PROVISIONS AND GUIDELINES FOR LAWYERS, NOTARIES, ACCOUNTANTS, TAX ADVISORS AND ADMINISTRATION OFFICES

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

August 2020
Financial Intelligence Unit

Ministry of Justice
Sint Maarten

Contents

1 INTRODUCTION

1.1. Introduction

Sint Maarten is a member of the Caribbean Financial Action Task Force on Money Laundering (CFATF).[1] The members adhere to the Financial Action Task Force (FATF) Recommendations.

The FATF 40 Recommendations are the international standards on combating and preventing money laundering and the financing of terrorism.[2] 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 Designated Non-Financial Businesses and Professions (DNFBP).
The purpose of these Provisions and Guidelines (P&G) is to provide the DNFBP's that are supervised by the Financial Intelligence Unit (FIU) with comprehensive legally binding guidance on implementing the legal requirements for measures designed to deter, detect and disrupt money laundering and terrorism financing. The DNFBP sector includes: Accountants; Lawyers; Tax Advisors; Car Dealerships; Jewelers; Real Estate Agencies; Administration Offices; Notaries; Pawn-shop; Project Developer; Games of Chance (casinos, lotteries, online gaming); Appraisers; Construction material suppliers and Rights of artworks or antiques and all other persons and companies that provide the services pursuant to article 2, paragraph 1, under b, sub 1° of the National Ordinance Combating Money Laundering and the Financing of Terrorism, AB 2019, GT no. 25. This particular P&G applies to the car dealers. For the services relevant to this group, please be referred to paragraph 1.6.

The Anti-Money Laundering (AML) legislation for Sint Maarten is laid down in the National Ordinance Combating Money Laundering and the Financing of Terrorism. Abovementioned legislation regards both financial as non-financial services.
In order to prevent the service provider from being abused for money laundering activities or the financing of terrorism, the National Ordinance Combating Money Laundering and the Financing Terrorism specifies that the service provider must identify the customer and 'the ultimate beneficial owner' (UBO) before providing a service to the customer or UBO. After the service provider has entered into a business relationship, the service provider will continue applying CDD to the customer. Furthermore, pursuant to the National Ordinance Combating Money Laundering and the Financing of Terrorism, the service provider is obliged to report unusual transactions to the FIU.

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

FIU pays utmost attention to the reliability and timeliness of the information provided in

[1] www.cfatf-gafic.org
[2] See www.fatf-gafi.org

this document. However, please note that the contents of these regulations and guidelines are subject to change, based on the dynamic FATF recommendations and the policies applied by the supervisor. 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 and / or amendments to these regulations and guidelines as well as other documents in the field of combating money laundering and terrorist financing.

1.2 Money laundering

Money laundering is rendered a criminal offence pursuant to the National Ordinance on a new penal code (AB 2013, no. 2) 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 stages:

- **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 (cheques, money orders, etc.).

- **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 recommendations.

- **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

Under Article 2:55 of the National Ordinance on a new penal code (AB 2013, no. 2)

terrorism and terrorist financing constitute a criminal offense on Sint Maarten. Terrorism financing provides funds for terrorist activity. It may involve funds raised from legitimate or criminal sources. With terrorism financing, the money need not necessarily originate from criminal acts, however it is used to support terrorist movements financially.

Terrorism is 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.

Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries 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.

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 legislation creates an obligation for the service provider to apply a risk-based approach (RBA) when establishing and continuing a service relationship with a customer. It is the service provider who bears the responsibility and legal obligation to undertake this risk assessment before establishing and when continuing a service relation with the 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 Financial Intelligence Unit (FIU) has the legal authority to supervise compliance with the risk assessment by the service provider. These Provisions and Guidelines offer guidance, among other things, on how to apply the risk based approach. It is up to the service provider to develop internal compliance policies and procedures in order to be able to fulfil its legal obligations.

1.5 Provisions and Guidelines

Pursuant to the NORUT (art. 22h, paragraph 3) and the NOIS (art. 2, paragraph 5 in conjunction with 11, par. 3), the FIU has the legal authority to issue binding guidelines.

The purpose of the P&G is to provide DNFBP that are supervised by FIU 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 finance 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 legislation and the P&G will result in administrative sanctions (e.g. penalty payments or fines)[3] being imposed on the service provider. Furthermore, an intentional or unintentional breach of the legislation and the P&G is considered an offence respectively a misdemeanor which can result in criminal sanctions (imprisonment or a fine)[4] being imposed on the service provider. Information on the legal procedure and enforcement of the legislation and these P&G will be given in chapter 6.

1.6 Who need to comply with the provisions and guidelines?

The duty to perform CDD and the reporting obligation is applicable to the service provider who, in or from Sint Maarten, renders a service as a profession or as a trade, as mentioned in article 1, paragraph 1, sub a, under 15 of the NORUT and article 1, paragraph 1, sub b, under 15 of the NOIS.

These services comprise the provision of advice or assistance for:

a. purchasing or selling real estate;
b. managing funds, securities, coins, government notes, precious metals, precious stones or other values;
c. establishing (incorporation) and managing of corporations, legal persons or similar bodies
d. buying, selling or taking over enterprises.

<u>Re a: the purchase or selling of real estate</u>
This service is interpreted in a broad sense. It includes all legal constructions that are used in order to achieve a purchase or sale of real estate. It includes the purchase or sale of a right of long lease.

<u>Re b: managing funds, securities, coins, government notes, precious metals, precious stone or other values</u>
This involves the custody or management of money and other valuables. It might, for

[3] Please see articles 22a and 22b paragraph 1 of the NORUT and article 9 and 9a paragraph of the NOIS
[4] Please see articles 23 of the NORUT and article 10 of the NOIS.

instance, involve the management of estate funds or acting as an administrator. The management of money, securities (shares) or other valuables would also include the provision of advice or assistance for opening or managing an account or advising in which jurisdictions financial resources could be invested.

Re c: establishing (incorporating) or managing of corporations, legal persons or similar bodies
The legal nature of the business organization, whether sole proprietorship, BV, NV, (limited liability) partnership, LLC or any other legal form of operation is not decisive for the applicability of the AML legislation and these P & G.

Re d: purchasing, selling and taking over businesses
This involves for example the provision of (legal) advice or assisting in the process of business acquisitions, which includes amongst others the purchasing or selling and (fiduciary) transferring of shares, tangible and intangible assets and/or other personal or absolute (property) rights related to the business. It furthermore includes among others. the provision of (legal) advice or assisting in mergers, management buy outs, dissolution of business organisations and winding up of a business. In general it covers all possible civil and company law advice or assistance in the process of purchasing, selling and taking over a business. The given examples of related activities are therefore not limitative but merely give an indication.

1.7 Duty to register

The service provider that provides services as mentioned in the legislation also has a duty to register at the Financial Intelligence Unit (FIU). In order to register the service provider has to complete a registration form. After completing the registration form, this will be (digitally) filed in the registry of the FIU. The registration form can be downloaded from the website of the FIU.

1.8 Exemptions with regard to professional secrecy

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report unusual transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. This exemption only covers information that lawyers, notaries or other independent legal professionals receive from or obtain through one of their customers:

a. In the course of ascertaining the legal position of their customer
b. In performing their task of defending or representing that customer in, or concerning judicial, administrative, arbitration or mediation proceedings.

Work relating to representing and defending a customer in court of law, ascertaining the

legal position of a customer, providing advice or assistance before, during and after a legal action in court proceedings or providing advice or assistance about instigating or avoiding legal action in court proceedings is therefore exempted.
Note should explicitly be made that this exemption of legal obligations does not apply when afore-mentioned service providers advice or provide assistance in determining the legal position of a customer with regard to the designated services, as mentioned in article 1, paragraph 1, sub a, under 15 of the NORUT and article 1, paragraph 1, sub b, under 15 of the NOIS.

1.9 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 by filling out the organizational change form. Please be referred to template 1.

2 RISK BASED CUSTOMER DUE DILIGENCE (CDD)

2.1 Introduction

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 service provider a profounder understanding of the identity of the customer and/or the Ultimate Beneficial Owner (UBO)[5] with whom he is doing business. The CDD includes identifying and verifying the customer and the UBO, if applicable, as well as taking other appropriate measures. The CDD measures are based on Recommendation 22 in conjunction with Recommendation 10 of the FATF.

The service provider is required to undertake CDD measures when:

- establishing business relations;
- carrying out occasional transactions that are above the applicable designated threshold:
  1. Cash transactions of NAf 25.000,- or above or the equivalent thereof in another currency
  2. Electronic transfers (including wire transfers) of NAf 500.000,- or above or the equivalent thereof in another currency
- transactions that are associated with money laundering or the financing of terrorism;
- there is a suspicion of money laundering or terrorism financing regardless of any exemptions or thresholds; or
- the service provider has doubts about the veracity or adequacy of previously obtained customer identification data.

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 service provider already disposes of relevant and valid CDD information there is no need to request this information once again) and should be conducted at appropriate times.

2.2. Risk Assessment

A risk based approach 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 some service providers may find useful.

[5] UBO is described as follows in terms of article 1, paragraph 1, under (j) of the NOIS. The UBO is a natural person who owns or holds a qualified participation or interest in a legal entity or company, or a natural person who is entitled to the assets or income from a trust or private foundation fund. A qualified participation or interest, in terms of article 1, paragraph 1, under (k) of the NOIS, is a direct or intermediate interest of 25% or more of the nominal capital, or a comparable interest, or the direct or intermediate ability to exercise 25% or more of the voting rights, or the direct or intermediate ability to exercise comparable control.

2.2.1. Moment of risk assessment

Risk assessments have to be performed throughout the course of business with the client but in any case, in written form, when:

- establishing business relations;
- carrying out occasional transactions that are above the applicable designated threshold

  1. Cash transactions of NAf 25.000,- or above or the equivalent thereof in another currency
  2. Electronic transfers (including wire transfers) of NAf 500.000,- or above or the equivalent thereof in another currency
- there is a suspicion of a client/transaction being involved with money laundering or terrorism financing, regardless of the transaction amount.

2.2.2 Risk categories

Risks can be found within four categories. We distinguish:

A. Country risks: Risk factors related to the origin of the customer, intermediate party, third person, beneficiary, product or institute involved in the transaction;
B. Customer risks: Risk factors related to the conduct, identification and characteristics of a client;
C. Product/service risks: Risk factors related to the characteristics of the service;
D. Transaction risks: Risk factors related to the establishment of the transaction, the chosen mode of payment and/or the payment construction and the source of payment funds in the transaction and/or the chosen method of delivery.

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

2.3. Customer Due Diligence (CDD)

According to the outcome of the service provider's assessment of the risk, there are three types of CDD that can be executed, namely:

1. Standard CDD
2. Simplified CDD
3. Enhanced CDD

The fact that the customer falls into one of the following risk categories does not automatically mean that money laundering or financing of terrorism is the case. The service provider should ensure that it has its own internal procedures in place with relation to the CDD.

2.3.1. Standard CDD

The Standard CDD comprises:

a. Identifying the customer and verifying that customer's identity using valid and reliable, independent source documents, data or information.

b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a way that the service provider knows who the actual beneficial owner is. In case the customer is a legal person, a partnership or any other legal entity, the CDD should include the service provider understanding of the ownership and the control structure of the customer.

c. Understanding and obtaining information on the purpose and intended nature of the business relationship.

d. Conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the service provider's knowledge of the customer, the business, the source of funds and the formulated risk profile.

Re a.: This means that the service provider should take duly care to establish the identity of the customer and the UBO in accordance with the provisions of the NOIS. This covers both identification of the customer and UBO and verification of their identity.

Re b.: This means that the service provider should take reasonable steps, if the customer is a legal person or any other legal business entity (e.g. syndicate, joint venture or partnership), to gain an understanding of the customer's ownership and control structure. This will involve the service provider establishing the identities of the natural persons who have controlling interests.

Re c.: This means that the service provider should establish the objective and intended nature of the business relationship. This includes an inquiry into the nature, origin and ultimate purpose of the goods involved in the transaction(s).

Re d.: This means that the service provider needs to perform an on-going check of the business relationship and the transactions undertaken, in order to test whether the customer information still complies with the risk profile that has been defined.
The service provider should set up an internal compliance regime in order to be able to professionally fulfil its obligations under the law as set out above under a, b, c and d. Please be referred to Chapter 5 for further information about the compliance regime.

When performing the CDD, please note that there may be new technologies (for example; the use of bitcoins, prepaid cards, internet payment) you need to be aware of in order to perform the CDD as accurate as possible. The service provider needs to be aware and updated with regards to these new technologies. In order to do this, the service provider needs to follow training in this regard.

If the service provider has already entered into a business relationship with the customer, it is obliged to terminate this relationship if it appears that it has not been able to perform parts a to c of the Standard CDD.

Once the business relationship has been terminated, the service provider should consider whether the specific circumstances amount to an (attempted) unusual transaction that should be reported to the FIU on the basis of the subjective indicator. For assessing the nature of a subjective indicator we refer to par. 3.2.2.

An example of a standard CDD form can be found in template 4.

2.3.2 Identification and verification

According to article 4 of the National Ordinance Combating Money Laundering and the Financing Terrorism, the service provider is obliged to establish the identity of the customer and/or the UBO, before providing a service to the customer. Identification involves the customer providing proof of his identity by handing over a valid identification document. A valid identification document is an Identification card, passport or driver'.

The service provider must sign and date on the copy of the client's identity document by

whom and when identification took place.

Pursuant to article 5 paragraph of the National Ordinance Combating Money Laundering and the Financing Terrorism it is prohibited to render a service, if the identity of a customer has not been established in the manner described in the National Ordinance Combating Money Laundering and the Financing Terrorism. This means that providing services to anonymous customers and customers with fictitious names is not permitted.

The method of identifying a customer and a UBO (whether local or foreign) that is a natural person or legal person is set forth in article 7 and 10 of the National Ordinance Combating Money Laundering and the Financing Terrorism. The service provider should then verify that the identity that has been provided coincides with the actual identity. Under Article 17, of the National Ordinance Combating Money Laundering and the Financing Terrorism, verification is based on the use of valid, reliable and independent sources.

2.3.2.1 Method of identification

I. Natural person(s)

Residents and non-residents that are temporarily present on Sint Maarten:
The service provider must have identified the natural person prior to providing the service, on the basis of a valid, original identity document. The following identification documents are currently allowed:

- a valid driver's licence;
- a valid identity card[6];
- a valid travel document or passport;
- another document to be designated by the Minister. Pursuant to the Ministerial Decree, the original of a valid residence permit accompanied by a valid passport is designated as such a document. If the original residence permit or the valid passport cannot be submitted, copies of these documents will suffice if accompanied by the submission of a statement issued by the competent authorities.[7]

Non-residents (not present on Sint Maarten during the transaction):

- a photocopy of a driver's licence, identity card or passport, provided that the photocopy in question is accompanied by a certified copy or extract from the Civil Registration Office of the domicile or residence of the customer; or
- forwarding one of the above-mentioned documents electronically, provided that the service provider receives a certified copy of said document, that is sent within two weeks after receiving the documents electronically.[8]

II. Legal person(s) or corporation(s)

[6] An identity card issued by the employer for an employee (an "employee identification card") is **not** allowed.
[7] Article 8 of the Ministerial Decree dated 15 March 2010 implementing the NOIS (N.G. 2010, no.11).
[8] This facility for identification, if the customer is a natural person, is included due to the international developments in the electronic field (see the National Ordinance on Electronic Agreements), but without detracting from the "Know your Customer" principle.

The identity of a legal person or corporation may currently be established using:

- a certified extract from the register of the Chamber of Commerce and Industry, or a similar institution in the country of establishment; or
- an identification document to be prepared by the service provider;.

The extract or identification document prepared by the service provider must contain the information specified by the Minister at the minimum. This information is[9]:

a. for the legal person or corporation: the legal entity, the registered (official) name, the trade name, the complete address, the place of establishment, country of registered office and, if the legal person or corporation is registered at a Chamber of Commerce and Industry or similar institute, the registration number as well as the country or island territory where that Chamber or similar institute is established.
b. for all proxy holders and authorized representatives: the name and date of birth and the document that is used for identification purposes.

<u>Legal person under public law in Sint Maarten</u>

The identity of a legal person or corporation under public law in Sint Maarten may currently be established using:

- a declaration of the management;
- a certified extract from the register of the Chamber of Commerce and Industry or similar institution ; or
- an identification document to be prepared by the service provider.

The extract or identification document must contain the information specified by the Minister at the minimum. This information is:

a. for the legal person or corporation: the legal entity, the registered (official) name, the trade name, the complete address, the place of establishment, country of registered office and, if the legal person or corporation is registered at a Chamber of Commerce and Industry or similar institute, the registration number as well as the country or island territory where that Chamber or similar institute is established;
b. for all proxy holders and authorized representatives: the name and date of birth and the document that is used for identification purposes.[10]

<u>Legal person under foreign public law</u>

The identity of a foreign legal person under public law may currently be established using:

- a certified extract from the register of the Chamber of Commerce and Industry or similar institution ; or
- an identification document to be prepared by the service provider; or
- a declaration issued by the competent authority.

For an example of an identification document to be prepared by the service provider, please be referred to template 6.

[9] Article 9 of the Ministerial Decree dated 15 March 2010 implementing the NOIS (N.G. 2010, no.11).
[10] Ministerial Decree dated 15 March 2010 implementing the NOIS (N.G. 2010, 11)

The extract or identification document must contain the information specified by the Minister at the minimum. This information is:

a. for the legal person or corporation: the legal entity, the registered (official) name, the trade name, the complete address, the place of establishment, country of registered office and, if the legal person or corporation is registered at a Chamber of Commerce and Industry or similar institute , the registration number as well as the country or island territory where that Chamber or similar institute is established;
b. for all proxy holders and authorized representatives: the name and date of birth and the document that is used for identification purposes.

2.3.2.2 Ensuring a valid identity document

When a service provider is providing services to an existing customer and/or UBO without having a valid identification document in his file, the service provider must first request a valid identity document from the existing customer and/or UBO before providing the service.

2.3.2.3 One time only identification

If a customer and UBO have been identified in accordance with the provisions in the NOIS, no further new identification is required for each new service. One time only identification in accordance with the NOIS is sufficient when performing a CDD. The service provider is entitled to rely upon the steps he has already taken to establish the identity, unless there is any doubt about the accuracy of the information. Reference is made in this context to the provisions in article 3, paragraph 6 of the NOIS. This sub-article specifies that the service provider must ensure of the correct identity information of the customer/UBO. If the information in question no longer coincides with reality, the service provider is then obliged to adapt the identity data.

2.3.2.4 Exemption from the obligation to identify

Exemptions from the obligation to identify persons may be issued by the Minister of Justice in terms of article 17, paragraph 9 of the National Ordinance Combating Money Laundering and the Financing Terrorism.

2.3.3 Representation

The service provider is obliged to inquire whether the natural person is acting on his own behalf or is acting as a n) (duly authorized) agent on behalf of a third party. In terms of article 7, paragraph 1, under e and article 8 of the National Ordinance Combating Money Laundering and the Financing Terrorism, the service provider must take reasonable steps to confirm the identity of the third party. If the natural person is acting on behalf of a third party, the service provider is obliged to establish the identity of both the natural person and the identity of the third party, using documents[11] submitted by the natural person.
In case of a chain of representatives, the service provider is obliged to identify the ultimate represented party.

2.3.4 CDD measures undertaken by intermediaries or third parties

Under the National Ordinance Combating Money Laundering and the Financing Terrorism, identification, verification and other CDD measures have to be primarily performed by the person providing the service.
The FIU shall, however, allow the service provider to rely on CDD measures of others, as set out in FATF Recommendations 10 and 17, if they are undertaken by an intermediary or third party, on the following conditions:

- The service provider relying upon a third party should immediately obtain the necessary information concerning elements a – c of the standard CDD measures set out in par. 2.3.1.

- The service provider should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available by the third party upon request without delay.

- The service provider should satisfy itself that the third party is regulated, supervised or monitored for and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

- When determining in which countries the third party can be established, countries should take into account all information available on the level of country risk.

In order to perform the above mentioned criteria, the service provider should take note of the mutual evaluations and other reports, assessments and reviews produced by the FATF, IMF (International Monetary Fund) or FSRBs (FATF Style Regional Body) and the public statements issued by the FATF.

[11] The documents specified in Article 3, NATIONAL ORDINANCE COMBATTING MONEY LAUNDERING AND FINANCING TERRORISM.

If there are any doubts in relation to the performed CDD, as undertaken by the intermediary or third party, the service provider must perform and complete the standard CDD, pursuant to FATF recommendation 10, a-c.

Where such reliance is permitted, the ultimate responsibility for compliance with appropriate risk oriented CDD measures remains with the service provider relying on the third party.

2.3.5 On-going due diligence on the business relationship

According to article 7, paragraph 1, under d of the National Ordinance Combating Money Laundering and the Financing of Terrorism. Risk based CDD implies furthermore that the service provider continually monitors the business relationship with the customer. This monitoring is a continuous process and is undertaken to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and the customer's risk profile, including where necessary the source of funds. This continuous monitoring of the business relationship means that the service provider should ask itself, for every service requested by the customer, whether that service fits the customer's profile. The service provider should also assess any changes in the customer's capacity or circumstances or assets against the risk of money laundering or terrorism financing.

File records of the above-mentioned on-going due diligence should also be retained. The filing has to be done in a way that makes it transparent why there were changes regarding the risks of money laundering or the financing of terrorism in the relationship with the customer.

2.4 Simplified CDD

The primary rule is that all customers must be subject to a standard CDD procedure. There are, however, circumstances in which the risk of money laundering or the financing of terrorism is lower, the information concerning the identity of the customer and UBO is in the public domain or else adequate controls are being exercised elsewhere in the national system. In these circumstances, the service provider is permitted to execute a simplified CDD in case the customer(s) is/are:

- Exempted businesses or service providers specified in section 2.3.2.4 of these P&G;
- Service providers that are subject to requirements to combat money laundering and terrorism financing consistent with the FATF recommendations and have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the recommendations to ensure compliance with those requirements. This does not imply that the service provider, upon determining the risk of the business relationship should not take other risk factors into account. Compliance with FATF recommendations is mostly based on mutual evaluations

which have been conducted some time ago.

When performing a simplified CDD, the service provider should collate and record information to confirm that the customer is in one of the categories mentioned above. The service provider is recommended to record, at the time of accepting the customer, the basis for his decision to opt for a simplified CDD.

A simplified CDD procedure is not permitted if there are suspicions of money laundering or financing of terrorism, or where specific larger risks are involved.[12]

The service provider should keep in mind that having a lower risk with regard to CDD does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for on-going monitoring of transactions.

If the customer is residing in another country, the service provider is only permitted to use the simplified CDD approach if the foreign country is in compliance with and has effectively implemented the FATF Recommendations. However, it should be clear that non-face-to-face business relationships can be indicative of a higher risk. This means that even though the customer initially is categorized as being of lower risk, a simplified CDD nevertheless cannot be executed because there is a non-face-to-face business relationship.

Please note that the simplified CDD should be in conformity with the lower risk factors (e.g. the simplified CDD should relate only to customer acceptance measures or to aspects of on-going monitoring).

An example of a standard and a simplified CDD form can be found in template 4.

2.4.1. Possible content of a simplified CDD

Pursuant to the above-mentioned primary rule of Article 7 in the National Ordinance Combating Money Laundering and the Financing of Terrorism, customers must be subjected to a standard CDD procedure. Under certain circumstances in which the risk of money laundering or the financing of terrorism is lower, a simplified CDD can be executed. These circumstances have to do, among other things, with the information concerning the identity of the customer and UBO being in the public domain or else adequate controls (e.g. supervision by authorized entities) being exercised elsewhere in the national system.

Based on the components of the Standard CDD a possible deviation from these components with the view to a simplified CDD can be allowed:

a. Identifying the customer and verifying that customer's identity using valid and reliable, independently sourced documents, data or information.

   A valid and reliable, independently sourced documents include the

[12] Explanatory note to Recommendation 10 FATF.

following:-

1) passport
2) identification card
3) driver's license

With regard to this component only the following deviations are allowed:
At the moment only the following entities are legally exempted from the identification and verification obligation:

- The exempt businesses or service providers specified in section 2.3.2.4. of these P&G;

b. Identifying the UBO and taking reasonable measures to verify the identity of the UBO, in such a way that the service provider knows who the actual UBO is. In case the customer is a legal person, a partnership or any other legal entity, the CDD should include the service provider's understanding of the ownership and the control structure of the customer.

With regard to this component no deviation is allowed. The UBO should always be known, unless it regards stock-listed companies as indicated in Article 6 paragraph 1 under a sub 3°.

The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

As already mentioned above, a simplified CDD procedure is not permitted if there are suspicions of money laundering or financing of terrorism, or where specific larger risks are involved.[13]

2.5 Enhanced CDD

Pursuant of Article 10 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, if there is an increased risk of money laundering and/or terrorism financing, the service provider is obliged to perform an enhanced CDD. The service provider should assess independently which cases involve an increased risk of money laundering and/or terrorism financing, on the basis of its own individual experience and

[13] Explanatory note to Recommendation 10 FATF.

reasonable opinion.

In the following cases, however, an enhanced CDD should always be performed:

A. PEP;

Article 10 paragraph 2 under i states that Politically Exposed Persons (PEP)[14], whether local or international, including international PEP residents in Sint Maarten must be subjected to enhanced CDD. A PEP is defined by FATF as an individual who is or has been entrusted with a prominent public function.
The PEP are divided into the following ranks:

- Foreign PEP: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

- Domestic PEP: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

- International organisation PEP: persons who are or have been entrusted with a prominent function by an international organisation, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

- Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. The following are in all cases classified as immediate family members: the spouse, partner who is equivalent to a spouse in terms of national law, children and their spouses or partners, brothers/sisters and parents.

- Close associates are individuals who are closely connected to a PEP, either socially or professionally.

As per article 11 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the service provider should be required to take reasonable risk management measures to determine whether a customer or ultimate beneficial owner is a domestic or a foreign PEP or a person who is or has been entrusted with a prominent function by an international organisation.

There are various ways to determine whether someone is a PEP, such as consulting public sources (Google, (digital) newspaper etc.) and subscription sources (e.g.

[14] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

www.transparancy.org, www.world-check.com and www.info4C.net). In many cases, however, the information may be found from whatever details are provided by the customer in response to questions that are generally asked before the business relationship is established.

If a PEP is a foreign person, the service provider must always ask itself whether the person should be buying the products from the organisation in question. In some cases the customer gains PEP status during the course of a business relationship. In these cases the customer's risk profile changes. The service provider must then subject a customer to an enhanced CDD.

B. as per Article 10, paragraph 2 under h and Article 12, paragraph 1, under a of the National Ordinance Combating Money Laundering and the Financing of Terrorism and countries as specified in section 2.5.1.1 of this P&G states that in this case, the service provider should always perform an enhanced CDD;

C. the provision of services to customers that are not physically present (non-face-to-face). With regard to the provision of services to customers who are not physically present there is a potentiality of a high risk when these customers are unable to be identified. This might, for instance, involve the use of the internet, where services can be offered but there is no physical customer contact.

However, the high risk regarding non-face-to-face business relationship can be mitigated when dealing with service providers that are subject to requirements to combat money laundering and terrorism financing consistent with the FATF recommendations. This is the case if these service providers have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the recommendations to ensure compliance with those requirements.

In the following paragraphs we will elaborate on the risk factors which can lead to an enhanced CDD. For an example of an enhanced CDD form, please be referred to template 5.

2.5.1 Higher risk factors

Article 12 of the National Ordinance Combating Money Laundering and the Financing of Terrorism states that the risks of money laundering can be assessed by using various risk indicators. The most commonly used risk indicators are: national or geographical indicators, customer indicators, product indicators and service indicators.

2.5.1.1 National/geographical indicators

Article 12, paragraph 1, under a states that the service provider shall pay specific attention to the national/geographical risk analysis gives the service provider useful information about potential money laundering risks. A country or geographical territory is in a higher

risk category in the following cases (non-exhaustive list):

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems. Identifying the "higher risk jurisdictions" is undertaken within the FATF by the International Cooperation and Review Group (ICRG) and is publicised by means of a list called the "Public Statement"[15] and a document called "Improving Global AML/CFT Compliance: On-going process".[16] Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations. The following sources can be consulted: www.fatf-gafi.org
- Countries identified by credible sources as having significant levels of corruption or other criminal activity (people trafficking, drug trade, prostitution, etc). The following sources can be consulted: www.fatf-gafi.org or www.transparency.org or www.icgg.org.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

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 policy of the United States and national security. The IMF, the World Bank and the Organisation for Economic Cooperation and Development (OECD) can also be classified as being reliable sources.

2.5.1.2 Customer indicators

Article 10, paragraph 2 states that customer indicators give the service provider information about potential money laundering risks. A customer falls in a higher risk category in the following cases (non- exhaustive list):

- customers and UBOs who are classified as PEP.[17] Please be referred to the explanation in paragraph 2.5.
- customers who are not physically present and who are also unable to be identified by a third party. Please be referred to the explanation in paragraph 2.5.
- where there is a substantial and inexplicable geographical distance between the service provider and the place where the customer is located, with no explicable reason;
- customers where the structure or nature of the entity or relationship makes it difficult to identify the UBO;
- customers who do not provide an address or provide different addresses with no explicable reason;
- customers of businesses dealing with large amounts of cash, where the nature of the services requested exposes the service provider to the risk of facilitating illegal

[15] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-feb-2014.html
[16] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-feb-2014.html
[17] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

transactions. These businesses include casinos and other businesses whose activities are related to games of chance; where the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- non-resident customers.
- companies that have nominee shareholders or shares in bearer form
- businesses that are cash-intensive.
- where the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

2.5.1.3 Product and service indicators

The service provider can also assess the risks of money laundering or the financing of terrorism by determining which of the services/products that he offers can be used by the customer for money laundering purposes. Some examples (i.e. not an exhaustive list):

- services were the service provider acts as an intermediary, arranging for the receipt and transfer of money through (the use of) third-party trust accounts that he manages. An example of this is a lawyer who arranges for an international bank transfer of funds for his customer[18];
- services that the customer asks for and that do not coincide with the customer's normal business activities;
- customers who offer payment for services that are excessively high in relation to the services that have been provided;
- services that are requested with a view to concealing the identity of the UBO from the authorities;
- the preparation of private loan agreements or debt acknowledgements, where the origins of finance are unclear;
- providing advice about back-to-back loans and loan back structures;
- Private banking;
- Non-face-to-face business relationships or transactions;
- Payment received from unknown or un-associated third parties.

2.5.1.4 Detection and deterrence of terrorist financing

The service provider must always take necessary measures to prevent the use of entities identified as vulnerable, such as charitable or non-profit organizations as conduits for criminal proceeds or terrorism financing.

The service provider must take into account the characteristics including types of

[18] Bank transfers are often used by criminals to move funds without hindrance. This is why recommendation 16 was adopted by the FATF. The purpose of Recommendation 16 is to have immediate access to basic information about those who instruct such money transfers. Where the service provider is asked to arrange a bank transfer in favour of his customer, he is obliged to record information relating to the sender. The information must consist of the name, address and account number.

transactions listed in the annex 1 to the FATF document entitled "Guidance for Financial Institutions in Detecting Terrorist Financing".[19] Those characteristics and transactions could be cause for additional scrutiny and could indicate funds involved in terrorist financing. In addition, service providers must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in:

- the list issued by the United Nations[20];
- the list issued by the European Union[21];
- Sanction Decree, (AB 2015, no 15);
- annex 2[22] to the FATF document" Guidance for Financial Institutions in Detecting Terrorist Financing"; and
- the listing[23] of the Office of Foreign Assets Control (OFAC) or of other national authorities.

2.5.1.5 Sanction lists

The United Nations and the European Union issue sanction lists with names of persons, entities or countries that are sanctioned. These sanctions are issued to combat terrorism worldwide and thus to restore international peace and safety.

The service provider must continuously compare the names in their customer database with the names on the above-mentioned lists. If the service provider suspects or has reasonable grounds to suspect that funds are linked or related to, or are (to be) used for terrorism, terrorist acts, or by terrorist organizations, it must report promptly its suspicion to the FIU. Reference is made to the reporting procedure in Chapter 3 of this P&G.

Moreover, the service provider must be vigilant in the use of nonprofit organizations for terrorist financing.

2.5.2. Enhanced CDD measures

In addition to the standard CDD specified in section 2.3.1, Article 10, paragraph 4 indicates that the enhanced CDD measures are to include performing the following activities:

1. a more thorough verification of identity data, including an assessment of whether the documents that are provided are genuine;
2. asking further critical questions in relation to the customer's background, business and

[19] The full document can be consulted at http://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf
[20] http://www.un.org/sc/committees/1267/pdf/AQList.pdf
[21] http://eur-lex.europa.eu
[22] http://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf
[23] http://www.treasury.gov/ofac/downloads/t11sdn.pdf

sector and updating more regularly the identification data of customer and beneficial owner;
3. exercising continuing extra supervision over the business relationship and its intended nature;
4. a more thorough investigation of the monetary traffic or cash flows concerned;
5. reserving the decision to enter into the business relationship transaction to senior management. 'Senior management' means members of the management team designated as such and given specific authority to enter into this type of business relationship, as well as persons appointed and authorised by the service provider to enter into such relationships;
6. take reasonable measures to establish the source of wealth and source of funds.

2.5.2.1 Enhanced CDD measures in relation to PEP

Article 11 of the NOCMLTF states, the service provider is required, in relation to foreign PEP (whether as customer or beneficial owner), in addition to performing standard CDD measures:

a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;
b. obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
c. take reasonable measures to establish the source of wealth and source of funds;
d. and conduct enhanced on-going monitoring of the business relationship.

3. THE REPORTING DUTY

3.1 Unusual transactions

First and foremost, it is of importance to point out the meaning of the word transaction. Under the National Ordinance Combating Money Laundering and the Financing of Terrorism, a monetary transaction is defined in art. 1, paragraph 1, under n as:

1º. 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, cheques, traveller's cheques, bank drafts or money orders; and

2º. 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 National Ordinance Combating Money Laundering and the Financing of Terrorism indicates that anyone who renders a service as a profession or as a trade, as referred to in article 2, first paragraph, under b sub 1° to 8°, in or from Sint Maarten, is obliged to report any unusual transaction, either executed or intended, to the FIU 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 service provider but also to intended unusual transactions. Intended unusual transactions include e.g. transactions that for whatever reason have not been executed by the service provider.

For example, the service provider may have a policy not to accept any cash payments. If the customer then decides to take his business elsewhere the service provider should report this as an intended unusual transaction.

3.2 Indicators

There are three indicators established for the service provider according to the Ministerial Decree, AB 2013, CT no. 489. These can be divided into two objective and two subjective indicators.

3.2.1 **Objective indicators**

Objective indicators explicitly indicate when a transaction should be reported as unusual. The service provider is obligated to report objectively. This will be a violation of the law. If an objective indicator applies to the transaction, reporting is mandatory.

The seven 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 using the code: **160101**

- Sanctions Regulation: **160102**

- A wire transfer that is greater than or equal to Naf 500.000 : **160103**

- A cash or cheque transaction of NA*f*. 25.000,- or above or the equivalent thereof in another currency, must be reported to the FIU using the code: **160104**

- All transactions (cash and wire transfers ≥ NAf 5.000 for casino / lottery / online gaming: **160105**

- Sending cash ≥ NAf 5.000 through money remitter office: **160106**

- Deposit cash ≥ NAf 5.000 on credit card or prepaid card: **160107**

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

3.2.2 **Subjective indicators**

There are two subjective indicators for service providers.

The subjective indicator implies that an unusual transaction must be reported if it gives rise by the service provider, based e.g. on his knowledge of the customer, the customer's business or the transaction involved, to a suspicion that the transaction may be associated with money laundering or the financing of terrorism.

Annex 1 to these 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 service provider will need to assess whether the transaction should be reported as suspicious. Article 33, paragraph 1 and 2 of the National Ordinance Combating Money Laundering and the Financing of Terrorism states that the violation of the reporting obligation, in so far committed intentionally, is considered a criminal offence.

The two subjective indicators are:

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

3.3 Reporting

Anyone who renders a service as a profession or as a trade is obliged to report an unusual transaction without delay to the FIU (Article 25 of the National Ordinance Combating Money Laundering and the Financing of Terrorism). Reporting can be done by sending a digitally completed reporting form or by delivering a manually completed reporting form in person to the FIU.

Most of the 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. 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 (internal reporting, chapter 3.3.3.), so that he/she can forward the unusual transaction reports to the FIU.

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

3.3.1 Time limit for reporting

Pursuant to article 25, paragraph 1 of the National Ordinance Combating Money Laundering and the Financing of Terrorism an (intended) unusual transaction must be reported immediately. The FIU interprets the term "immediately" as follows:

For reports based on an objective indicator
The service provider must send its unusual transaction report within 48 hours after the transaction has been executed, or after the intention to execute an unusual transactions has taken place.
A request for extension must be directed in writing to the director of the FIU, stating the reasons for the request for extension. The FIU 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 (CO) to the FIU should **not exceed 48 hours**.

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

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 to the FIU, stating the reasons for this request.

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

3.3.2 Information to be reported

Article 25, paragraph 2 of the National Ordinance Combating Money Laundering and the Financing of Terrorism states that, a report shall contain the following information:

a. in respect of natural persons:
   1º. the client's identity as established on the basis of article 3, paragraph 3;
   2º. the type, number, date and place of issue of the client's proof of identification;
   3º. the nature, time and place of the transaction;
   4º. the scope, destination and origin of the funds, securities, precious metals or other assets involved in the transaction;
   5º. the circumstances on the basis of which the transaction is designated unusual; and
   6º. 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;
   7º. 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
   9º. 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 and Industry, its registration number at the Chamber of Commerce and 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, 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, 3° to 6°;

3.3.3 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 3.2.1 and 3.2.2. 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. 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 and NA*f* 25.000 or above or the equivalent in another currency.

3.3.4 Indemnity for the service provider and its employees on making a report

The service provider that has submitted a report pursuant to article 25 of the National Ordinance Combating Money Laundering and the Financing of Terrorism is not liable, according to article 29 and 30 (Indemnity), for any damage or loss sustained by a customer or third party as a result of that report, unless such damage or loss is the consequence of an intentional act or conscious recklessness of the person who has reported. The same rule applies to an employee of the reporting service provider. This includes directors, officers, managers or other employees in general.

With regard to the criminal liability of the service provider and its employees, including the directors, officers, managers or other employees in general, it is stipulated in article 14 that data or information that, in accordance with articles 30 of the National Ordinance Combating Money Laundering and the Financing of Terrorism.

3.3.5 Confidentiality of the report

All data and information that have been supplied or received pursuant to the provision by or in accordance with Article 27 of the National Ordinance Combating Money Laundering and the Financial of Terrorism are confidential. The service provider and its directors, senior management, and employees are not allowed to divulge any information, with regard to the FIU and its legal tasks, to customers and/or third parties (tipping off prohibition).

4 RECORD KEEPING

Chapter IV of the National Ordinance Combating Money Laundering and the Financing of Terrorism contains Article 22 and Article 23, which relates to the storage of data and information acquired by 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 service provider shall keep the data relating to the unusual transaction as well as the data gathered within the scope of the customer investigation (customer due diligence) for a period of at least ten 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 or cheque transaction of NA*f.* 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 service provider must sign and date on the copy of the client'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 concerning the reported unusual transaction (if an unusual transaction report has been filed with the FIU)
- Internal reports that did not lead to unusual transaction reports to the FIU
- Bill of sales of the vehicle

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 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

Article 17, paragraph 1 and Article 25, paragraph 2 under a, sub 1° & 2° 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 service provider is obliged to maintain the following records of a natural person.

For a customer, UBO, the vendor, and the representative

Article 17, 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 service provider is 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 service provider 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 article 17, paragraph 2 & 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the identity of a legal person or corporation may be established using a certified excerpt from the register of the Chamber of Commerce and 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 service provider with such a document, the service provider can let the representative fill out the details of the legal person or corporation on a form. Please be referred to template 6 in this regard.

The service provider 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.

As per Article 25, paragraph 2 under b, a legal entity (company) can be identified by providing the following:

- legal form;
- official name according to the Articles of Incorporation (or Articles of Association);
- trade name (Doing Business As - DBA) if applicable;
- address;
- place of establishment;
- country of registered office;
- registration number with a Chamber of Commerce or similar institution, as well as the place where that Chamber of Commerce or similar institution is registered.
- what type of product/service the transaction is about.

The service provider is 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 service provider 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.

4.3. Record keeping of unusual transactions

The service provider must keep the data relating to the unusual transactions in files. The data must be recorded in such a way as to enable the supervisor 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 service provider is required to keep documentation regarding its findings on complex, unusual large transactions, or unusual patterns of transactions, available for competent authorities and supervisors for a period of ten years.

If an unusual transaction highlighted by an employee at the service provider is <u>not</u> reported to the FIU, there should be a record of the reasons why the report was not submitted to the FIU 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 and/or the management.

The National Ordinance Combating Money Laundering and the Financing Terrorism does not require the termination of services to the customer as a result of filing an unusual transaction report with the FIU. However, it is in the best interest of the service provider, with a view to possible intentional, culpable or habitual money laundering situations[24], to consider the facts and circumstances when deciding whether or not the relationship with the customer can be continued.

[24] articles 2:404 (intentional money laundering), 2:405 (habitual money laundering) and 2:406 (money laundering through default).

4.4 Period for maintaining records

Pursuant to article 22 and 23 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the service provider must record data in such a manner that they are accessible. Pursuant to abovementioned articles, the data, referred to in article 6, has to be saved until:

- ten years after terminating the agreement on the basis of which the service was rendered; or
- ten years after executing a service, as referred to in art 2, par. 1b, under 2°.

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 supervisory 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 service provider. The information must be filed in such a way that the supervisory agency can examine the basis upon which the service was provided.

5 COMPLIANCE REGIME

The FIU may (at any time) initiate an audit at the service provider in order to supervise if the legal obligations are met. The FIU will inform the service provider about the information that the service provider will need to have at hand for the audit. During the audit the FIU will check whether the service provider has complied with the provisions of the National Ordinance Combating Money Laundering and the Financing of Terrorism and the P&G. According to Article 20, paragraph 2 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the service provider should therefore set up a compliance regime.

A well designed, applied and monitored regime will provide a solid foundation for compliance with the legislation. Not all individuals and entities operate under the same circumstances; hence, the compliance regime will have to be tailored to fit the service provider's 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 article 20, paragraph 2 and 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, a service provider shall conduct an adequate policy as well as a compile written procedures and measures which focus on preventing and combating money laundering and the financing of terrorism. The compliance policy and internal procedures must be kept up-to-date.

The compliance regime of the service provider must include the following elements:

1. a written compliance policy internal procedures and controls – art. 20 para 1 & 4;
2. the appointment of a compliance officer – art. 21, para 2 & 3;
3. setting up an on-going employee training programme – art. 21, para 1;
4. an independent evaluation to assure the quality of the compliance regime – art 20, para 5 & 6.

5.1 Compliance policy and internal procedures

Change of various factors may bring along that the service provider's 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 and/or products by the service provider. 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.

Pursuant to Article 20, paragraph 4 & 5 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the policies and procedures have to be

approved by the senior management of the service provider. Senior management refers to individuals at the highest level of organizational management within the service provider who have the day-to-day responsibilities of managing the business.

Article 21 states that it is important for the staff to be properly informed about the contents of the service provider's compliance policy and internal procedures, particularly those members of staff working in the areas of customer identification, recording data and reporting unusual transactions.

In the compliance policy, internal procedures regarding risk based CDD and reporting of unusual transactions need to be established. Annex 3 provides some guidelines for an internal compliance policy and risk assessment that some service providers may find useful. The FIU has also drafted a template that can be used to set up a compliance policy. Please request the FIU to send you the latest version. A compliance policy should cover at least the following aspects:

- a commitment of the service provider to abide by the AML/CFT legislation
- 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

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

Pursuant to article 19, paragraph 1 of the of the National Ordinance Combating Money Laundering and the Financing of Terrorism, a service provider 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 (i.e. FATF Recommendations) for the prevention and combating of money laundering and the financing of terrorism. The service provider is required to pay particular attention that this principle is observed with respect to its branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations.

The service provider is required to inform the FIU 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 and/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.

5.2 The appointment of a compliance officer

Pursuant to article 21, paragraph 2 and 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, the compliance officer plays an important role with regard to compliance with legislation, the P&G, and compliance policies or procedures that are operational within the service provider.

The service provider can appoint a compliance officer on a full time or a part time basis based on its financial resources. 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 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 service provider must inform the FIU that the company falls in this category and would like for senior management to fulfil the duties of the compliance officer. The FIU will then approve of this request.

It is also possible that a small 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.

5.2.1. Duties of the compliance officer

Pursuant to article 21, paragraph 2 and 3 of the National Ordinance Combating Money Laundering and Financing Terrorism, the (principal) duty of a compliance officer is to ensure that the service provider correctly complies with the existing legislation and regulations. The compliance officer may achieve this by giving training, advice and direction to employees and/or management on how to comply with internal procedures regarding risk assessment, CDD and reporting unusual transactions. It is also important for the CO 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 service provider reports the unusual transactions to the FIU and assesses them on their completeness and correctness. He or she bears the responsibility for record keeping of all reported unusual transactions. The compliance officer is preferably the contact person within the service provider for all communication with the FIU.

The compliance officer will furthermore play an important part within the business during

the screening of new employees. The service provider 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 organisation without the management exerting undue influence with regard to the filing of reports to the FIU. 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 compliance policy. If the FIU undertakes an audit or investigation at the service provider, it will ask you 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 service provider. It should however be pointed out that, in case of a violation of the legislation and/or the P&G, a (administrative or criminal) sanction can be imposed on the service provider. Chapter 6 provides more information about supervision and enforcement.

5.2.2. Transfer of tasks

The compliance officer has various duties as mentioned in paragraph 5.2.1. 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 service provider needs to communicate this to the FIU. 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.

5.3 Setting up an on-going training programme

Pursuant to article 21, paragraph 1 of the National Ordinance Combating Money Laundering and Financing of Terrorism, a service provider is responsible for ensuring that, to the extent relevant for the performance of their duties, its 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 framework of Sint Maarten and an indication of expected developments ;
- the sanctions that can be imposed if a service provider violates the AML/CFT legislation including the P&G;
- 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, news papers and Google search.
- contact the FIU, 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, seminars and using communication resources (e.g. email, newsletters and/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 service provider. This is in order to determine the most relevant topics for the training programme. Key personnel include:

- those members of staff working in the field of Customer Due Diligence, recording of the information and the reporting of unusual transactions;
- the compliance officer;
- management

The service provider should maintain a list of the (key-) personnel that participated in the training programs and/or specific courses dealing with combating money laundering and terrorism financing. Please be referred to template 8 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.

5.4 An independent evaluation to assure the quality of the compliance regime

Service providers must carry out regular assessments of the adequacy of their systems and controls to ensure that they manage the money laundering and terrorism financing risks effectively and are compliant with the National Ordinance Combating Money Laundering and the Financing of Terrorism and the P&G. Service providers must therefore ensure that appropriate monitoring processes and procedures are established and maintained to regularly review and test the effectiveness of their policies and procedures. Pursuant to article 20, paragraph 4 & 5 of the National Ordinance Combating Money Laundering and the Financing of Terrorism and to FATF recommendation 18, the service provider should ensure that an independent evaluation of the compliance regime is executed.

Such an evaluation should take place at least every 2 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 service provider 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 programme, (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. The results of an evaluation should be recorded in writing and submitted to the service provider's 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 service provider. In any case, the service provider can take on an AML/CFT professional firm of person to perform an independent evaluation of the compliance regime. Pursuant to article 20, paragraph 6 of the National Ordinance Combating Money Laundering and Financing Terrorism, these findings of the periodic evaluations, shall be recorded in writing and a copy sent to the Office for Disclosure.

6 SUPERVISION AND ENFORCEMENT

6.1. General

Pursuant to article 31, paragraph 1 of the National Ordinance Combating Money Laundering and the Financing of Terrorism and together with the P&G form a basis for supervision and enforcement by the FIU.

As mentioned before, the FIU is the supervisory agency for the DNFBP's. This means that the FIU has to ensure compliance of the DNFBP's with the National Ordinance Combating Money Laundering and the Financing of Terrorism and the P&G. When a service provider is not compliant with the legislation and the P&G, the FIU has the power to take enforcement measures. In the next paragraph both aspects of the supervisory task, supervision and enforcement as per Article 31, paragraph 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, will be explained.

6.2. Supervision

In order to supervise the DNFBP's, the FIU, pursuant to article 11, paragraph 3 and 4 of the National Ordinance Financial Intelligence Unit, article 31 of the Administrative Enforcement National Ordinance, article 5 and 31, paragraph 2 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, has the following authorities:

Issuance of P&G;

1) The FIU has the legal authority to issue binding P&G in order to encourage and enforce compliance by the service providers with the National Ordinances. Request all information necessary for the execution of its task;
2) Supervisory officials, appointed by the FIU, are, for example, authorized to request the service provider to hand over or provide any further data or information and are entitled to examine customer files and documents of service providers, as well as taking copies of these files and documents.
3) Request inspection of all the books, documents and other information carriers, such as electronic files, and to take copies of such or to take them along temporarily The FIU has the right to demand examination of all files.
4) Subject goods to inspection and investigation, to take them along temporarily and to take samples of them;
5) Enter all locations, with the exception of private residences without the explicit permission of the occupant, accompanied by persons designated by them;
6) Investigate vessels, stationary vehicles and the cargoes thereof;
7) Enter private residences or parts of vessels destined as a private residence, without the explicit permission of the occupant.

Every person is legally obliged to give the appointed officials of the FIU all the cooperation demanded pursuant to the National Ordinance.

6.3. Enforcement

Violation of the legislation, including the P&G is sanctionable. When the FIU decides to impose a sanction it will issue a written administrative decision directed to the service provider. The administrative decision will contain a motivation of the reasons why a sanction was imposed on the service provider.

Pursuant to article 2 paragraph 3 of the National Ordinance Administrative Enforcement such an administrative decision is subject to objection and/or appeal. This means that an interested party has the right to file an objection and/or appeal in Court of First Instance. After the Court of First instance has given a verdict, the law furthermore gives the possibility to appeal in the Common Court of Justice.
Article 4 and article 10 of the National Ordinance Administrative Enforcement (AB 2018, no. 22) and article 19 of the National Ordinance FIU, contains a range of instruments for the enforcement of compliant behaviour by the service providers.

Pursuant to article 31, paragraph 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism, sanctions can be imposed both under administrative and Criminal Code. The choice for imposing administrative sanctions (fine or penalty) depends amongst others on the nature, gravity and scale of the infringement and will only be made if the infringement is of such a nature that criminal sanctions would be inappropriate. If the choice is made to impose an administrative fine, the path to the criminal court is ruled out, and vice versa.

6.3.1. Administrative Sanctions

As mentioned before, the FIU has the power to impose an administrative sanction on the service provider if it violates its obligations under the laws. The administrative sanctions that can be imposed are:

1) **Administrative penalty (article 31, paragraph 3 of the National Ordinance Combating Money Laundering and the Financing of Terrorism and article 50 of the Administrative Enforcement National Ordinance)**
   The FIU can impose a fine if the service provider does not comply or does not comply in due time with its legal obligations. The maximum amount of the fine is NA*f*. 4,000,000. The FIU will indicate in its administrative decision the specific circumstances that led to the fine.

2) **Incremental penalty (article 22, paragraph 2 of the Administrative Enforcement National Ordinance)**

   The FIU will indicate in its administrative decision the specific circumstances that led to the penalty payment.

3) **Enforcement action (article 34, paragraph 3 of the Administrative enforcement National Ordinance)**

6.3.2. Publication of the administrative sanction (article 12, paragraph 7 of the Administrative Enforcement National Ordinance)

The FIU has the authority to make the infringement on which a penalty or fine is imposed, publicly known. If the FIU decides to publish the sanction, the name, address and place of residence of the (legal) person on which a fine or penalty is imposed will be mentioned.
Publication of a complete or partial report in which a violation has been established is based on both the prevention perspective and the legitimation perspective. Active disclosure of inspection data serves the following intended purposes:

- promoting compliance with regulations;
- informing the public for a warning;
- to provide the public with insight into the way in which supervision is carried out (on behalf of the community).

6.3.3. Sanctions based on the Criminal code

1. Each action in breach of the provisions under or pursuant to articles 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 National Ordinance Combating Money Laundering and Terrorism Financing shall, to the extent it was intentional, be punished by either a prison sentence of a maximum of four years or a financial penalty of the sixth category.
2. Each action in breach of the provisions under or pursuant to articles 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 National Ordinance Combating Money Laundering and Terrorism Financing shall, to the extent it was unintentional, be punished by either imprisonment for a maximum of one year or a financial penalty of the sixth category.
3. If an action in breach of the provisions of article 27 of the National Ordinance Combating Money Laundering and Terrorism Financing 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 misdemeanours.
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.

Template 1: Organizational change Form (for FIU)

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*	☐Jewelers ☐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.*	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	
Email address *This should be a working email 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	
Email 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 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	
Email 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 / Person responsible for reporting **Signature Director**

Company stamp

PLEASE NOTE:

- **MAKE SURE THE FORM IS SIGNED BY THE COMPLIANCE OFFICER/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 EMAIL ADDRESS:** Supervision.department@fiu.gov.sx , rosebiani.boston@fiu.gov.sx.
- **THIS FORM CAN ALSO BE HAND DELIVERED TO THE FIU 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.

Template 2: Risk Assessment form

Risk assessment – KYC - 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 Customer Due Diligence (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 Customer Due Diligence (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 laws and regulations 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 clients).
- 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 Customer Due Diligence.

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 Companies responsibility (RBA) to execute a balanced risk assessment;
- In the annexes the FIU 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 clients 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, clients, products, experience etc. Please select the risk assessment questions in the Annex 1 that apply to your company's client/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 client.

Client 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 client: *The name of the client*	
Changes made (if applicable): *If it is an existing client 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.**	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			

CLIENT RISK FACTORS	YES	NO	PTS
A. Client behavior			
1. Is the customer mysterious or evasive about the motive of the transaction?	10 -25 (example)	0	
2. Is the behavior of the client peculiar in any way (e.g. nervous)?	10 (example)	0	
Please continue filling out the risk assessment questions applicable specific to your business.			
B. Client identification			
3. Does the customer have an irregular address?	10 (example)	0	
4. Does client 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 CLIENT 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. Client type (characteristics)			
6. Is it a non-face-to-face client?	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			

PRODUCT FACTORS	YES	NO	PTS
1. Does the client purchase the real estate property	5-20 (example)		

with the intention to start a commercial cash intensive business?			
2. Is or was the real estate property involved related to a criminal law procedure?	5 (example)		
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 client 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.

Template 3: Examples Risk Profile

HIGH
Country - Nationality of the client *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 client in your client base**
Client - Type of client - Behavior *Example:* - *Client is a nervous natural person;* **Please note: These are (two examples of) the typical characteristics of a type of high risk client in your client base**
Product - Type of real estate *Example:* - *High priced real estate property* **Please note: These are (two examples of) the typical characteristics of a type of product(s) typical of a high risk client in your client base**
Payment/transaction - 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 client in your client base**
Other **Please note: These are the other typical characteristics of a high risk client in your client 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: - *An US client* **Please note: These are (two examples) the typical characteristics of a type of normal risk client in your client base**
Client - Type of client *Example:* - *Retired US client* **Please note: These are the typical characteristics of a type of normal risk client in your client base**
Product - Type of real estate property *Example:* - *Condo/villa* **Please note: These are (two examples of) the typical characteristics of a type of product(s) typical of a normal risk client in your client 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 client in your client base**
Other **Please note: These are the other typical characteristics of a normal risk client in your client base**
Comments and remarks

Explain the reason(s) for choosing above risk profile.

PLEASE NOTE: 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 client in your client base**
Client - Type of client *Example:* - *Government owned company : GEBE* **Please note: These are the typical characteristics of a type of low risk client in your client base/company**
Product - Type of real estate property *Example:* - *Commercial property* **Please note: These are (two examples of) the typical characteristics of a type of product(s) typical of a low risk client in your client 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 client in your client base/company**
Other **Please note: These are the other typical characteristics of a low risk client in your client base/company**
Comments and remarks

Explain the reason(s) for choosing above risk profile.

PLEASE NOTE: Write down all the peculiarities

Signature compliance officer
Name:
Date:

Procedure for setting up a risk profile

Introduction:

- This procedure is to be used when setting up risk profiles for specific clients in the Company client 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 client, divided over the different risk categories (country, client, 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 client a low risk, a normal risk client a normal risk and a high risk client a high risk. The risk assessment needs to be analyzed as a whole.

1. Finish the risk assessment form for the clients in your client 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 client.
4. Under “client” you can fill out the characteristics that have to do with, for example, the type of client, its behavior or anything else that has to do with the client 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 client.
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.

Template 4: Standard + Simplified CDD form

A. FOR YOUR CLIENTS

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

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

CLIENT (companies)		
Legal name:		
DBA name:		
Please attach: A copy of the Chamber of Commerce 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:

Template 5: Enhanced CDD

A. FOR YOUR CLIENTS

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

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

CLIENT (companies)		
Legal name:		
DBA name:		
Please attach: A copy of the Chamber of Commerce 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:

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	

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:

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 client 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 $ ……., €……..)
- ☐ Subjective: Transaction deviates from the profile of the customer
- ☐ Subjective: Suspicious transaction
- ☐ Other :

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

Type of client

- ☐ Natural person
- ☐ Legal person

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

PLEASE NOTE: Enclose a copy of the identification papers of the client to this report.

Signature employee
Date:

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 or not)

☐ Unusual Transaction Report (UTR) to FIU

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

Date UTR (if applicable)		Time	

PLEASE NOTE: Enclose the confirmation letter if reported!

_____ _____
Signature compliance officer Signature senior management
Date: Date:

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 client paying with counterfeit bills, or false identification.
   - Sanctions Decree: 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 sanctions decree
   - 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.
   - Client profile: When a transaction deviates from the profile of the customer
   - Suspicious/fishy feeling: anytime you have a suspicious or fishy feeling that a client 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 client.
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 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 for confirmation letter.
9. Close the internal report and file it together with the confirmation letter.

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 (exp. on-site, of video etc.)*	*Numbers of hours*	*Date training completed and certificate received*

Template 9: Evaluation Log

Date evaluation	Topics of evaluation	Improvement points	Completed	Rating

Annex 1: Risk analysis related to the services provided by the professionals sector

1. **The FIU Sint Maarten makes a distinction between categories of risks. Categorisation takes place between:**
    I. Country risks
    II. Customer risks
    III. Product and service risks
    IV. 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 notary.

- *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/it identity?

- Is the customer mysterious or evasive about the identity of the ultimate beneficial owner (UBO)?
- Is the customer mysterious or evasive about the motive of the transaction?
- Does the customer try to avoid a personal meeting?
- Does the customer ask for unexpected speed?
- Does the customer change legal advisor/notary in a short period of time without legitimate reason?
- Is there a PEP that is engaged in unusual private business given the parties involved?
- Is the customer secretive about the purpose of the transaction?
- Does the customer use an agent or intermediary without any apparent reason?
- Is the customer not concerned about the level of fees to be paid?
- Does the customer frequently change legal structure?
- Is the customer a company that has nominee shareholders or shares in bearer form?

- *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 Gmail, Hotmail etcetera?
  - Is there an absence of documentation to verify the customers 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)?
  - Is the customer a non-face-to-face client?

- Does the customer act on behalf of an unidentified person that he/she represents?
- Is the customer a company with a complex ownership structure?
- Does the customer have a criminal record?
- Are the parties involved connected without apparent reason?
- Are the shareholders of the company under legal age?
- Are other parties involved in the transaction not formal parties to the transaction?
- Is the person a high net worth individuals?
- Is the customer a company with a business that is cash intensive?

c. Product and service risks

Definition: Risk factors related to the characteristics of the services of the notary.

- Does the customer request to use the services of a notary without that service having an actual legal content?
- Does the customer request to act for multiple parties without actually meeting them?
- Are there multiple appearances of the same parties in transactions over a short period of time?
- Are there A-B-C real estate transactions with rapidly increasing value of the real estate concerned?
- Is the customer located at a geographical distance from the notary and is there no legitimate or economic reason for using this legal professional over a notary that was located closer?
- Are there unexplained changes in instructions from the customer?
- Is there use of a complicated legal structure without legitimate reason?
- Does the service ask for the use of legal/corporate structures related to multiple countries without an apparent link to the customer, the transaction or for any other legitimate or economic reason?
- Are there U-turn transactions demanded in the service, e.g. transactions to the (escrow) account of the notary or other entity with the purpose to be sent back to the originating account in a short time frame?
- Is the service related to large financial transactions by recently established companies?
- Is there a power of attorney being sought for the disposal of assets under unusual conditions and without logical explanation?
- Is the service related to non-profit organizations that are engaging in activities other than its purpose or that are not typical for that organization?
- Is there lack of (legal) reasons for the tax/legal/notarial service requested?

- Is the service related to investment(s) in real estate without any links to the place, location or property?
- Are there purchases of properties for family members of the customer where there is a lack of personal contact that gives doubt to the nature of the transaction?
- Is there an unusual level of investment in a dormant company?

d. Transaction risks

Definition: Risk factors related to the establishment of the transaction, the chosen mode of payment and/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 or cheques?
  - 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 too early in the transaction or different than is custom?
- 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 or its shareholder's?
- Is the transaction financed by a loan (back) construction?
- Is finance is 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 laws and regulations
- 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 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 (CO)

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 CO, his/her contact details
- If there an assistant CO, 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)

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 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 service provider and

If relevant, attach relevant CDD forms or templates.

1.5. Unusual transaction reporting

The service provider is obliged to report unusual transactions if encountered during the course of business. The CO is the main responsible person for reporting unusual transactions to the FIU. It is advised, especially in companies with more than 2 employees, to have an internal reporting procedure in order to facilitate the CO'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 CO
- 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 providers business

If relevant, attach relevant internal reporting forms or procedures.

1.6. Record Keeping

Records need to be kept accessible and secure for 5 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 service provider, including the CO 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 two years the compliance regime of the service provider 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 evaluator
- Other practical agreements made with the 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 CO 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 CO
- Procedures and frequency of evaluation of the employees
- Communication methods and frequency of this between senior management and the CO
- Communication methods and frequency of this between the CO and the employees
- A summary of the appropriate monitoring arrangements in place to ensure that the firm's 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

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 two (2) 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 service provider
- Academic level: someone that has an academic degree in for example finance, law or economics
- Knowledgeable of or able to learn the AML/CFT legislation 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 service provider. It is not the intention for the evaluator to look into transactions, reported or not reported, or customer/client files. This is the task of the supervisors of the FIU. The compliance officer of the company is not allowed to show the evaluator the customer/client files as this is against the confidentiality clause as mentioned in article 20 of the NORUT.

Before starting an evaluation

It is very important to read the Provisions & Guidelines (P&G) of the respective sector that is going to be evaluated as they contain extended information on the obligations of the service providers. 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.

Attention! The information in this document is for guidance on how to perform an evaluation of a compliance regime. An evaluator can add more questions or evaluation methods if deemed appropriate.

B. Checkpoints

These are the points of a compliance regime that 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 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 clients/customers/products/services. The risk factors that need to be considered/weighed are:

A. Product/service risks
B. Customer/client 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 service provider carries out. These are:

- Politically Exposed Persons (PEPs)
- High risks countries
- Non-face-to-face clients/customers

For more information on the risk factors, high risks and risk assessment in general, please be referred to Chapter 2 of the 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 service provider should have a written AML/CFT compliance policy. In this policy, the 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 service provider to abide by the AML/CFT legislation
- 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 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 clients, 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 the P&G and the respective template of the compliance policy that the FIU 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 (CO)
The 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
- Giving training, advice and direction to employees and/or management on how to comply with AML/CFT obligations
- 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
- Screen new employees

The CO can be an internal person from within the company or it can be someone that is appointed externally. If the 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 CO should be at least at management level to understand and implement the requirement
- The CO should operate independently
- The CO should have unrestricted access to relevant information

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

For more information on the CO and his/her duties and responsibilities please be referred to chapter 5 of the P&G and the respective template of the compliance policy that the FIU distributed to the service providers.

What an evaluator needs to review:
- Is there a CO appointed at manager level
- Does the CO operate independently?
    - ✓ Does the CO need approval from senior management for anything? If so, for what?
    - ✓ Does the CO have access to information?
    - ✓ Does the CO make decisions independently? If so, for what?
- Does the CO have an overview on the AML/CFT regime of the service provider?
- Does the CO adhere to the internal reporting procedure?
- Does the CO adhere to the reporting procedure to the FIU?

- Does the CO have enough time to comply with obligations/tasks? How fast are tasks completed?
- Does the CO have sufficient AML/CFT knowledge?
    - ✓ Does he/she keep the knowledge up to date?
    - ✓ How frequent does he/she follow training?
- How does the CO communicate with staff/management?
- How does the CO react to changes in the AML/CFT legislation?
    - ✓ How does the CO incorporate/implement changes?
- What is the procedure for new employees?
    - ✓ Does the CO 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 CO
- Interview with senior management
- Interview with employees
- Observation of reporting procedure
- Check policy for tasks and responsibilities CO

Ad 4. Training program

The service providers must make sure its staff and management have up-to-date knowledge of AML/CFT. That is why the 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 CO
    - ✓ Management

Training should cover, at least, the following topics:

- general information about money laundering and terrorism financing;
- an explanation of the legal framework of Sint Maarten and an indication of expected developments;
- the sanctions that can be imposed if a service provider violates the AML/CFT legislation including the P&G;
- 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 the 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 knowledge of employees sufficient?
- Is the AML/CFT 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 service provider?

Suggestions of methods to review the above:

- Review training material
- Interview employees
- Interview management
- Interview CO
- Review training program procedures

Ad 5. Internal procedures

There are different internal procedures that a service provider needs to have in order to comply with its AML/CFT obligations. The mandatory ones are for Customer Due Diligence, reporting of unusual transactions and recordkeeping. These procedures need to be, preferably, written down in the compliance policy of the service. The reason why it is chosen to cover these in a separate paragraph is because they are very important obligations.

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 4 elements:
1. Identification and verification of the identity of the client/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 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 the P&G). A simplified CDD is not mandatory but a standard and enhanced CDD are.

Please be referred to Chapter 2 of the 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 legislation
  - ✓ Are clients/customers being identified in a proper way?
  - ✓ Are UBO/s 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 client/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 with indicators. The specific indicators can be found in Chapter 3 of the P&G. The CO is responsible for the reporting of unusual transactions to the FIU. 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 CO when an unusual transaction is discovered. The CO will then assess the internal report and report on his/her turn to the FIU.
What an evaluator needs to review:

- Are the right transactions being reported to the CO?
  - ✓ Do employees understand the indicators?
- Are the right transactions being reported to the FIU?
  - ✓ Do the CO 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 CO aware of the *no tipping off* clause?

Suggestions of methods to review the above:

- Review of the internal reporting procedure and/or forms
- Interview with employees dealing with transactions
- Interview with CO

Recordkeeping
A service provider needs to keep transaction records, CDD records and reporting records for at least 5 years after a business relationship has ended.

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

What an evaluator needs to review:

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

Suggestions of methods to review the above:

- Test of record keeping system
- Interview CO
- Observation of archives

Internal controls & communication
It is important that there be sufficient communication between the CO, management and the employees to make sure that everybody knows what their responsibility is in the AML/CFT regime of the service provider. Internal controls are also necessary to make sure that the 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 CO & employees?
  - ✓ Does the CO evaluate the employees?
  - ✓ How frequent do meetings/evaluations take place?
  - ✓ Are meetings recorded in minutes?
  - ✓ How are problems/issues identified and/or brought up?
  - ✓ How are solutions being created for problems raised?
- Is there sufficient communication between CO & management?
  - ✓ Does the CO give feedback to management? How often?
  - ✓ Are meetings recorded in minutes?
  - ✓ How are problems/issues identified and/or brought up to management?
  - ✓ How are solutions being created for problems raised?

Suggestions of methods to review:
- Interview CO
- 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 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 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 within 30 days of finalization of the report.

Any questions or comments? Please contact the Supervision Department of the FIU at: judith.bain@fiu.gov.sx or call us on 542-3025 ext. 112.