor this and, where appropriate, enhance the measures taken. Senior management refers to individuals at the highest level of organizational management within the company who have the day-to-day responsibilities of managing the business.

3.1 Compliance policy and internal procedures

A well-designed, applied and monitored regime will provide a solid foundation for compliance with legislation. Not all individuals and entities operate under the same circumstances; hence, the compliance regime will have to be tailored to fit the gaming service providers' individual needs. The degree of detail of the compliance policy and procedures depends in part on the nature, size, complexity of the commercial activities, and the risk of exposure to money laundering and terrorism financing. A risk based compliance policy should preferably be tailor-made according to the typical customer and services of the institution in which the services are provided.

Pursuant to Art. 20 (3) of the NOCMLTF, gaming service providers pursue an adequate policy and have adequate procedures aimed at preventing the misuse of new technological developments, new products, new business practices and tools for money laundering and terrorist financing. The procedures referred to in the first sentence also relate to the risk assessment prior to the introduction of new products and business practices and the application of new or developing technologies.

The FIU Sint Maarten has also drafted a template that can be used to set up a compliance policy. Please request the FIU Sint Maarten to send you the latest version. A compliance policy should cover at least the following aspects:

- a commitment of the gaming service providers to abide by the AML/CFT framework.
- Customer Due Diligence: policy on acceptable identification and verification.
- assessing business relationship with the customer and in case of variations on CDD what measures the service provider will take.
- on-going monitoring procedures.
- internal controls and communication (staff, compliance officer and senior management).
- monitoring and managing of compliance with legislation.
- suspicious and/or unusual transaction reporting.
- record keeping of information.
- training of staff.
- the role of the Compliance Officer.
- periodical reviewing of procedures.

In the compliance policy, internal procedures regarding risk based CDD and reporting of unusual

transactions need to be established. Annex 3 of this P&G provides some guidelines for an internal compliance policy and risk assessment that gaming service providers may find useful.

Change of various factors may bring along that the gaming service providers' compliance policy and internal procedures have to be adapted from time to time. These changes might e.g. include legislative adaptations or the provision of new services or products by the gaming service providers. The policies and procedures should be regularly evaluated. If after the evaluation it is concluded that that they are not functional, they should be amended.

3.1.1 Independent Evaluation

Pursuant to Art. 20 (4) of the NOCMLTF, the identification and assessment, referred to paragraph 1, and the procedures and measures, referred to in paragraphs 2 and 3, shall at all times relate to the gaming service providers' internal organization and internal audits, as well as to the employment, function changes, background, education, information provision and ongoing training of the relevant personnel and the application of CDD, the recording of data and information, the internal decision-making process for the submission of reports, as well as to the periodic evaluation of the effectiveness of these procedures and measures.

Pursuant to Art. 20 (5) of the NOCMLTF and to FATF Rec. 18, gaming service providers shall periodically conduct reviews of procedures and measures in order to assess whether and to what extent they are vulnerable to money laundering or terrorist financing as a result of their activities and activities and shall submit them to an independent audit.

Such an evaluation should take place at least every three (3) years. The evaluation must be documented (a written report), including a follow-up plan depending on the outcome of the evaluation. The evaluation is necessary to ensure that the quality of the compliance regime of the gaming service providers is assured. An evaluation should at least cover the effectiveness of the compliance policy and procedures, determine the functioning of the Compliance Officer and evaluate the training program (Please be referred to the guideline in this regard in Annex 4).

An evaluation of this sort has a practical component. Its goal is to verify whether all staff is working in line with the compliance policies and procedures. If this is not the case, compliance policies and procedures should be amended as soon as possible. The results of an evaluation should be recorded in writing and submitted to the gaming service providers' management with the request to adopt corrective measures on a swift base.

The evaluation should be done by an external party that is not involved in the day to day business of the gaming service providers. In any case, the gaming service providers can take on an AML/CFT professional firm or person to perform an independent evaluation of the compliance regime.

Pursuant to Art. 20 (6) of the NOCMLTF, these findings of the periodic evaluations, shall be recorded in writing and a copy sent to the FIU Sint Maarten.

3.2 Setting up an on-going training programme

Pursuant to Art. 21 (1) of the NOCMLTF, gaming service providers are responsible for ensuring that, to the extent relevant for the performance of their duties, their employees are familiar with the provisions of these national ordinances and follow periodic education and training courses which enable them to recognize unusual transactions.

The training program should be documented and should, at least, cover:

- general information about money laundering and terrorism financing.

- an explanation of the legal and regulatory framework of Sint Maarten and an indication of expected developments.
- the sanctions that can be imposed if a gaming service provider violates the AML/CFT framework.
- the identity, tasks and responsibilities of the Compliance Officer.
- the potential effect of any breach of the law on the business, its employees and its customers.
- the risks of money laundering and terrorism financing that the business faces.
- the vulnerabilities of the business' products and services.
- new technologies with regards to money laundering and terrorism financing.
- the policies, (identification and verification of customer) procedures and controls that have been put in place to reduce and manage the risks.
- risk based CDD measures.
- how to recognise unusual transactions and potential suspicious activity.
- the procedures for making a report to the Compliance Officer including who can do this.
- the procedure of record keeping.
- the circumstances when consent is to be sought from senior management (for example when taking on PEPs as customers) and the procedure to be followed in such a case.
- reference to money laundering typologies in the respective business sector.
- screening procedures to ensure high standards when hiring employees.
- adequate safeguards on the confidentiality and use of information exchanged, should be in place.
- reference to specific sources of information, e.g. world check, world compliance, OFAC, newspapers and Google search.
- contact the FIU Sint Maarten, if there may be additional information needed.

A training programme may furthermore include aspects such as taking courses, participation in the information sessions of the FIU Sint Maarten, seminars and using communication resources (e.g. E-mail, newsletters or periodical meetings) that are specifically designed to inform and raise awareness among members of staff.

All personnel must participate in an on-going training programme. However, in order to set up an effective training programme it is necessary to identify key personnel of the gaming service providers. This is in order to determine the most relevant topics for the training program. Key personnel include:

- those members of staff working in the field of CDD, recording of the information and the reporting of unusual transactions.
- the Compliance Officer.
- management.

Gaming service providers should maintain a list of the (key-) personnel that participated in the training programs or specific courses dealing with combating money laundering and terrorism financing. Please be referred to Template 8 of this P&G for an example of a Training Log.

Further requirements for the training include:

- Training has to be at least once a year;
- Training must be certified;
- Documentation of the training must be kept consisting of:
  - The names of the personnel who received AML/CFT training.
  - The name/content of that AML/CFT training.
  - The name of the company/organization that offered the training.

- The date the training was held.

3.2.1 The appointment of a Compliance Officer

Pursuant to Art. 21 (2) of the NOCMLTF, gaming service providers have a person who, on behalf of his organization, is in particular responsible for ensuring compliance with the legal requirements in the field of preventing and combatting money laundering and terrorist financing.

Art. 21 (3) of the NOCMLTF states that gaming service providers have at least one person within its organization who is responsible for the internal receipt and assessment of potential reports and submitting reports on behalf of the gaming service providers to the FIU Sint Maarten.

The gaming service providers can appoint a Compliance Officer on a full time or a part time basis based on its financial resources. Based on paragraph 2, the person appointed should be at least at management level, so that he/she is able to understand and implement the legal requirements. It is also possible for the gaming service provider to hire an external party.

An exception is made for the appointment of a Compliance Officer in a small company. If a company has 15 employees or less, the senior management may fulfil the duties of the Compliance Officer.

The gaming service providers must inform the FIU Sint Maarten that the company falls in this category (≤ 15 employees) and would like for senior management to fulfil the duties of the Compliance Officer. The FIU Sint Maarten shall decide on this request by means of a written decision of the Director of the FIU Sint Maarten.

It is also possible that a small gaming service provider does not wish to appoint one of its own employees as Compliance Officer but uses the services of an external organisation in order to fulfil the duties of the Compliance Officer.

Art. 21 (4) of the NOCMLTF states that gaming service providers inform the FIU Sint Maarten of the appointment of the persons referred to in the second and third paragraph, within one month after the effective date of such appointment.

3.2.2 Duties of the Compliance Officer

Pursuant to Art. 21, paragraphs 2 and 3 of the NOCMLTF, the (principal) duty of a Compliance Officer is to ensure that the gaming service providers correctly comply with the existing legislation and regulations. The Compliance Officer may achieve this by giving training, advice and direction to employees or management on how to comply with internal procedures regarding risk assessment, CDD and reporting unusual transactions. It is also important for the Compliance Officer to communicate with management in order to ensure smooth implementation of the AML/CFT obligations.

The Compliance Officer is preferably the person who on behalf of the gaming service providers reports the unusual transactions to the FIU Sint Maarten and assesses them on their completeness and correctness. The Compliance Officer bears the responsibility for record keeping of all reported unusual transactions. The Compliance Officer is preferably the contact person within the gaming service providers for all communication with the FIU Sint Maarten.

The Compliance Officer will furthermore play an important part within the business during the screening of new employees. The gaming service providers must establish and adhere to proper policies and procedures when screening its employees for criminal records.

The Compliance Officer must be able to operate independently within the organization without the management exerting undue influence with regard to the filing of reports to the FIU Sint Maarten.

The Compliance Officer must be able to fulfil the compliance duties without running the risk of being laid off for executing his work. For the performance of his duties, the Compliance Officer must have unrestricted access to the relevant information (e.g. the records where data regarding CDD is stored, findings of customer investigations and all transactions). It is important that the responsibilities of the Compliance Officer are set out in writing, preferably in the company's compliance policy. If the FIU Sint Maarten undertakes an audit or investigation at the gaming service provider, it will ask to produce a document containing the responsibilities of the Compliance Officer.

It is the Compliance Officer who bears responsibility for implementing the compliance regime for the gaming service providers. It should however be pointed out that, in case of a violation of the AML/CFT framework, an administrative or criminal sanction can be imposed on the gaming service providers. Chapter 6 of this P&G provides more information about supervision and enforcement.

Transfer of tasks

The Compliance Officer has various duties as above mentioned. In case the appointed Compliance Officer cannot fulfil his/her duties due to a heavy workload or prolonged absence, duties or tasks of the originally appointed Compliance Officer can be shared with or transferred to another employee or third party by senior management. The gaming service providers need to communicate this to the FIU Sint Maarten. These specific duties should be laid down in the compliance policy.

It should be pointed out that even if the compliance work is delegated in this way, it is the Compliance Officer who remains responsible for implementing the compliance regime.

4 RECORD KEEPING

Chapter IV of the Art. 21 (3) of the NOCMLTF contains Art. 22 and Art. 23, which relate to the storage of data and information acquired by gaming service providers, or in other terms recordkeeping. The purpose of recordkeeping is to keep a file whenever a customer/vendor has an unusual transaction. The gaming service provider shall keep the data relating to the unusual transaction as well as the data gathered within the scope of the customer investigation (CDD) for a period of at least ten (10) years, after the report is made. The data shall be kept in an accessible manner and filed in such a way as to enable the supervisor to inspect the records at any moment.

A file will be kept of every customer/vendor who carries out a cash transaction of NAf 25,000. -or above, or the equivalent amount in another currency. The file should contain:

- A verified copy of the customer/vendor identification document(s) or a copy of the CDD form which includes the ID information of the customer/vendor;
- The gaming service providers must sign and date on the copy of the customer's identity document to indicate by whom and when identification took place;
- The filled out CDD form, containing the company information (if applicable);
- Other documents (if applicable);
    - A copy of the confirmation letter of the FIU Sint Maarten concerning the reported unusual transaction (if an unusual transaction report has been filed with the FIU Sint Maarten);
    - Internal reports that did not lead to unusual transaction reports to the FIU Sint Maarten.

A distinction should be made between:

- Local/domestic customers or vendors or transactions (receipts, invoices, contracts);
- International customers or vendors/transactions (receipts, invoices, contracts).

These files need not necessarily be kept in one dossier. It is also possible to file separate dossiers. The important part is for these files to be accessible for the FIU Sint Maarten during an audit.

According to the recordkeeping obligation, a file can be kept of:
- a natural person (in the role of a customer or supplier/vendor);
- a company (in the role of a customer or supplier/vendor).

4.1 Record-keeping of identification documents of natural persons

Art. 17 (1) and Art. 25 (2), under a, sub 1° & 2° of the NOCMLTF states that a natural person can be:
- a customer;
- an Ultimate Beneficial Owner (UBO);
- the vendor that does not represent a company;
- the person representing a company (the representative).

The gaming service provider is obligated to maintain the following records of a natural person.

<u>For a customer, UBO, the vendor, and the representative</u>

Art. 17 of the NOCMLTF states that the natural person can be identified with the following documents:

- A valid passport.
- A valid identity card.
- A valid drivers' license.

In case it is not possible to make a copy of the identification document, then the following information must be copied (hand-written) from the abovementioned documents:

- surname.
- forename(s).
- date of birth.
- place of birth.
- residence or place of establishment (if available).
- what type of product/service the unusual transaction is about?

As verification:

- the nature, number, date and place of issuance of the document that has been used to confirm the identity.

The gaming service providers are recommended, for practical reasons, to make a copy of the original identity document (the document that has been used to confirm identity), as this will contain the information detailed above. The gaming service providers should note, on the copy of the identity document, when the identification was carried out and by whom. This makes it easier to prove that identification was undertaken before providing the service.

4.2 Record-keeping of identification documents of a legal entity (company)

Pursuant to Art. 17, paragraphs 2 and 3 of the NOCMLTF, the identity of a legal person or corporation may be established using a certified excerpt from the register of the Chamber of Commerce & Industry or similar institution in the country where the legal person is established. If, for a reason, the representative of the legal person cannot provide the gaming service providers with such a document, the gaming service providers can let the representative fill out the details of the legal person or corporation on a form. Please be referred to Template 6 of this P&G in this regard.

The gaming service providers must confirm the date when and by whom identification was undertaken, in order to establish that the identification took place before the service was provided.

<u>As per Art. 7 (3), under b, of the NOCMLTF a legal entity (company) can be identified by providing the following:</u>

> 1°. the legal form, the deed of incorporation, the Articles of Association, the trade name, the address and, if the legal person is registered with the Chamber of Commerce & Industry, the registration number with the Chamber of Commerce & Industry as well as the way in which the identity has been verified with a reliable and independent source; and
> 2°. of those in a managerial position, those who act on behalf of the legal person, of the beneficial owner and of those who have effective control over the legal person, the surname, the first names and the date and place of birth as well as the manner in which the identity has been verified with a reliable and independent source.

4.3 Record keeping of Unusual transactions

The gaming service providers must keep the data relating to the unusual transactions in files. The

data must be recorded in such a way as to enable the FIU Sint Maarten to see at one glance which employee was involved in the internal reporting as well as the considerations or documents/facts underlying the report.

Moreover, the gaming service providers are required to keep documentation regarding their findings on complex, unusual large transactions, or unusual patterns of transactions, available for competent authorities and supervisors for a period of ten (10) years.

If an unusual transaction highlighted by an employee at the gaming service provider is not reported to the FIU Sint Maarten, there should be a record of the reasons why the report was not submitted to the FIU Sint Maarten by the Compliance Officer. This record should be signed by the Compliance Officer or by the person charged within the institution with the compliance function or the management.

The NOCMLTF does not require the termination of services to the customer as a result of filing an unusual transaction report with the FIU Sint Maarten. However, it is in the best interest of the gaming service providers, with a view to possible intentional, culpable or habitual money laundering situations[6], to consider the facts and circumstances when deciding whether or not the relationship with the customer can be continued.

4.4 Period for maintaining records

Pursuant to Art. 22 (2) of the NOCMLTF, gaming service providers shall, for a period of at least ten (10) years after the execution of a transaction, keep all data relating to transactions at national and international level that is necessary to promptly comply with a request for information by a competent authority. The storage is always done in such a way that individual transactions can be reconstructed at any time and can serve as evidence for the prosecution of criminal offenses.

Art. 22 (3) of the NOCMLTF states that gaming service providers keep for a period of at least ten (10) years after the termination of the business relationship or the execution of a transaction all data obtained through CDD, accounting, business correspondence referred to in Art. 3 (3) paragraph and the results of any analysis of unusual transactions that are necessary to promptly respond to a request for information by a competent authority. The storage is always done in such a way that individual transactions can be reconstructed at any time and can serve as evidence for the prosecution of criminal offenses.

Pursuant to Art. 23 of the NOCMLTF gaming service providers shall keep the copies referred to in Art. 17 (6) of the NOCMLTF, in an accessible manner for at least ten (10) years after the time of termination of the business relationship and shall provide them without delay on request to a competent authority.

The data that has to be saved includes all data gathered from the identification and verification of the customer, all necessary records on transactions (both domestic and international) and all records obtained through other CDD measures. Examples of such data are copies or records of official identification documents like passports, identity cards, driving licences or similar documents, account files and business correspondence, including the results of any analysis (e.g. inquiries to establish the background and purpose of complex and unusual large transactions).

This information must be filed in such a way that it is available and accessible to the competent authority at any point. Any amendments in relation to the customer's risk profile and other relevant information (e.g. contact information) must be updated and retained by the gaming service

[6] Arts. 2:404 (intentional money laundering), 2:405 (habitual money laundering) and 2:406 (money laundering through default) CrC.

providers. The information must be filed in such a way that the competent authority can examine the basis upon which the service was provided.

5 THE REPORTING DUTY

5.1 Unusual Transactions

Pursuant to Art. 24 of the NOCMLTF, by ministerial regulation, after consultation with the FIU Sint Maarten, and if necessary for each group of gaming service provider or categories of transactions to be distinguished, the Minister of Justice will determine indicators on the basis of which it is assessed whether a transaction is classified as an unusual transaction.

First and foremost, it is of importance to point out the meaning of the word "transaction". Under the NOCMLTF, a monetary transaction is defined in Art. 1(1), under n, as:

> 1°. cash transaction: a payment, including a payment with tax aspects, with the aid of cash or a similar means of payment, including credit cards or prepaid payment instruments (prepaid cards), debit cards, bank drafts or money orders; and
> 2°. cashless transaction: a payment, including a payment with tax aspects, by means of the transfer of an amount of money to an account intended for cashless payments at a bank or an equivalent financial institution;

The NOCMLTF indicates that anyone who renders a service as a profession or as a trade, as referred to in Art. 2 (1), under b, sub 1° to 8° and paragraphs 3 and 4, in or from Sint Maarten, is obliged to report any unusual transaction, either executed or intended, to the FIU Sint Maarten immediately. Whether a transaction is considered unusual, is determined by objective and subjective indicators.

Intended Transactions:
The reporting duty pertains not only to unusual transactions that have actually been executed by the gaming service providers but also to intended unusual transactions. Intended unusual transactions include e.g. transactions that for whatever reason have not been executed by the service providers.

5.2 Indicators

There are three (3) indicators established for the gaming service providers according to the Ministerial Decree (AB 2013, GT no. 489).

5.2.1 Objective Indicators

Pursuant to the Ministerial Decree Indicators (AB 2013, GT no. 489), objective indicators explicitly indicate when a transaction should be reported as unusual. The gaming service providers are obligated to report objectively. This will be a violation of the law. If an objective indicator applies to the transaction, reporting is mandatory.

The objective indicators are:

- A transaction that is reported to law enforcement and of which the funds are related to the proceeds of a criminal activity or terrorism financing must also be reported to the FIU Sint Maarten, using the code: 160101
- A transaction that is reported based on the National sanction ordinance must be reported to the FIU Sint Maarten, using the code: 160102
- All transactions (cash and wire transfers) equal to or above NAf 5,000. -- for casino/ online gaming and lotteries must be reported to the FIU Sint Maarten, using the code: 160105

The unusual transaction covers both the receipt and the disbursement of the cash.

5.2.2 Subjective Indicators

An unusual transaction must be reported if it gives rise of a suspicious of ML/TF by the gaming service providers, based e.g. on his knowledge of the customer, the customer's business or the transaction involved.

Annex 1 to this P&G contains a list of red flags on the basis of which a decision can be made as to whether a transaction should be classified as unusual. This list is not exhaustive. If one or more of these red flags are applicable, the gaming service providers will need to assess whether the transaction should be reported as suspicious. Art. 33, paragraphs 1 and 2 of the NOCMLTF states that the violation of the reporting obligation, in so far committed intentionally, is considered a criminal offence.

There are two (2) subjective indicators according to the Ministerial Decree Indicators (AB 2013, GT no. 489).

The two (2) subjective indicators are:

- A transaction that deviates from the profile of the customer: 160201
- A transaction that gives the gaming service providers a suspicious feeling that it relates to money laundering or terrorism financing: 160202

5.3 Reporting

Gaming service providers are obligated to report an unusual transaction without delay to the FIU Sint Maarten (Art. 25 of the NOCMLTF). Reporting can be done by sending a digitally completed reporting form or by delivering a manually completed reporting form in person to the FIU Sint Maarten.

Most of the gaming service providers are businesses with more than one employee. Within the institution a particular person should be designated to forward the unusual transaction reports to the FIU Sint Maarten. This person is called the Compliance Officer. It is up to the institution to employ internally an independent acting Compliance Officer or to designate an external person to execute the compliance duties. The rest of the employees that handle transactions are required to report these to the Compliance Officer, so that he/she can forward the unusual transaction reports to the FIU Sint Maarten.

It is the gaming service providers' responsibility to take care that their employees apply the rules correctly and to see that unusual transactions are promptly and correctly reported to the FIU Sint Maarten. There should therefore be a written internal reporting procedure for all employees within the institution, where the services are provided.

5.3.1 Time limit for reporting

Pursuant to Art. 25 (1) of the NOCMLTF an (intended) unusual transaction must be reported immediately. The FIU Sint Maarten interprets the term "immediately" as follows:

- For reports based on an Objective indicator

The gaming service providers must send their unusual transaction report within 48 hours after the transaction has been executed, or after the intention to execute an unusual transaction has taken place.

A request for extension must be directed in writing to the director of the FIU Sint Maarten, stating the reasons for the request for extension. The FIU Sint Maarten will then inform the respective reporting entity in writing of its decision within 24 hours.

- Subjective Reports (reports based on a Subjective Indicator)

The time period between the execution of the unusual transaction (or the intention to execute an unusual transaction) and the reporting of the unusual transaction by the Compliance Officer to the FIU Sint Maarten shall not exceed 48 hours.

If in those 48 hours the Compliance Officer concludes that more time is needed to gather information, then the FIU Sint Maarten must be notified and requested to give the Compliance Officer more time to report the transaction. The FIU Sint Maarten then decides how much extra time is granted. The Compliance Officer then finalizes the assessment of the transaction within the time stipulated by the FIU Sint Maarten and reports it to the FIU Sint Maarten.

In the case that the above-mentioned time periods are absolutely not feasible, the reporting entity will send a request for another extension in writing (by E-mail) to the FIU Sint Maarten, stating the reasons for this request.

The FIU Sint Maarten will inform the reporting entity in writing within 24 hours of its decision. Depending on each individual situation the FIU Sint Maarten will decide the maximum extension period.

5.3.2 Information to be reported

Art. 25 (2) of the NOCMLTF states that, a report shall contain the following information:

a. in respect of natural persons:
   1°. the customer's identity as established on the basis of Art. 3 (3);
   2°. the type, number, date and place of issue of the customer's proof of identification;
   3°. the nature, time and place of the transaction;
   4°. the scope, destination and origin of the funds, securities, precious metals or other assets involved in the transaction;
   5°. the circumstances on the basis of which the transaction is designated unusual; and
   6°. if it relates to a transaction involving an item which has a higher value than that established by the Minister in a ministerial regulation, a description of the item concerned;
   7°. the indicator or indicators on the basis of which the transaction has designated unusual;
   8°. the type and number of the bank account used in the transaction; and;
   9°. the bank statements and business-related correspondence.

b. in respect of legal entities incorporated under the laws of Sint Maarten:
   1°. the legal form, the name given in the Articles of Association, the trade name, the address and, if the legal entity is registered with the Chamber of Commerce & Industry, its registration number at the Chamber of Commerce & Industry as well as the way in which its identity has been verified;
   2°. the surnames, first names, places and dates of birth of those who act on behalf of the legal entity and the ultimate beneficiary; and
   3°. the data referred to under a, sub 3° to 6°.

c. in respect of foreign legal entities and comparable entities:
   1°. documents on the basis of which the identity has been verified;
   2°. the surnames, first names and dates of birth of those who act on behalf of the legal entity and the ultimate beneficiary; and
   3°. the data referred to under a, sub 3° to 6°.

The FIU Sint Maarten is allowed to request additional information from the gaming service providers.

5.3.3 Internal Reporting

Internal reporting of unusual transactions to the Compliance Officer should be executed by making use of the objective or subjective indicators as mentioned in paragraph 5.2.1 and 5.2.2. In case the salesperson/employee carries out the transaction, and files an internal report (template 7) it must be submitted to the Compliance Officer. The Compliance Officer then assesses the internal report to file the unusual transaction report to the FIU Sint Maarten. The Compliance Officer will not let the employee know whether the unusual report was filed or not. Please remember that identification is obligatory in case of a cash transaction of NAf 25,000.-- or above or the equivalent in another currency.

Tipping off prohibition

All data and information that have been supplied or received pursuant to the provision by or in accordance with the NOCMLTF are confidential. The gaming service providers and their directors, senior management, and employees are not allowed to divulge any information, with regards to the FIU Sint Maarten and its legal tasks, to customers and/or third parties (tipping off prohibition).

6 CONFIDENTIALITY

Art. 27 of the NOCMLTF states the following:

1. To secrecy, except insofar as the necessity for publication arises from the objective of this national ordinance, is obligated:
   a. a gaming service provider who makes a report pursuant to Art. 25 or who provides further data or information to the FIU Sint Maarten upon request;
   b. the director and the other staff of the gaming service provider, referred to under a;
   c. persons and bodies that provide data or information to the FIU Sint Maarten on request or grant access to the registers and other information sources under their control;
   d. the director and the other personnel of the FIU Sint Maarten who, by virtue of the application of this national ordinance or of decisions taken pursuant to this national ordinance, performs or has fulfilled any task, and in doing so has taken cognizance or can take note of data or information that is provided or received; and,
   e. the supervisors of gaming service providers as referred to in article 1 who, in the performance of their duties, take cognizance of data, information and facts that may indicate money laundering or terrorist financing.
2. A supervisor who, in the performance of his duties, discovers facts that may indicate money laundering or terrorist financing, will inform the FIU Sint Maarten without delay, if necessary in deviation from the applicable statutory duty of confidentiality.
3. A gaming service provider may, notwithstanding the provisions of the first paragraph, make notifications to:
   a. gaming service providers that belong to the same group and that have at least complied with the obligation to perform a CDD;
   b. gaming service providers, established or having their registered office in a country within the Kingdom of the Netherlands, who carry out their activities, whether or not as employees, within the same legal entity or network;
   c. a lawyer, civil-law notary, junior civil-law notary, broker, accountant or financial enterprise, established or having its registered office in a country within the Kingdom of the Netherlands, provided that it concerns the same customer and the same transaction and the communication is solely intended to prevent money laundering and financing of terrorism;
   d. a lawyer, civil-law notary, junior civil-law notary, broker, accountant or financial enterprise, established or having its registered office in a country within the Kingdom of the Netherlands, who is subject to equivalent obligations in terms of professional secrecy and protection of personal data, and belong to the same professional category, as long as it concerns the same customer and the same transaction and the communication is solely intended to prevent money laundering and terrorist financing.
4. For the purposes of paragraph 3, network means: “the larger structure to which the person belongs and which jointly shares ownership, management or control of compliance with the obligations.”

Pursuant to Art. 28 of the NOCMLTF, privacy regulations of financial institutions may not result in the implementation of the reporting national ordinances being obstructed.

7 INDEMNITY

Pursuant to Art. 29 of the NOCMLTF:

1. A gaming service provider who has made a report as referred to in Art. 25 in good faith or has provided data or information to the FIU Sint Maarten, is indemnified from criminal and civil liability for violation of a prohibition on disclosure of information under (an agreement or) any legal or regulatory requirement.
2. The first paragraph applies mutatis mutandis to liability for the damage suffered by a customer, intermediary or third party as a result, unless the damage is the result of deliberate or deliberate reckless action by the gaming service provider.
3. The first and second paragraphs apply mutatis mutandis to the director and the other personnel of the gaming service provider who has cooperated in or were involved in acts as referred to in the first paragraph.

Pursuant to Art. 30 of the NOCMLTF, data or information that has been reported or otherwise provided in good faith by the gaming service providers in implementation of the provisions of or pursuant to this national ordinance cannot serve as a basis for or for the purpose of an investigation or prosecution on the basis of suspicion of, or as evidence in respect of a charge of money laundering or terrorist financing.

Art. 29 (2) 2 of the NOCMLTF states that, the first paragraph applies mutatis mutandis to the director and the other personnel of the gaming service providers who cooperated in or were involved in acts as referred to in the first paragraph.

8 SUPERVISION AND ENFORCEMENT

8.1 GENERAL

The FIU Sint Maarten has as the supervisor of the DNFBP sectors, the assigned legal tasks as mentioned in Art. 3, paragraph 2 of the NOFIU. These legal tasks can be divided in specific supervisory tasks, specific analysis tasks and specific enforcement tasks.

Examples of the FIU Supervisory tasks are:

- collecting, recording, processing and analyzing the data obtained by the FIU Sint Maarten from the DNFBP sector in order to add value to such data and to examine whether these data could be important in preventing and combatting ML, TF/PF, and the underlying crimes, pursuant to the national reporting ordinances.
- providing information and training to the service providers, persons and authorities charged with monitoring compliance with a National Ordinance on reporting unusual transactions, to the Public Prosecutor's Office, and to the civil servants charged with detecting and investigating criminal offences as well as to the public regarding the manifestations and the prevention and combatting of ML and TF/PF.
- advising on and, on request, formulating national policy for the prevention and combatting of money laundering and terrorist financing that is based on the risk assessment, and promoting the implementation of that policy and cooperation between supervisors, investigative authorities and other parties responsible for implementing that policy.

Examples of the FIU Analysis tasks are:

- conducting investigation at a gaming service provider if a person is not included in a register as referred to in Art. 4, and there is a suspicion that he or she is involved in money laundering or the financing of terrorism.
- conducting investigation on its own initiative or at the request of an authority as referred to in Art. 7.
- carrying out operational and strategic analyses of data and intelligence and research into developments in the field of ML and TF/PF, and into the improvement of methods to prevent and combat ML and counter TF/PF, as well as movement or upon request dissemination of the results thereof to the relevant authorities.

Examples of the FIU Sint Maarten enforcement tasks are:

- monitoring the compliance of the gaming service providers with the National Reporting Ordinances and this P&G, and the imposing of administrative sanctions;
- providing the possibility of a reconsideration of the initial decision to impose an administrative sanction on a non-compliant gaming service provider, in the objection procedure.

Within administrative law the term 'supervision on compliance' (= the implementation of regulations) is a synonym for enforcement. Within this enforcement context the term "supervisor" (a natural person performing his functional tasks) is defined as: "*a by or pursuant to a national ordinance designated person by an administrative body, charged with supervising compliance with or pursuant to a national ordinance.*" (Art. 1, paragraph 1, under j of the National Ordinance Administrative Enforcement).

Pursuant to Art. 1, under o of the NOFIU, "supervisor" is defined as: "*an employee of the FIU who*

supervises the way in which a service provider implements the provisions of the NOCMLTF."

The sanctions pallet of the FIU Sint Maarten consists of administrative sanctions, civil law sanctions and criminal law sanctions.

- imposing administrative sanctions involves the FIU Sint Maarten;
- imposing civil law sanctions involves the judge of the Court of First Instance;
- imposing criminal law sanctions involves the Public Prosecutor's Office.

8.2 ENFORCEMENT

8.2.1. Administrative law sanctions

When a gaming service provider is not compliant with the AML/CFT framework or this P&G, the director of the FIU Sint Maarten has the authority to impose enforcement measures.

Within administrative law a division can be made between remedial sanctions and punitive sanctions.

- Administrative remedial sanction:

"*an administrative sanction leading to termination or the complete or partial undoing of a violation or the consequences thereof or to prevent a recurrence of an offence.*"
(See: Art. 1 (1), under f of the National Ordinance Administrative Enforcement)

The Director of the FIU Sint Maarten can make use of two (2) different corrective sanctions:

(1) the order for incremental penalty payments, and
(2) the order for administrative coercion.

Ad 1. The incremental penalty payment consists of a written order for full or partial repair of a violation within a specified period, and the obligation to pay a sum of money, if the assignment is not carried out or not carried out on time. The maximum amount of the incremental penalty payment is always included in the sanction decision of the Director of the FIU Sint Maarten. The appeal clause is always mentioned in the sanction decision as well.
The procedure for imposing an incremental penalty payment is regulated in Arts. 22-33 of the National Ordinance Administrative Enforcement.

Ad 2. The order for administrative coercion consists of a written order given to the addressee to fully or partially remedy a violation, and the authority of the administrative body to factually execute the burden if the order is not carried out or not carried out on time. An example would be the closing of the office of the gaming service provider for a certain period of time.

The procedure for imposing an order for administrative coercion is regulated in Arts. 34-45 of the National Ordinance Administrative Enforcement.

- Administrative punitive sanction:

"*an administrative sanction that is intended to impose harm to the offender.*"
(See: Art. 1 (1), under e of the National Ordinance Administrative Enforcement)

The FIU Sint Maarten can make use of a punitive sanction:

(1) the administrative fine.

The legal authority of the FIU Sint Maarten to impose administrative sanctions, derives from:

Art. 31 (3) of the NOCMLTF:

> "*To implement this national ordinance, the FIU Sint Maarten and the Central Bank are authorized to impose an order for incremental penalty payments, an order for administrative coercion and an administrative fine. The National Ordinance Administrative Enforcement applies to both the FIU Sint Maarten and the Central Bank, provided that the administrative fine, referred to in Art. 55 of that national ordinance, amounts to no more than NAf 4,000,000.*"

The Arts. 50-57 of the National Ordinance Administrative Enforcement are related to the authority to impose an administrative fine, and describe the legal procedure.

Art. 19 of the NOFIU:

1. "*The National Ordinance Administrative Enforcement enters into force for the FIU, on the understanding that an administrative fine as referred to in Art. 55 of that national ordinance amounts to no more than NAf 4,000,000.*
2. *The FIU is authorized in any event to impose an order for incremental penalty payments, an order for administrative coercion and an administrative fine.*"

- Other administrative procedural options

If an imposed primary administrative sanction by the FIU Sint Maarten on a gaming service provider does not have the intended effect, there are the following subsequent procedural options:

- the FIU Sint Maarten may impose an order for administrative coercion after imposing an order for incremental penalty payments;
- the FIU Sint Maarten may impose an administrative fine after the imposition of an order for incremental penalty payments;
- After imposing an administrative fine, the FIU Sint Maarten may re-impose a fine (this time doubled) in the case of repeat offences;
- the FIU Sint Maarten may contact the Public Prosecutor's Office after the imposition of an administrative fine to have a criminal sanction imposed by the Public Prosecutor's Office.

The following aspects, among others, play a role in the decision to file a report:

- the complexity of criminal law norm violations, the need to use criminal coercive measures, the concurrence with predicate offences, the culpability, social unrest or impact and the expected effect of administrative, disciplinary, civil or criminal settlement.

With regard to conduct for which an administrative fine can be imposed and which is also a criminal offense, coordination takes place between the FIU Sint Maarten and the Public Prosecutor's Office.

8.2.2. CIVIL LAW SANCTIONS

In the context of FATF Rec. 35 (Sanctions), it shall be noted here for completeness that pursuant to Art. 24(1) of Book 2 of the Civil Code of Sint Maarten, the Court may dissolve a legal person if: (a.) "*its objects or activities are wholly or partly contrary to morality, public order, the law or the articles of association.*" This includes non-financial service providers who, as legal persons, commit violations of the requirements of the NOCMLTF, the National Ordinance Reporting Cross-Border Cash Transports, the National sanction ordinance and its underlying National sanction

decree, and the P&G, in the course of their activities.

Subsequently, Art. 24(4) of Book 2 of the Civil Code Sint Maarten provides that this said dissolution can be requested by the Court by an interested party or the Public Prosecutor's Office (PPO). Given its supervisory task on the integrity of the financial system of Country Sint Maarten, the FIU Sint Maarten can be considered an interested party. In this regard, the FIU Sint Maarten and the PPO can make further agreements (covenant).

Moreover, if a gaming service provider, being a legal person, has been convicted by irrevocable judgment for ML or TF, pursuant to Art. 25(1)(c) of Book 2 of the Civil Code of Sint Maarten, such legal person shall be dissolved by an order of the Sint Maarten Chamber of Commerce & Industry.

8.2.3. CRIMINAL LAW SANCTIONS

Art. 33 of the NOCMLTF:

1. Each action in breach of the provisions under or pursuant to Arts. 3, 4, 5, 6, 8, 10, 11, 12, 15, 16, 17, paragraph 6, 18, 19, 20, 21, 22, 23, 25, 26, paragraph 1, 27 or 37, paragraph 2 of the NOCMLTF shall, to the extent it was intentional, be punished by either a prison sentence of a maximum of four (4) years or a financial penalty of the sixth category (NAf 1,000,000.).
2. Each action in breach of the provisions under or pursuant to Arts. 3, 4, 5, 6, 8, 10, 11, 12, 15, 16, 17, paragraph 6, 18, 19, 20, 21, 22, 23, 25, 26, paragraph 1, 27 or 37, paragraph 2 of the NOCMLTF shall, to the extent it was unintentional, be punished by either imprisonment for a maximum of one (1) year or a financial penalty of the sixth category (NAf 1,000,000.).
3. If an action in breach of the provisions of Art. 27 of the NOCMLTF results in the report or the information becoming known to the person/entity to whom/which the report or information relates, the prison sentence for the infringement shall be increased by one and a half times.
4. The facts deemed punishable in paragraph 1 shall be considered criminal offences. The facts deemed punishable in paragraph 2 shall be considered misdemeanors.
5. The party committing the act is punishable, as well as the directors and executives, irrespective of whether these are natural persons, legal entities, groups of natural persons or legal entities, or organizations.

TEMPLATES

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 1: Organizational Change Form

A. Company category

Do you or does your company provide one or more of the services corresponding to one or more of these sectors? *Please check the relevant box(es) and proceed to*	☒ Gaming service providers ☐ Dealers in Precious Metals and Stones ☐ Car dealers ☐ Lawyers ☐ Notaries ☐ Accountants ☐ Tax advisors ☐ Administration offices ☐ Real Estate companies/agents

B. Company details

Contact Details	
Company name *This is the name as mentioned in the Chamber of Commerce & Industry.*	Click here to enter text.
Company DBA name *This is the name the company does business as.*	Click here to enter text.
Physical address company • *This is the address where the company is physically situated.* • *street, number, area*	Click here to enter text.
Postal address company - *If applicable* - *Street, number, area*	Click here to enter text.
Country *This is the country in which the company is physically situated.*	Click here to enter text.
Telephone number 1	
Fax number	
E-mail address *This should be a working e-mail address for the company.*	Click here to enter text.
Website	

C. Company directors/Statutory representatives

Company directors/statutory representative	
First name	
Last name	

Date of birth	
Nationality	
ID document type	Choose an item.
ID document number	
Function	
Home address - *street, number, area*	Click here to enter text.
Country	
Zip code *If applicable.*	Click here to enter text.
Telephone number 1	
Telephone number 2	
E-mail address	

*Please attach for every director/statutory representative the following document: A copy of the ID document mentioned above.

D. Ultimate Beneficial Owner (UBO)

UBO	
First name	
Last name	
Nationality	
Home address *Street, number, area*	
Country	
Zip Code *If applicable.*	Click here to enter text.
Profession	
Percentage of holding or interest	

*Please attach the following document: An organizational chart of the company/group of companies. This to give the FIU Sint Maarten insight in the structure of the company.

A. Compliance Officer (CO)

Person who is responsible for the reporting/Compliance Officer	
First name	

Last name	
Date of birth	
Nationality	
ID document type*	Choose an item.
Function	
E-mail address	

*Please attach the following document: A copy of the ID document of the person who is responsible for reporting/Compliance Officer

B. Compliance regime

1. Compliance policy and internal procedures, training or evaluation procedures

Description of change(s)

C. Signature form

Changes applicable as of date:	

---------- ----------

Signature Compliance Officer or Person responsible for reporting

Signature Director FIU Sint Maarten

Company stamp

PLEASE NOTE:

- MAKE SURE THE FORM IS SIGNED BY THE COMPLIANCE OFFICER OR PERSON WHO IS RESPONSIBLE FOR REPORTING, AND THE DIRECTOR.
- MAKE SURE THE FORM IS STAMPED.
- AFTER FILLING IN THE FORM, SAVE IT AS A DOCUMENT ON YOUR COMPUTER. SEND IT BACK, TOGETHER WITH THE ATTACHMENTS, TO THE FIU AT THE FOLLOWING E-MAIL ADDRESS: Supervision.department@fiu.gov.sx
- THIS FORM CAN ALSO BE HAND DELIVERED TO THE FIU SINT MAARTEN OFFICE.

Procedure submission of organizational changes

1. Choose the relevant category that your company falls under.
2. Fill out the changes in question under B-G.
   - If there are changes in the compliance regime, please give an accurate description of these changes.
3. Close the form by entering the date of the change and provide the form with the relevant signatures.
4. Send the form to the FIU Sint Maarten.

Template 2: Risk Assessment Form

Risk assessment – Know Your Customer - Points
A risk assessment implies that the service provider assesses realistic risks involved within the operation of its business. The Company needs to give points to each risk factor detected in its risk assessment. The outcome of the assessment is the first indication for the type of CDD (simplified, standard or enhanced due diligence) that the company has to execute.

Risk profile
The outcome of the risk assessment is summarized in a written risk profile, which will let the company know what CDD needs to be performed corresponding with a respective profile.

Points of consideration
- Risk assessment is mandatory. Following this way of assessment is not;
- This template is an example to give you directed guidance on how to perform a risk assessment;
- Following this guidance is not mandatory. Reporting entities may choose to comply with the AML/CFT framework using alternative methodologies;
- This template is based on categories of risk factors. Each category has underlying risk factors that might be applicable for your company and that you have to choose on the basis of the list in Annex 1 (risk assessment questions for customers);
- The risk questions pertain to the different risk factors and are accompanied by a range of points that have the purpose of giving an indication of the risk involved;
- You need to implement the risk factors with the accompanying risk assessment questions in the risk assessment form below. The outcome in the form will guide you on how to perform a CDD.

Point system
- The points given to the different risk assessment questions in this Risk Assessment Form are examples of the weight to give to the risk factors;
- These points are not binding. Ultimately it is the Company's responsibility to execute a balanced risk assessment;
- In the annexes the FIU Sint Maarten has given an indication of the range of points that can be given to the risk factors pertaining to the risk assessment questions;
- Make sure the points mount up to a logical total so it is very clear when you have a low, normal or high risk outcome;
- There are some situations that by their nature have to lead to immediate high risk and thus executing an Enhanced CDD. These situations cannot be modified when using this risk assessment and therefore receive the maximum amount of points, being:
    - Questions and points about Politically Exposed Persons (PEPs) (50 points);

- Questions and points about customers from High Risk or sanctioned countries.

These two points have to be incorporated in your risk assessment form:

- Always fill out your risk assessment report specifically to the details of your own company, customers, products, experience etc. Please select the risk assessment questions in the Annex 1 that apply to your company's customer/country/product or transaction;
- Note that, in order to be able to assess the risks, risk assessment questions will always have to be asked to the customer.

Customer Risk Assessment Form ! EXAMPLE !

Date assessment: *This will be the date when the risk assessment is performed.*	
Name assessor: *The name of the person performing the assessment*	
Name customer: *The name of the customer*	
Changes made (if applicable): *If it is an existing customer and a risk assessment has already been made, the changes made to a risk assessment can be filled out here*	
Comments: *Other comments the assessor might have*	

COUNTRY RISK FACTORS	YES	NO	PTS
1. Is the customer from a country with a higher risk on the FATF public statement list? (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2014.html) PLEASE NOTE: Include other high risk, sanctions list countries that are applicable to your business. Check the P&G and the website of the FIU Sint Maarten.	50 (non-modifiable)	0 (example)	
2. Does payment (wire or credit card) come from/go to a financial institution with an origin in a country with a higher risk on the FATF public statement list? (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2014.html) PLEASE NOTE: Include other high risk, sanctions list countries that are applicable to your business.	50 (non-modifiable)	0 (example)	
Please continue filling out the risk assessment questions applicable specific to your business.	CHOOSE FROM ANNEX 1		
TOTAL SCORE CATEGORY			

CUSTOMER RISK FACTORS	YES	NO	PTS
A. Customer behavior			
1. Is the customer mysterious or evasive about the motive of the transaction?	10 -25 (example)	0	
2. Is the behavior of the customer peculiar in any way (e.g. nervous)?	10 (example)	0	
Please continue filling out the risk assessment questions applicable specific to your business.			
B. Customer identification			
3. Does the customer have an irregular address?	10 (example)	0	
4. Does customer act reluctant to provide ID?	10-20 (example)	0	
Please continue filling out the risk assessment questions applicable specific to your business.	CHOOSE FROM ANNEX 1		
ONLY IN CASE THE CUSTOMER IS A COMPANY - *<u>Please note</u>: You have to always verify who the authorized representatives are of the company and the UBO*			
5. Is it (made) difficult to establish the identity of the UBO? <u>PLEASE NOTE</u>: The UBO is the natural person(s) that holds 25% or more shares/interest/ownership control in the company.	10-50 (example)	0	
Please continue filling out the risk assessment questions applicable specific to your business.			
C. Customer type (characteristics)			
6. Is it a non-face-to-face customer?	10-50 (example)	0	
7. Is there a PEP (Politically Exposed Person) involved? PLEASE NOTE: To know this check - Newspapers - Google - www.transparancy.org	50 (non-modifiable)	0	
Please continue filling out the risk assessment questions applicable specific to your business.	CHOOSE FROM ANNEX 1		
TOTAL SCORE CATEGORY			

TRANSACTION FACTORS	YES	NO	PTS
A. Establishment of transaction			
1. Is the transaction established in an abnormal rapid/fast way?	10-30 (example)		
2. Did the customer inquire to possibilities of refunding?	5-20 (example)		
Please continue filling out the risk assessment questions applicable specific to your business.	CHOOSE FROM ANNEX 1		

B. Payment			
3. Is there a high level of transactions just below the reporting threshold?	20 – 50 (example)		
4. Is it an unusually large transaction?	5 – 20 (example)		
Please continue filling out the risk assessment questions applicable specific to your business.	CHOOSE FROM ANNEX 1		
TOTAL SCORE CATEGORY			

Outcome

< 10 : You have the choice between performing a simple CDD or a standard CDD.

10-49 : Standard CDD.

50 : Enhanced CDD.

Total score risk assessment	
Outcome	☐ Low risk → Simplified CDD ☐ Normal risk → Standard CDD ☐ High risk → Enhanced CDD

Procedure to create a company specific risk assessment form

This procedure is used to customize the risk assessment form specific to your company.

1. Choose the risk questions for each risk category that are relevant for your company. Please refer to Annex 1.
2. Give each selected question points based on the weight of the risk specific to your company. A higher risk is a higher point. Stay within the indicated point range.
3. Fill out the risk questions in the first column of the risk assessment form corresponding to each risk category.
4. Fill out the chosen points corresponding with the relevant risk question in the second column under "yes".
5. Sum up the points given in the risk assessment.

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 3: Examples Risk Profile

HIGH
<u>Country</u> - Nationality of the customer *Example:* - *Iranian (Iran is a FATF high risk country)* Please note: These are (two examples of) the typical characteristics of a type of high risk customer in your customer base
<u>Customer</u> - Type of customer - Behavior *Example:* - *Customer is a nervous natural person;* Please note: These are (two examples of) the typical characteristics of a type of high risk customer in your customer base.
<u>Payment/transaction</u> - Type or origin of payment - Delivery *Example:* - *Payment with credit card from offshore account* - *Partly cash payment* Please note: These are (three examples of) the typical characteristics of a type of payment typical of a high risk customer in your customer base.
<u>Other:</u> Please note: These are the other typical characteristics of a high risk customer in your customer base.
Comments and remarks

Explain the reason(s) for choosing above risk profile. Please note: Write down all the peculiarities

---

Signature Compliance Officer

In case of High Risk:

Signature approval senior management

Name:

Date:

NORMAL
Country - Nationality Example: - *A USA customer* Please note: These are (two examples) the typical characteristics of a type of normal risk customer in your customer base.
Customer - Type of customer *Example:* - *Retired USA customer* Please note: These are the typical characteristics of a type of normal risk customer in your customer base.
Payment/Transaction - Payment type *Example:* - *Credit card* Please note: These are the typical characteristics of a type of payment or transaction typical of a normal risk customer in your customer base
Other Please note: These are the other typical characteristics of a normal risk customer in your customer base
Comments and remarks Please explain the reason(s) for choosing above risk profile. Please note: Please write down all the peculiarities.

Signature Compliance Officer

Name: Date:

LOW
Country - Nationality *Example:* - *Government owned business established in St. Maarten* Please note: These are the typical characteristics of a type of low risk customer in your customer base.
Customer - Type of customer *Example:* - *Government owned company: GEBE* Please note: These are the typical characteristics of a type of low risk customer in your customer base/company.
Payment/transaction - Type of payment - Purpose of payment *Example:* - *Company credit card* Please note: These are (two examples of) the typical characteristics of a type of payment typical of a low risk customer in your customer base/company.
Other Please note: These are the other typical characteristics of a low risk customer in your customer base/company.
Comments and remarks Please explain the reason(s) for choosing above risk profile. Please note: Please write down all the peculiarities.

Signature Compliance Officer

Name: Date:

Introduction:

- This procedure is to be used when setting up risk profiles for specific customers in the Company customer base;
- The risk assessment form should be filled out before a risk profile can be created. Based on the filled out characteristics of the risk assessment, a risk profile can be made;
- The outcome of the risk assessment always indicates a level of risk (high, normal, low). In the risk profile all the characteristics of the selected level of risk are written down;
- For example: if the risk assessment indicates a high level of risk then all the characteristics of this high risk are explicitly laid down in the risk profile of the customer, divided over the different risk categories (country, customer, product/service and payment/transaction). At the end write down a short conclusion about the high risk;
- Depending on the risk assessment, you choose specific characteristics that can make a low risk customer a low risk, a normal risk customer a normal risk and a high risk customer a high risk. The risk assessment needs to be analyzed as a whole.

1. Finish the risk assessment form for the customers in your customer base. The risk outcome will determine which risk profile you need to use.
2. Select a risk profile (high, normal, low).
3. Under “country” you can fill out the characteristics that have to do with the country, for example, the nationality of the customer.
4. Under “customer” you can fill out the characteristics that have to do with, for example, the type of customer, its behavior or anything else that has to do with the customer itself.
5. Under “payment/transaction“ you can fill out the characteristics that have to do with, for example, the payment or the transaction itself that is linked to a type of customer.
6. Under “product” you can fill out the characteristics that have to do with one or more specific products.
7. Under “other” you can fill out the extra characteristics you want to add.
8. Give a summary/conclusion about the decision to choose the risk profile.

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 4: Standard + Simplified CDD form

A. FOR YOUR CUSTOMERS

REPRESENTATIVE OF THE CUSTOMER (if applicable)
Name:
Surname:
Please attach: A copy of valid verified identification for the representative.

CUSTOMER (natural persons)
Name:
Surname:
Please attach: A copy of valid verified identification for the customer.

CUSTOMER (companies)		
Legal name:		
DBA name:		
Please attach: A copy of the Chamber of Commerce & Industry extract of the company or in case not obtainable, the filled out identification document for companies.		
Ultimate Beneficial Owner(s) of the company		
Name	Date of birth	Percentage of interest/shares
Please attach: Copy of valid verified identification. Or if not obtainable fill out on company identification form.		
Questions What is the purpose of your purchase?		

Signature of person that filled out the form: .....

Name person that filled out the form: .....

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 5: Enhanced CDD

A. FOR YOUR CUSTOMERS

REPRESENTATIVE CUSTOMER (if applicable)
Name:
Surname:
Address:
Place:
Birth date:
Please attach: A copy of valid verified identification for the representative.

CUSTOMER (natural persons)
Name:
Surname:
Address:
Place:
Birth date:
Occupation:
Please attach: A copy of valid verified identification for the customer.

CUSTOMER (companies)		
Legal name:		
DBA name:		
Please attach: A copy of the Chamber of Commerce & Industry extract of the company or in case not obtainable, the filled out identification document for companies.		
Ultimate Beneficial Owner(s) of the company		
Name	Date of birth	Percentage of interest/shares

Please attach: Copy of valid verified identification. Or if not obtainable fill out on company identification form.
Questions
1. What is the purpose of your purchase?
2. What is the source of funds for this purchase?

Signature of person that filled out the form: ……..

Name person that filled out the form: ……

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 6: Identification document companies

Name of employee carrying out the identification: .....

Date identification: .....

Time identification: .....

Details of the Company	
Statutory name	
Trade name (DBA)	
Legal form	
Address	
Place of establishment	
Country of establishment	
Registration number	
Country of Chamber of Commerce & Industry	

Authorized representative for the Company 1	
Name	
Date of birth	
Type of identification document	

Authorized representative for the Company	
Name	
Date of birth	
Type of identification document	

Ultimate Beneficial Owner of the Company 1	
Name	
Date of birth	
Percentage of interest/shares	

(If there are more than one, please add more columns)

Signature of person that filled out the form: .....

Name person that filled out the form: .....

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 7: Internal reporting form

Date	
Time	
Location	
Employee name	

Transaction

- ☐ Executed transaction (transaction/deal/sale closed)
- ☐ Intended transaction (transaction/deal/sale not closed)

Type of unusual transaction

- ☐ Objective: Reported something to the law enforcement
- ☐ Objective: Mentioned customer on a list adopted by the Sanctions Decree
- ☐ Objective: An occasional transaction or wire transfer of NAf 500,000. --
- ☐ Objective: Cash transaction of NAf 25,000.-- or above (fill out if desired USD ..., EUR...)
- ☐ Subjective: Transaction deviates from the profile of the customer
- ☐ Subjective: Suspicious transaction
- ☐ Other:

Amount of transaction/deal/sale	
Description of goods/service	

Type of customer

- ☐ Natural person
- ☐ Legal entity

Description of circumstances (describe the situation that led to the reporting of this unusual transaction)

Signature employee
Date:

Note: Please enclose a copy of the identification papers of the customer to this report.

FOR COMPLIANCE OFFICER FOR COMPLIANCE OFFICER FOR COMPLIANCE OFFICER

Date receipt internal report	
Date internal report complete	
Missing details/documents (if applicable)	

……
Signature Compliance Officer

Date:

Subjective assessment Compliance Officer

Date start of assessment		Time	
Date end of assessment		Time	

Assessment

Red flags applicable:
Description of outcome assessment/steps taken:

Conclusion (the decision whether to report to the FIU Sint Maarten or not)

☐ Unusual Transaction Report (UTR) to FIU Sint Maarten

☐ No Unusual Transaction Report to FIU Sint Maarten (in this case, the senior management also has to sign below)

Date UTR (if applicable)		Time	

……
Signature Compliance Officer
Date:

……
Signature senior management
Date:

Note: Please enclose the confirmation letter if reported!

Procedure internal reporting for employees

Please note:

- When you encounter an Unusual transaction, fill out the Internal Report Form right after.
- Fill out the Internal Report Form yourself.

Submitting the Internal Report Form

1. Fill out the basic details:
   - Date: date of the executed or intended unusual transaction;
   - Time: the exact time of the executed or intended unusual transaction;
   - Location: the address of the store/branch/office where the unusual transaction took place;
   - Employee: the name of the employee involved in the unusual transaction.
2. Check the relevant type of transaction:
   - Executed: if the transaction/deal has been closed;
   - Intended: if the transaction/deal has not been closed or has been aborted.
3. Check the type of Unusual transaction:
   - Law enforcement: when you report something to law enforcement that has a connection to money laundering or terrorism financing such as a customer paying with counterfeit bills, or false identification;
   - National sanction regulation: when a transaction is from or on behalf a natural person, legal person, group or entity in a country mentioned on the list adopted by the National sanction regulation;
   - Wire transfer: if the transaction involves a wire transfer of NAf 500,000. -- or above or in other currencies;
   - Cash unusual transaction: if the transaction is a cash transaction of NAf 25,000. -- or above or in other currencies;
   - Customer profile: when a transaction deviates from the profile of the customer;
   - Suspicious/fishy feeling: anytime you have a suspicious or fishy feeling that a customer or a transaction is connected to money laundering or terrorism financing.
4. Fill out the amount of the total transaction.
5. Fill out a description of the services/goods involved.
6. Check the type of customer.
7. Give an ample/broad description of the situation regarding the unusual transaction.
8. Attach the identification documents and the invoice/receipt (if applicable) to the internal report and give it to the Compliance Officer.

Procedure Internal reporting for the Compliance Officer

Unusual transaction reports using objective indicator

1. Compliance Officer receives internal report.
2. Compliance Officer fills out his/her part of the internal report.
3. Compliance Officer contacts the employee who filed the internal report.
    - If approved, go to step 5.
    - If information missing, go to step 4.
4. Collect missing information/documents from employee that filled out the internal report. When complete, go to step 5.
5. Sign for approval.
6. File an unusual transaction report (within 48 hours of transaction time)
    - Login on the SERT portal: http://portal.fiu-sxm.net/
    - Fill out a new report.
    - Call FIU Sint Maarten for confirmation letter.
7. Close the internal report and file it together with the confirmation letter.

Unusual transaction reports using subjective indicator

1. Compliance Officer receives internal report.
2. Compliance Officer fills out his part of the internal report.
3. Compliance officer contacts the employee who filed the internal report.
    - If approved, go to step 5.
    - If information missing, go to step 4.
4. Collect missing information/documents from employee that filled out the internal report. When complete, go to step 5.
5. Sign for approval.
6. Compliance Officer has 10 working days for an assessment of the internal report.
    - Decision to report? Go to step 8.
    - Decision not to report? Go to step 7.
7. Write down on the internal report the reasons for not reporting and close the internal report.
8. File an unusual transaction report (within 48 hours of the decision to report).
    - Login on the SERT portal: http://portal.fiu-sxm.net/
    - Fill out a new report.
    - Call FIU Sint Maarten for confirmation letter.
9. Close the internal report and file it together with the confirmation letter.

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 8: Training Log

Company Name:	Date:

Name/title training	*Name training organization and instructor*	*Participant(s) name(s)*	*Date of training and place*	*Type of training (on-site, or video, etc.)*	*Amount of hours*	*Date training completed and certificate received*

FINANCIAL INTELLIGENCE UNIT
Ministry of Justice - Sint Maarten

Template 9: Evaluation Log

Date evaluation	Topics of evaluation	Improvement points	Completed	Rating

ANNEXES

ANNEX 1: Risk analysis related to the services provided by the Gaming Service Providers

1. The FIU Sint Maarten makes a distinction between categories of risks. Categorization takes place between:
    I. Country risks.
    II. Customer risks.
    III. Transaction risks.

2. The outcome of the risk assessment is laid down in a risk profile which is determining the type of Customer Due Diligence (simplified, standard or enhanced) that the Company has to perform.

a. Country risks

Definition: Risk factors related to the origin of a customer, intermediate party, third person, product or institute involved in the transaction.

- Is the customer (natural person or company) from a jurisdiction/country with a higher risk on ML/TF?
- Are there intermediate/third parties in the transaction involved from a jurisdiction/country with a higher risk on ML/TF?
- Does payment come from a financial institute/party with an origin in a jurisdiction/country with a higher risk on ML/TF?
- Does the country of establishment of a customer score a 50 or less on the corruption perception index of Transparency International?
- Is the customer from a sanctioned jurisdiction/country?
- Are there intermediate/third parties in the transaction involved from a sanctioned jurisdiction/country?
- Does payment come from a financial institute with an origin in a sanctioned jurisdiction/country?
- Is payment done through a construction (legal, corporate or otherwise) by which the origin of the finance is unclear?

b. Customer risks

Definition: Risk factors related to the conduct, identification and characteristics of the customers of the Gaming service providers.

- *Is the conduct of the customer reason to suppose ML/TF risk factors?*
    - Is the conduct of the customer peculiar in any way (e.g. nervous)?
    - Is the customer mysterious or evasive about his/her identity?
    - Is the customer vague or evasive about the identity of the ultimate beneficial owner (UBO)?
    - Is the customer vague or evasive about the motive of the transaction?

- Does the customer try to avoid a personal meeting?
- Does the customer ask for unexpected speed?
- Is there a PEP that is engaged in unusual private business given the parties involved?
- Does the customer use an agent or intermediary without any apparent reason?

- *Is the identification of the customer reason to suppose risks for ML/TF?*
  - Is the customer evasive about its identity or the identity of the UBO?
  - Is it problematic to ascertain the identity of the customer or the UBO?
  - Is there a difference between the mailing address and the regular address of the customer?
  - Does the customer bear a regular address (e.g. use of shell bank, post box address, industrial zone)?
  - Does the customer provide false identification documentation?
  - Is the customer a company that cannot be found on the internet?
  - Is the customer a company using an unusual domain part such as G-mail, Hotmail etcetera?
  - Is there an absence of documentation to verify the customer's clarification of ID?

- *Are the characteristics of the customer reason to suppose risks for ML/TF?*
  - Does the transaction not coincide with the social economical profile of the customer?
  - Does the transaction not coincide with the age of the customer?
  - Does the transaction not coincide with the age of other parties involved?
  - Is the customer a Politically Exposed Person (PEP)?
  - Does the customer act on behalf of an unidentified person that he/she represents?
  - Are other parties involved in the transaction not formal parties to the transaction?
  - Is the person a high net worth individuals?

c. Transaction risks

Definition: Risk factors related to the establishment of the transaction, the chosen mode of payment or the payment construction and the source of payment funds in the transaction.

- *Are there risk factors related to the establishment of the transaction?*
  - Is the transaction established in an abnormal/unusual rapid way (e.g. no negotiations between parties)?
  - Does the customer act on behalf of an (unidentified) third party?
  - Do you have the impression that the customer uses third persons to give the transaction an appearance of legitimacy (e.g. straw man)?

- *Are there risk factors related to the chosen mode of payment or the payment construction or the source of payment funds in the transaction?*

- Does the customer or third party pay for the transaction with a large amount of cash?
- Does the customer or third party pay for the transaction with a company credit card?
- Is there a high level of cash payment for transactions just below the reporting threshold?
- Is payment of the transaction unusually large?
- Does payment of the transaction take place through an offshore bank account?
- Is payment of the transaction made by an (unidentified) third party?
- Is there insufficient knowledge about the customer's source of funds for the payment?
- Is there insufficient knowledge about the customer's source of wealth?
- Are there funds being sent to one or more countries with high levels of (bank) secrecy?
- Are there requests for payments to third parties?
- Is there an amount of cash in the transaction that is inconsistent with the socio-economic profile of the customer?
- Are there deposits of funds stalled without playing?
- Is the Source of Funds unusual as there is no apparent explanation?
- Is the Source of Funds unlikely given the professional profile of the customer?
- Is the transaction financed by a loan (back) construction?
- Is finance provided by a lender, other than a financial institution?

ANNEX 2: Minimum requirements compliance policy

Part of having a compliance regime is creating and implementing a compliance policy. The compliance policy is a manual that a service provider creates that is specific to its type of business. The compliance policy needs to contain an elaboration on certain subjects. These should be at least the following elements:

- Policy statement;
- Compliance Officer;
- Risk assessment;
- Customer Due Diligence;
- Unusual transaction reporting;
- Record keeping;
- Training;
- Evaluation of the compliance regime;
- Internal controls and communication;
- Approval.

1.1. Policy Statement

This section should include a general statement of the service provider's recognition of its legal obligations to have procedures and controls in place to deter, disrupt and detect money laundering and terrorist financing. This section should include, preferably, statements of declarations on:

- The culture and values to be adopted and promoted within the business towards the prevention of money laundering and the financing of terrorism.
- A commitment to ensuring all relevant staff are made aware of the law and their obligations under it and are regularly trained in how to recognise unusual transactions and suspicious activity.
- A commitment to adhering to the AML/CFT framework.
- Adoption and promotion of the prevention of money laundering and terrorism financing in the service provider's company.
- Ensuring that the risks in relation to money laundering and terrorism financing are properly assessed and managed.
- Ensuring that Customer Due Diligence is performed properly and according to standards.
- Ensuring that unusual transactions are being reported to the FIU Sint Maarten promptly and adequately.
- Ensuring that files are kept according to the record keeping requirements.
- Ensuring that the compliance regime is kept up to date with the latest AML/CFT obligations.
- Allocation of responsibilities to specific persons.

1.2. Compliance Officer

A Compliance Officer needs to be appointed. This section in the compliance policy needs to include:

- The contact details of the Compliance Officer.
- When the Compliance Officer was appointed and for which period.
- A description of the duties of the Compliance Officer.
- If there is an assistant Compliance Officer, his/her contact details.
- If there an assistant Compliance Officer, his/her delegated duties.

1.3. Risk Assessment

Service providers need to assess and manage the risks involved with their businesses. This section in the compliance policy need to include:

- A summary of the service providers approach to assessing and managing its money laundering and terrorism financing risks.
- A summary of the approach for reviewing and updating risks.
- A summary of the approach of reviewing controls so that the policies and procedures continue to effectively manage the risks.
- A description of the risks factors relevant for the service provider.
- A description of the risks assessment procedure.

If relevant, attach relevant risk assessment procedures/programs.

1.4. Customer Due Diligence (CDD)

Gaming service providers need to perform CDD on their customers. When there is a normal risk involved a standard CDD needs to be performed. A low risk coincides with a simplified CDD and a high risk with an enhanced CDD. The section on CDD in the compliance policy needs to include:

- A summary of the gaming service providers' procedures for carrying out appropriate CDD, including identifications and verification of the identity of the customers.
- A summary of the service providers monitoring checks on the basis of their risk based approach.
- Clear distinction between different types (standard, simplified, enhanced) CDD and when these specific CDD procedures will be applied.
- Ensuring that employees have satisfactory systems and procedures in place for undertaking CDD.
- All extra measures that (in case of a high risk) are going to be taken by the gaming service providers.

If relevant, attach relevant CDD forms or templates.

1.5. Unusual Transaction reporting

The gaming service provider is obliged to report unusual transactions if encountered during the course of business. The Compliance Officer is the main responsible person for reporting unusual transactions to the FIU Sint Maarten. It is advised, especially in companies with more than two (2) employees, to have an internal reporting procedure in order to facilitate the compliance officer's reporting job. This section in the compliance policy should include:

- A description of the internal reporting procedure.
- A description of the reporting procedure of the Compliance Officer.
- The analysis or monitoring procedure to detect unusual transactions.
- The consent procedure for carrying out transactions.
- A summary of the reporting indicators.
- A description of the red flags that can be used in the service provider's business.

If relevant, attach relevant internal reporting forms or procedures.

1.6. Record Keeping

Records need to be kept accessible and secure for ten (10) years after a business relationship with a customer has ended. This section in the compliance policy needs to include:

- An explanation on how transaction, payment and CDD information is recorded and held.

1.7. Training

The staff of the gaming service providers, including the Compliance Officer and management, need to be trained on AML/CFT risks, trends and methods. The section on training needs to include:

- A description of the training procedure.
- A description of which employees are trained and when.
- A description of how training documentation is kept.
- A description of training methods and topics.

If relevant, attach relevant documentation.

1.8. Evaluation

Every three (3) years the compliance regime of the gaming service providers needs to be evaluated by an external evaluation. This section in the compliance policy needs to include:

- A description of the point on which the compliance regime will be evaluated.
- The contact details of the external evaluator.
- Other practical agreements made with the external evaluator.

If relevant, attach relevant documentation.

1.9. Internal controls and communication

A good internal control and communication procedure is essential in complying with the AML/CFT obligations. This is especially important in a large company where there are different types of functions, roles and responsibilities. This section in the compliance policy needs to include:

- Senior management responsibilities.
- Control mechanisms/procedures to make sure that employees follow internal procedures.
- Control mechanisms/procedures to make sure that the Compliance Officer follows internal procedures and abides by the duties given to him/her.
- Procedures for dealing with new employees or employees that have changed function.
- Procedures and frequency of evaluation of the Compliance Officer.
- Procedures and frequency of evaluation of the employees.
- Communication methods and frequency of this between senior management and the Compliance Officer.
- Communication methods and frequency of this between the Compliance Officer and the employees.
- A summary of the appropriate monitoring arrangements in place to ensure that the gaming service providers' policies and procedures are being carried out.

If relevant, attach relevant documentation.

1.10. Approval

The compliance policy needs to be approved and signed for by senior management. This section needs to include:

- A statement of approval by senior management.
- Signature of senior management.
- Name of the person in senior management that has signed for approval.

ANNEX 3: Guideline on the evaluation of the compliance regime

A. Goal
B. Checkpoints
C. Report of the evaluation

A. Goal

Gaming service providers have to implement a compliance regime in order to comply with the AML/CFT obligations. The compliance regime consists of the following elements:

1) A written compliance policy and internal procedures.
2) A Compliance Officer.
3) An ongoing training program.
4) Evaluation of the compliance regime.

In order to make sure that the compliance regime is implemented correctly and effectively it has to be evaluated every three (3) years by an external independent person or company.

Who can be an evaluator?

- An external person/a company: someone who or a company that is not involved in the day to day business of the gaming service providers;
- Professional level: someone who or a company that has a track record of experience in the field of compliance;
- Knowledgeable of or able to learn the AML/CFT framework and requirements.

What is NOT part of the evaluation?

The intention of the evaluation is to focus on the procedures and the effectiveness thereof of the gaming service providers. It is not the intention for the evaluator to look into transactions, reported or not reported, or customer/customer files. This is the task of the supervisors of the FIU Sint Maarten. The Compliance Officer of the company is not allowed to show the evaluator the customer/customer files as this is against the confidentiality clause as mentioned in Art. 20 of the NOFIU.

Before starting an evaluation

It is very important to read the P&G of the respective sector that is going to be evaluated as it contains extended information on the obligations concerned. Throughout this guideline reference will be made to specific relevant chapters of the P&G. A suggestion is also to enter into a confidentiality agreement between the evaluator and the company.

B. Checkpoints

These are the points of a compliance regime that at least need to be reviewed by the evaluator:

1) Risk assessment in connection with nature, size and complexity of the business.
2) Compliance policy.
3) Compliance Officer.
4) Training program.
5) Internal procedures of the company.
   - Customer Due Diligence (CDD);
   - Reporting of Unusual Transactions;
   - Recordkeeping;
   - Controls & Communication.

Ad 1. Risk assessment in connection with the nature, size and complexity of the business
The gaming service providers have to take on a risk based approach when doing business. They have to perform a risk assessment and have risk profiles of their customers/customers/products/services. The risk factors that need to be considered/weighed are:

A. Product/service risks.
B. Customer/customer risks.
C. Country/geographical risks.
D. Transaction risks.

Risk assessments can have three possible outcomes; Low, Medium or High Risk. However, there are certain factors that will immediately be a High Risk, no matter which type of business the gaming service provider carries out. These are:

- Politically Exposed Persons (PEPs);
- High Risk countries;
- Non-face-to-face customers/customers.

For more information on the risk factors, High risk and risk assessment in general, please be referred to Chapter 2 of this P&G.

What an evaluator needs to review:

- Is the risk assessment method/program adequate?
  - ✓ Is it according to the nature, size and complexity of the business?
  - ✓ Does it pinpoint higher risks?
  - ✓ Is it documented?
  - ✓ How often is it updated?
  - ✓ Are all the risk factors taken into consideration?
  - ✓ Is the one performing the risk assessment knowledgeable in AML/CFT?
- Is the risk assessment actually performed in an adequate way?
  - ✓ Are there risks assessments of the business?

Suggestions of methods to review the above:

- Observation of the risk assessment procedure.
- Interview with the Compliance Officer.

Ad 2. Compliance policy
Every gaming service provider should have a written AML/CFT compliance policy. In this policy, the gaming service provider needs to elaborate on how to comply with its AML/CFT obligations and establish procedures in order to comply with these. Minimum subjects that need to be elaborated upon in a compliance policy are:

- A commitment of the gaming service provider to abide by the AML/CFT framework.
- The identifying and assessing of potential risks.
- Customer Due Diligence policy: on acceptable identification and verification, assessing business relationship with the customer in case of variations on CDD what measures the gaming service provider takes.
- On-going monitoring procedures.
- Internal controls and communication (staff, Compliance Officer and senior management).
- Monitoring and managing of compliance with legislation.
- Unusual transaction reporting.
- Record keeping of information.

- Training of staff.
- The role of the Compliance Officer.
- Procedure for the evaluation of the compliance regime.

Furthermore, besides the abovementioned minimum subjects, a compliance policy needs to be:

- Kept up to date;
- Approved by senior management;
- Known to staff, especially the ones who deal with customers, transactions or recordkeeping.

The level of detail of the compliance policy is based on the nature, size and complexity of the business.

For more information on the compliance policy please be referred to Chapter 5 of this P&G and the respective template of the compliance policy that the FIU Sint Maarten distributed to the service providers.

What an evaluator needs to review:

- Is there an adequate AML/CFT compliance policy?
  - ✓ Are all the minimum subjects covered in the compliance policy?
  - ✓ Is it in written form?
  - ✓ Are the procedures described in accordance with the size, nature and complexity of the business?
  - ✓ Is the policy approved by senior management?
- How frequent is the policy reviewed and updated?
  - ✓ Is it adapted to changes in procedures, legislation etcetera?
- Is the policy known to staff?
- Are there repercussions on not following the policy?

Suggestions of methods to review the above:

- Interview with senior management.
- Interview with relevant staff to check awareness.
- Check policy.

Ad 3. Compliance Officer

The gaming service providers should appoint a Compliance Officer. The Compliance Officer should be responsible for the implementation of the compliance regime. The duties of the Compliance Officer are at least:

- Report unusual transactions to the FIU Sint Maarten;
- Giving training, advice and direction to employees or management on how to comply with AML/CFT framework;
- Assess internal unusual transaction reports on correctness and complexity;
- Keep records of all reported unusual transactions;
- Being a contact between the service provider and the FIU Sint Maarten;
- Screen new employees.

The Compliance Officer can be an internal person from within the company or it can be someone that is appointed externally. If the gaming service provider is a small business (less than 15 employees), someone from senior management can be appointed as the Compliance Officer. The requirements for the Compliance Officer are:

- The Compliance Officer should be at least at management level to understand and implement the requirement;
- The Compliance Officer should operate independently;
- The Compliance Officer should have unrestricted access to relevant information.

If the tasks of a Compliance Officer are delegated to another person, this person's functioning should also be scrutinized.

For more information on the Compliance Officer and his/her duties and responsibilities please be referred to Chapter 5 of this P&G and the respective template of the compliance policy that the FIU Sint Maarten distributed to the gaming service providers.

What an evaluator needs to review:

- Is there a Compliance Officer appointed at manager level?
- Does the Compliance Officer operate independently?
    - ✓ Does the compliance Officer need approval from senior management for anything? If so, for what?
    - ✓ Does the Compliance Officer have access to information?
    - ✓ Does the Compliance Officer make decisions independently? If so, for what?
- Does the Compliance Officer have an overview of the AML/CFT framework related to the gaming service provider?
- Does the Compliance Officer adhere to the internal reporting procedure?
- Does the Compliance Officer adhere to the reporting procedure to the FIU Sint Maarten?
- Does the Compliance Officer have enough time to comply with obligations/tasks? How fast are tasks completed?
- Does the Compliance Officer have sufficient AML/CFT knowledge?
    - ✓ Does he/she keep the knowledge up to date?
    - ✓ How frequent does he/she follow training?
- How does the Compliance Officer communicate with staff/management?
- How does the Compliance Officer react to changes in the AML/CFT framework?
    - ✓ How does the Compliance Officer incorporate/implement changes?
- What is the procedure for new employees?
    - ✓ Does the Compliance Officer help screen the new employee?
    - ✓ Does the new employee receive an introductory training before start of function?
    - ✓ Does the new employee get a copy of the compliance policy?

Suggestions of methods to review the above:

- Interview with and observation of the Compliance Officer.
- Interview with senior management.
- Interview with employees.
- Observation of reporting procedure.
- Check policy for tasks and responsibilities Compliance Officer.

Ad 4. Training program

The gaming service providers must make sure its staff and management have up-to-date knowledge of the AML/CFT framework. That is why the gaming service provider needs to have an ongoing training program set up. Requirements for the training are:

- Training has to be once a year at least;
- The training program should be documented;
- Training should be for all staff members, but in any case:
    - ✓ Members of staff working in the field of CDD, recordkeeping and transactions.

- ✓ The Compliance Officer.
- ✓ Management.

Training should cover, at least, the following topics:

- general information about money laundering and terrorism financing.
- an explanation of the AML/CFT framework of Sint Maarten and an indication of expected developments.
- the sanctions that can be imposed if a gaming service provider violates the AML/CFT framework.
- the identity, tasks and responsibilities of the Compliance Officer.
- the potential effect of any breach of the law on the business, its employees and its customers.
- the risks of money laundering and terrorism financing that the business faces.
- the vulnerabilities of the business' products and services.
- new technologies with regards to money laundering and terrorism financing.
- the policies, (identification and verification of customer) procedures and controls that have been put in place to reduce and manage the risks.
- risk based CDD measures.
- how to recognize unusual transactions and potential suspicious activity.
- the procedures for making a report to the Compliance Officer including who can do this.
- the procedure of record keeping.
- the circumstances when consent is to be sought from senior management (for example when taking on PEPs as customers) and the procedure to be followed in such a case.
- reference to money laundering typologies in the respective business sector.
- screening procedures to ensure high standards when hiring employees.
- adequate safeguards on the confidentiality and use of information exchanged, should be in place.
- reference to specific sources of information, e.g. world check, world compliance, OFAC.

For more information on training, please be referred to Chapter 5 of this P&G.

What an evaluator needs to review:

- Is there an ongoing training program?
  - ✓ Is there documentation on followed training?
  - ✓ Is there a training log?
  - ✓ Is there an official organization that provides training?
- Has training been followed by all staff members?
  - ✓ Once a year?
  - ✓ Are there certificates?
  - ✓ Who followed training?
- Is the AML/CFT framework knowledge of employees sufficient?
- Is the AML/CFT framework knowledge of management sufficient?
- Have all new employees followed training? What is the procedure?
- What is the procedure to adjust training to the needs of the gaming service provider?

Suggestions of methods to review the above:

- Review training material.
- Interview employees.

- Interview management.
- Interview Compliance Officer.
- Review training program procedures.

Ad 5. Internal procedures

There are different internal procedures that a gaming service provider needs to have in order to comply with the AML/CFT framework. The mandatory ones are related to CDD, reporting of unusual transactions and recordkeeping. These procedures need to be, preferably, written down in the compliance policy of the gaming service provider.

Customer Due Diligence (CDD)

Based on the risk assessment made CDD needs to be performed. In case of a Medium, Low or High Risk, respectively a standard, simplified or enhanced CDD needs to be performed. The standard CDD consists of four (4) elements:

1. Identification and verification of the identity of the customer/customer.
2. Identification and verification of the identity of the UBO.
3. Understanding the nature and purpose of the business relationship.
4. Ongoing monitoring.

The simplified and enhanced CDD are variations of the standard CDD, whereby in case of a simplified CDD less questions are asked, and in case of an enhanced CDD extra questions are asked. For an enhanced CDD, in any case, the Source of Funds (SOF) is an extra measure that has to be taken. The other extra measures are based on the gaming service provider's judgement but need to be proportionate and commensurate with the Risk.

For foreign PEPs, specific extra measures are required to be taken (please be referred to paragraph 2.5.2.1 of this P&G). A simplified CDD is not mandatory but a standard and enhanced CDD are.

Please be referred to Chapter 2 of this P&G for more information of the different CDD measures.

What an evaluator needs to review:

- If CDD is being performed in accordance with the AML/CFT framework
  - ✓ Are customers/customers being identified in a proper way?
  - ✓ Are UBOs being identified in a proper way?
  - ✓ Is there an understanding of the nature and purpose of a business relationship?
  - ✓ Is the frequency of monitoring adequate according to the risk?
- Is enhanced CDD being performed in an adequate way
  - ✓ Are the extra measures proportionate and commensurate with the risks?
  - ✓ Is the frequency of monitoring adequate?
  - ✓ Is the SOF being asked of the customer/customer?
  - ✓ Are there correct measures being taken in case of a foreign PEPs?

Suggestions of methods to review the above:

- Review of the CDD procedures.
- Testing of CDD procedures.

Reporting of Unusual transactions

The reporting of unusual transactions is based on specific indicators. These specific indicators can be found in Chapter 3 of this P&G. The Compliance Officer is responsible for the reporting of unusual transactions to the FIU Sint Maarten. In a company with more than one (1) employee it is

recommended to have an internal reporting procedure. The employees that handle transactions should report to the Compliance Officer when an unusual transaction is discovered. The Compliance Officer will then assess the internal report and report on his/her turn to the FIU Sint Maarten.

What an evaluator needs to review:

- Are the right transactions being reported to the Compliance Officer?
  - ✓ Do employees understand the indicators?
- Are the right transactions being reported to the FIU Sint Maarten?
  - ✓ Does the Compliance Officer understand the indicators?
- Is the internal reporting procedure functioning properly?
  - ✓ Is all the necessary information available?
- Is confidentiality adhered to?
  - ✓ Are the employees aware of the *no tipping off* clause?
  - ✓ Is the Compliance Officer aware of the *no tipping off* clause?

Suggestions of methods to review the above:

- Review of the internal reporting procedure or forms.
- Interview with employees dealing with transactions.
- Interview with Compliance Officer.

Recordkeeping

A gaming service provider needs to keep transaction records, CDD records and reporting records for at least ten (10) years after a business relationship has ended.

For more information on recordkeeping, please be referred to Chapter 4 of this P&G.

What an evaluator needs to review:

- Are files/records being created of transactions and/or customers/customers?
- Is a distinction being made between local and foreign?
- Are the files accessible in case of an audit by the FIU Sint Maarten?
- Are the files dated properly?

Suggestions of methods to review the above:

- Test of record keeping system.
- Interview Compliance Officer.
- Observation of archives.

Internal controls & communication

It is important that there be sufficient communication between the Compliance Officer, management and the employees to make sure that everybody knows what their responsibility is pertaining to the AML/CFT framework related to the gaming service provider. Internal controls are also necessary to make sure that the gaming service provider identified weaknesses on time in order to correct them. This is especially vital in a medium to large sized company with a large staff.

What evaluators need to review:

- Is there sufficient communication between Compliance Officer & employees?
  - ✓ Does the Compliance Officer evaluate the employees?
  - ✓ How frequent do meetings/evaluations take place?
  - ✓ Are meetings recorded in minutes?

- ✓ How are problems/issues identified or brought up?
- ✓ How are solutions being created for problems raised?

- Is there sufficient communication between Compliance Officer & management?
  - ✓ Does the Compliance Officer give feedback to management? How often?
  - ✓ Are meetings recorded in minutes?
  - ✓ How are problems/issues identified or brought up to management?
  - ✓ How are solutions being created for problems raised?

Suggestions of methods to review:

- Interview Compliance Officer.
- Interview employees.
- Interview management.
- Review minutes/notes of meetings.

C. Report of the evaluation

The evaluation needs to be properly documented. The report should contain at least:

- the scope of the evaluation;
- the findings of the evaluation;
- any updates that were made to the policies and procedures during the evaluation period;
- status of implementation of abovementioned changes;
- identified deficiencies and weaknesses in policies and procedures;
- recommended corrective actions and follow-up actions.

Comments & reactions senior management

- Within 30 days of the evaluation the evaluator writes a report and sends it to senior management of the gaming service provider together with a request for comments and reactions.
- Senior management gives its comments within 14 days of receiving the report. In their comments they have to indicate a reasonable timeline for taking the follow-up actions.
- The evaluator has 14 days to finalize the report after receiving the comments of senior management of the gaming service provider. After finalization of the evaluation report it is signed by the evaluator and senior management.
- Hereafter, a copy of the report is sent to the Supervision Department of the FIU Sint Maarten within 30 days of finalization of the report.

Any questions or comments? Please contact the Supervision Department of the FIU Sint Maarten at: Supervision.department@fiu.gov.sx or call us on 542-3025 ext. 116.