CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Company (Trust) Service Providers

September 2013

TABLE OF CONTENTS

PREFACE

The FATF standards have been revised to strengthen global safeguards and further protect the integrity of the financial system by providing jurisdictions with more effective tools to take action against financial crime. At the same time, these revised standards also address new areas relative to corruption, the financing of proliferation of weapons of mass destruction and tax crimes. Jurisdictions will now have to adhere to the revised FATF standards and all mutual evaluations during the FATF fourth round of evaluations will be conducted based on the aforementioned revised standards.

Whereas the new methodology to be used in the fourth round of evaluations has been adopted, the new International Co-operation Review Group's (ICRG) referral criteria are still being discussed.

Curaçao and Sint Maarten still have to address some issues in the Recommended Action Plan set out in the CFATF Mutual Evaluation Reports as a result of the lastly conducted evaluation of both jurisdictions. The recommended actions are based on the former FATF 40 Recommendations and the FATF 9 Special Recommendations.

In light of the aforementioned the Bank has, in order for both Curaçao and Sint Maarten to be fully compliant with the FATF 40 Recommendations and the FATF 9 Special Recommendations with regard to the Bank's Provisions and Guidelines on AML & CFT, revised these Provisions and Guidelines.

These revised Provisions and Guidelines reflect therefore fully the observance of the recommended action plan made by the CFATF.

In the next revision of the Provisions and Guidelines reference to the renewed FATF Recommendations will be incorporated.

I NATURE AND LEGAL BASIS OF THE PROVISIONS

The Centrale Bank van Curaçao en Sint Maarten (hereafter the "Central Bank") is committed to the fight against money laundering and terrorist financing. Because of this commitment, and Curaçao and Sint Maarten being a member of both the Financial Action Task Force on Money Laundering (FATF)[1] and the Caribbean Financial Action Task Force (CFATF)[2], the Central Bank has introduced a comprehensive framework to prevent and combat money laundering and terrorist financing.

These Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Company (Trust) Service Providers are issued by the Central Bank pursuant to the following legal provisions:

- The NORUT, article 22h, paragraph 3;
- The NOIS, article 2, paragraph 5, and article 11, paragraph 3; and
- The National Ordinance on the Supervision of Trust Service Providers, article 11, paragraph 1 (N.G. 2003, no. 114).

Laws or executive decrees
The main laws or executive decrees relating to money laundering and terrorist financing (where applicable as amended) are:

a) The Code of Criminal Law (Penal Code) (N.G[3]. 2011, no. 48);
b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT);
c) The National Decree containing general measures on the execution of articles 22a, paragraph 2, and 22b, paragraph 2, of the National Ordinance on the Reporting of Unusual Transactions (National Decree on Penalties and Administrative Fines for Reporters of Unusual Transactions) (N.G. 2010, no. 71);
d) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS);
e) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
f) Ministerial Decree with general operation of May 21, 2010, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Decree Indicators Unusual Transactions) (N.G. 2010, no. 27);
g) Ministerial Decree with general operations of March 15, 2010, implementing the National Ordinance on Identification of Clients when Rendering Services (N.G. 2010, no. 11);
h) Ministerial Decree with general operation of March 15, 2010 for the execution of the NORUT (N.G. 2010, no. 10);
i) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93) ;
j) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74);

[1] See appendix 1 for the definition or explanation or summary.
[2] See appendix 1 for the definition or explanation or summary.
[3] N.G.: National Gazette, official national publication.

k) National Decree providing for general measures, of 8th August 2011, for the implementation of articles 1, first paragraph, subsection b, under 16º, 6, subsection d, under 12º and 11, second paragraph, of the National Ordinance on the Identification of Customers when Providing Services (National Decree designating services, data and supervisors under the National Ordinance on the Identification of Customers when Providing Services); and
l) National Decree providing for general measures, of 8th August 2011, for the implementation of articles 1, first paragraph, subsection a, under 16°, and 22h, second paragraph, of the National Ordinance on the Reporting of Unusual Transactions (National Decree designating services, data and supervisors under National Ordinance on the Reporting of Unusual Transactions).

These laws and decrees serve as the basis for further actions by the financial sector of Curaçao and Sint Maarten to detect and deter money laundering and terrorist financing.

The Provisions and Guidelines contribute to the adequate implementation by all supervised (financial) institutions and individuals of:

- relevant provisions of all the above-mentioned Ordinances and decrees;
- sound internal policies and procedures to detect and deter money laundering and terrorist financing.

The objective of the above-mentioned policies and procedures is to minimize the possibility that supervised (financial) institutions and individuals become involved in money laundering and terrorist financing activities, and thus minimize the risks that their reputation and that of the financial sector of Curaçao and Sint Maarten will be adversely affected. Some of those policies and procedures are described in chapter II.

I.1 Money laundering

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. In practice money laundering covers all procedures to change the identity of illegally obtained funds (including cash) so that it appears to have originated from a legitimate source. All money laundering has three common factors:

1) criminals need to conceal the true ownership and origin of the money;
2) they need to control the money; and
3) they need to change the form of the money.

A simple transaction may be just one part of a sophisticated web of complex transactions illustrated below. Nevertheless, the earliest key stage for the detection of money laundering operations is where the cash first enters the financial system.

Stages of money laundering

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert (financial) institutions to criminal activity.

1) Placement:
During this first stage of the money laundering process, illegal monies are introduced into the financial system e.g. through deposits in a bank account. Illegal proceeds are easier to detect at the placement stage, when the physical currency enters the financial system.

2) Layering:
Illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

3) Integration:
This stage provides apparent legitimacy to criminally derived wealth or income. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

I.2 Terrorist financing

An institution that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activities, is committing a criminal offence. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activities or were derived from lawful activities but intended for use in support of terrorism.

To help financial institutions identify financing of terrorism, the FATF issued a publication titled: "Guidance for Financial Institutions in Detecting Terrorist Financing"[4] dated April 24, 2002. The publication provides guidance to (financial) institutions to identify financial transactions related to terrorism and also provides the institution with websites containing lists of persons and organizations suspected of being involved terrorism.

The Central Bank instructs the supervised institutions to continuously match their clients' database with the names on the United Nations list.[5] .

I.3. Risk-Based Aproach

Based on the FATF recommendations, particularly those related to (a) customer due diligence (Recommendations 5, 6, 8 and 9), (b) businesses' internal control systems (Recommendation 15), and (c) approach of oversight/monitoring (Recommendation 24), company (trust) service providers are allowed to apply a Risk-based Approach ("RBA"). By adopting a RBA, it is possible for company (trust) service providers[6] to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This entails that although all clients should be subject to the minimum due diligence standards outlined in section II.2.A of these Provisions and Guidelines, clients identified by the institution as high risk must be subject to enhanced customer due diligence

[4] The full document can de consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
[5] The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.
[6] The activities of trust service providers operating in Curaçao or Sint Maarten are similar to those of company service providers operating in other jurisdictions.

while low risk clients may be subject to simplified/reduced customer due diligence, as outlined in section II.2.A.

Company (trust) service providers applying the RBA must document their policies, procedures and controls relative to their applied RBA. Furthermore, they must on an ongoing basis monitor the effective operations of the policies, procedures and controls concerning their RBA and, when needed, make the necessary amendments to these policies, procedures and controls.

I.4 Sanctions

Company (trust) service providers are required to comply with the compulsory requirements set out in the NORUT and/or NOIS and the Provisions and Guidelines. Breaches of the obligations set out under aforesaid regimes are punishable and will result in disciplinary action(s) by the Central Bank.

During its on-site examinations, the Central Bank will assess the supervised institutions' and the individuals' compliance with these Provisions and Guidelines and all other Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) legal obligations. Breaches of the obligations set out under aforesaid regulations are subject to sanctions by the Central Bank.

II PROVISIONS AND GUIDELINES ON THE DETECTION AND DETERRENCE OF MONEY LAUNDERING AND TERRORIST FINANCING FOR COMPANY (TRUST) SERVICE PROVIDERS

This chapter addresses the relevancy of the detection and deterrence of money laundering and terrorist financing for company (trust) service providers[7]. The due diligence process applicable to the company (trust) service providers described in this chapter, comprises the due diligence process relative to the company (trust) service providers' clients and, if applicable, the clients of the persons placed on Exhibit "A" and "B" to the company (trust) service providers' license. Subsequently, some policies and procedures for company (trust) service providers to detect and deter money laundering and terrorist financing are addressed as well as the information and documentation to be collected from their clients. The chapter concludes with a listing of the information and documentation of the relevant policies and procedures that the company (trust) service providers must provide to the Central Bank.

Company (trust) service providers must at all times adhere to the stipulations in these Provisions and Guidelines. In the event that another party is entrusted with (part of) a company (trust) service provider's activities relative to AML/CFT, the company (trust) service provider remains ultimately responsible to ensure adherence to these Provisions and Guidelines.

The Central Bank requires all company (trust) service providers that have outsourced (part of) their activities relative to AML/CFT, to clearly indicate in an agreement that the person to whom they have outsourced (part of) these activities will adhere to the laws and regulations related to money laundering and terrorist financing applicable to the company (trust) service provider while carrying out his or her duties for the company (trust) service provider. This contract must be signed by both the company (trust) service provider and the person to whom (part of) the AML/CFT activities of the company (trust) service provider are outsourced.

II.1 The relevancy of the detection and deterrence of money laundering and terrorist financing for company (trust) service providers

The occurrence of money laundering and terrorist financing and the counter measures to detect and deter these phenomena has over the past years been more evident in the traditional banking sector than in the other (financial) sectors.

However, as banks are continuously taking measures to detect and deter money laundering and terrorist financing, other institutions, including company (trust) service providers, have become increasingly vulnerable to money launderers and terrorists as they seek to launder their funds derived from criminal activities and finance their terrorist activities respectively.

Company (trust) service providers are less conducive to the initial placement of criminally derived funds than other types of financial institutions, such as banks. Nonetheless, company (trust) service providers are prone to be used for the set up and management of complicated structures through which money may be laundered or terrorist funds channeled. Company (trust) service providers may thus be misused for money laundering and terrorist financing purposes at particularly the layering and integration stages.

[7] See Appendix 1 for the definition or explanation or summary.

It is therefore imperative that all company (trust) service providers be constantly vigilant in deterring criminals from engaging in any form of money laundering and terrorist financing. Public confidence in company (trust) service providers, and hence their stability, can be undermined by adverse publicity as a result of their unwittingly use by criminals for money laundering and terrorist financing purposes. If company (trust) service providers do not establish proper policies and procedures to adhere to, they may unwittingly be used by criminals for the entering or mediation of transactions from or intended for criminal activities.

In this context, the Central Bank is issuing these Provisions and Guidelines to further promote and maintain the financial stability, soundness and reputation of company (trust) service providers operating in or from Curaçao and Sint Maarten. These Provisions and Guidelines must serve as a tool for further implementation of the NOIS and NORUT.

Due to the diversity in the activities of company (trust) service providers, the nature and scope of their vigilance systems may vary according to their size and complexity. Nonetheless, company (trust) service providers must exercise due diligence by ensuring that at least they have in place policies and procedures including a policy statement covering certain aspects relevant to the detection and deterrence of money laundering and terrorist financing. This is further discussed in the next sections.

II.2 Policy statement

The Board of Directors[8] and senior management[9] of a company (trust) service provider must issue a policy statement that clearly expresses the commitment of the company (trust) service provider to combat the abuse of its facilities and services for money laundering and terrorist financing purposes. The obligation to issue a policy statement also applies to a natural person that provides trust services to international companies. The policy must state the company (trust) service provider's intention to comply with current anti-money laundering and terrorist financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions.

This policy statement is a statement of "Best Practice" of the company (trust) service provider, which outlines the company (trust) service provider's policies and procedures and must also be communicated to the employees of the company (trust) service providers being a legal person.

The policy statement[10] also must cover the following items:

- The implementation of a formal system of internal control to identify (prospective) clients, deter, detect, and report unusual transactions, and keep adequate records of the clients and transactions.

[8] See Appendix 1 for the definition or explanation or summary.
[9] See Appendix 1 for the definition or explanation or summary.
[10] In the design, update and implementation of their policy statement, the Bank instructs company (trust) service providers to (continuously) observe the relevant standards from international (standard setting) bodies and ensure that these standards are included in their policy statements. Those standards include amongst others: "The Forty Recommendations" and the "Special Recommendations on Terrorist Financing" of the Financial Action Task Force (FATF). The relevant documents are located at http://www.fatf-gafi.org.

- The preparation of an appropriate training plan for and the training of personnel of a company (trust) service provider that is a legal person or for the company (trust) service provider that is a natural person to increase awareness and knowledge in the area of money laundering and terrorist financing prevention and detection.

- The appointment of one or more compliance officers at management level[11], responsible for ensuring the day-to-day compliance with these procedures. The officer must have the authority to investigate unusual transactions extensively. If the company (trust) service provider is a natural person, this natural person must be entrusted with the compliance function.

- A system of independent testing of the policies and procedures by the company (trust) service provider's internal audit personnel or by a competent external source to ensure their effectiveness.

In the design, update, and implementation of their policy statement, the Central Bank instructs company (trust) service providers to (continuously) observe the relevant standards from international (standard-setting) bodies and ensure that these standards are included in their policy statements.

II.2.A Detection and deterrence of Money Laundering

Company (trust) service providers have the obligation to identify their (prospective) clients/customers [12], including, where applicable, the (ultimate) beneficiaries [13] of their prospective clients/customers, before rendering them their services. Company (trust) service providers must maintain an information program to inform those clients of the objectives of the relevant anti-money laundering legislation and inherent requirements for company (trust) service providers. The internal procedures of a company (trust) service provider must clearly indicate for which services clients or their representatives must identify themselves and which identification documents are acceptable.

The allowed client identification documents and the nature of the transaction are prescribed in the NOIS [14]. The required information must be regularly updated and adequately documented. Company (trust) service providers must have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, account files and business correspondence and on their retention period for current as well as terminated business relationships. An important objective for company (trust) service providers is to be able to retrieve this information, without any undue delay. Hence, the Central Bank requires the company (trust) service providers to implement a checklist containing identification and/or transaction information, and to maintain a centralized record keeping system to retain copies. Company (trust) service providers must ensure that the

[11] Management level is considered a position whereby the compliance officer has:
1. unlimited access to all relevant information for the execution of his/her task;
2. authority to analyze cases independently; and
3. authority to report to the Financial Intelligent Unit (MOT).

[12] See Appendix 1 for the definition or explanation or summary.

[13] See Appendix 1 for the definition or explanation or summary.

[14] See Appendix 1 for the definition or explanation or summary.

identification documents are valid at all times. Reference is in this respect also made to article 3, paragraph 3 of the NOIS.

Furthermore, company (trust) service providers must have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions. These policies and procedures must apply when establishing customer relationships and when conducting ongoing due diligence. Examples of non-face-to-face business relationships or transactions include: business relationships or transactions concluded over the internet or by other means such as through the post. Measures for managing the risks must include specific and effective customer due diligence procedures that apply to non-face-to-face clients. Examples of issues to be addressed in these procedures are: the certification of documents presented; the requisition of additional documents to complement those which are required for face-to-face clients; the development of independent contact with the customer; reliance on third party's introduction and the requirement that the first payment be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Foreign branches and subsidiaries

Company (trust) service providers are required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e., host country) laws and regulations permit. Company (trust) service providers are required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations.

Where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (i.e., host country) laws and regulations permit.

Company (trust) service providers are required to inform the Central Bank 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.

Customer due diligence ("CDD")

Before the provision of trust services to a client, identification of a prospective client must be made from documents issued by reliable sources as prescribed in the NOIS and whenever applicable/possible the directors, representatives or Ultimate Beneficial Owners of the prospective client must be interviewed personally. Company (trust) service providers are also required to obtain and document information on the purpose and intended nature of the business relationship with their (prospective) clients prior to offering them their services.

Company (trust) service providers are in that respect required to request their client to fill out and sign the Source of Funds Declaration Form[15] enclosed in Appendix 2 to these Provisions and Guidelines, both at the establishment of the business relationship and subsequent receipt of funds for capitalization, payments, transfers or incoming funds destined for other purposes. The Source of Funds Declaration Forms must be kept on file.

[15] See Appendix 2.

Furthermore, company (trust) service providers are encouraged to perform antecedent screening on persons subject to CDD. This could be done by e.g. searching the internationally accepted authoritative lists on the internet.

Face-to-face CDD

When conducting face-to-face CDD or executing transactions for which instructions have been received on a face-to-face basis, a company (trust) service provider must:

- provide a copy of the original identification document or the original transaction document with the text: "Mr. and or Mrs. ……. appeared to me in person"; and a stamp with the prevailing date; and
- add the signature of the client as well as the name and signature of the employee who performed the CDD or executed the transaction, to the original document.

Non-face-to-face CDD

When identification takes place on a non-face-to-face basis, a copy of the identification document is sufficient, under the condition that the identification document is accompanied by a certified extract of the civil registry of births, marriages and deaths of the place of residence of the party concerned or that the document is certified by a notary public or embassy/consulate. The name, address and telephone number of the notary public or embassy/consulate, as well as the name and contact details of the institution's officer who actually performed the CDD must be clearly indicated. Furthermore, the submitted copy of the identification document, including the photograph, must be clearly legible.

Identification of (prospective) clients by company (trust) service providers

As indicated in the definition in appendix 1, the term "client" in the context of a company (trust) service provider, does not only refer to the international company to which trust services are provided, but also to the applicant upon whose instructions the business relationship with the company (trust) service provider is established. The applicant who provides the instructions may or may not be the prospective international company to which trust services are provided.

Therefore, the company (trust) service provider must look beyond the international company for due diligence purposes and, depending upon the circumstances, requests proof of identity of any of the following parties:

- the (managing and supervisory) directors of the international company;
- the (ultimate) beneficial owners or beneficiaries of the international company;
- in case any of the parties mentioned above is a legal entity, the directors of and the (ultimate) beneficial owners holding a qualifying interest[16] in the legal entity. Please note that a proof of registration of the legal entity with the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation must also be requested.

Pursuant to article 3 of the NOIS, the identity of the above-mentioned parties (whether resident or non-resident) must be established through one of the following valid documents:

- a driver's license;
- an identity card issued;

[16] See Appendix 1 for the definition or explanation or summary.

- a travel document or passport;
- other document to be designated by the Minister of Finance.

Verification of the identity of resident individuals

In addition, the identity of a **resident** individual must be verified when a business relationship is established with the international company. The identity of a resident individual that has previously been subjected to the company (trust) service provider's CDD must also be verified when the company (trust) service provider has doubts about the veracity or adequacy of the identification data obtained in the past from this individual. Examples of verification include:

- checking a local telephone directory;
- seeking confirmation of identity or activities at other institutions;
- verifying occupation and name of employer;
- requesting reference letter(s);
- checking name and address of references;
- requesting a copy of an utility bill.

Verification of the identity of non-resident individuals

Verification of the identity of **non-resident** individuals must be obtained by reference to one or more of the following ways, as deemed practical and appropriate:

- existing banking relationships of the individual;
- international or home country telephone directory;
- personal reference by a known business relationship;
- embassy or consulate in home country of address provided by the individual;
- original or certified copy of utility bill showing the name and complete address of the person concerned;
- tax bill/refund showing the name and complete address of the person concerned;
- if a personal account check is tendered to the company (trust) service provider, comparison of signature thereon; and
- if provided, cross reference address printed on personal check to permanent address provided by the individual.

Company (trust) service providers should complete the verification of the non-resident individuals subjected to its CDD before or during the establishment of the business relationship, provided that:

a) This occurs as soon as reasonably practicable.
b) This is essential in order to not to interrupt the normal conduct of business..
c) The money laundering risks are effectively managed.

Verification of the existence and nature of the international company's business

In addition to obtaining the identification documents of the above-mentioned parties associated with the international company, the company (trust) service provider must verify the existence and nature of the international company's business through reliable identification documents, with preference for originals and official documents.

The existence and nature of a (prospective) international company must be legally identified with the aid of a certified extract from the register of the Chamber of Commerce and

Industry, or an equivalent institution, in the country of domiciliation, or with the aid of an identification document to be drawn up by the company (trust) service provider. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.

Documents regarding the international company containing at least the following information must be kept on file:

- official name according to its articles of association or similar document[17];
- trade name, if different;
- registered address in full;
- country of incorporation and/or country of seat;
- registration number in the country of incorporation or establishment;
- organizational chart of the structure of which the international company is part of; and
- name of the persons who exercise ultimate effective control in the international company; and
- control structure of the international company.

The company (trust) service provider may require additional information to be provided by the international company, such as:

- shareholders' register;
- certificate of incorporation;
- articles of association;
- a list to include full names of all directors (including supervisory directors, if applicable) to be signed by a minimum number of those directors sufficient to form a quorum;
- a list to include names and signatures of other officials authorized to sign on behalf of the international company, together with a designation of the capacity in which they sign;
- audited financial statements/cash flow statements; and
- business plan.

If a company (trust) service provider is unable to comply with the aforementioned CDD requirements, the company (trust) service provider should not commence a business relation with a proposed client. In addition, the company (trust) service provider should consider filing a report with the Financial Intelligence Unit ("FIU"). The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties ("MOT").

Ongoing CDD

The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. While the on-going due diligence process must also include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the company (trust) service provider's knowledge of the client, its business and risk profile, and where necessary, the source of funds. In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the FIU.

[17] Documents such as Memorandum & Articles of Association and/or Certificate of Incorporation and/or Certificate of Good Standing.

Company (trust) service providers must apply CDD requirements to existing customers[18] and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

Examples of when it may otherwise be an appropriate time to do so is when:

(a) a transaction of significance takes place;
(b) there is a material change in the way that the account is operated;
(c) customer documentation standards change substantially; and
(d) the company (trust) service provider becomes aware that it lacks sufficient information about an existing customer.

In the latter instances, updated copies of the identification document must be collected and retained.

Furthermore, the company (trust) service provider must ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.

Identification of Politically Exposed Persons

Company (trust) service providers must have appropriate risk management in place to determine whether its (proposed) clients are considered political exposed persons ("PEP's) and must conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The institution's decision to enter into business relationships with a PEP must be taken at its senior management level. The institution must make reasonable efforts to ascertain that the PEPs source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. Company (trust) service providers must not accept or maintain a business relationship if the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, institutions must obtain senior management's approval to continue the business relationship. Where the institution is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

Nominee shareholder service[19]

All company (trust) service providers that provide nominee shareholder services and/or provide custody of bearer shares must know the true identity of the person/persons (resident or non-resident) for whom assets are held or are to be held, including the (ultimate) beneficial owner(s). The identity of these clients must be established in accordance with the identification procedures previously mentioned.

Anonymous accounts or accounts in fictitious names

Anonymous accounts or accounts in fictitious names are prohibited.
Where numbered accounts are opened by a company (trust) service provider on behalf of its clients, the company (trust) service provider is required to maintain this account in such a way

[18] Existing customers as at the date that the national requirements are brought into force.
[19] See Appendix 1 for the definition or explanation or summary.

that full compliance can be achieved with the FATF Recommendations. For example, the company (trust) service provider must properly identify the customer in accordance with these criteria, and the customer identification records must be available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

Beneficiaries of a trust[20] as the (ultimate) beneficiaries of a client

The following types of trusts are broadly identified:

- **Bare trust / Fixed trust**: In a Bare/Fixed trust, property is vested in the trustee by the settlor, for the benefit of the beneficiary. There are no complicated rules as to how the trustee may decide who benefits from the trust or indeed what the trust property actually is. The bare trust can also be described as a fixed trust because the beneficiaries' interests are clearly defined.
- **Discretionary trust**: In a Discretionary trust, trustees have the power to distribute the property as they think fit in accordance with the rules set out in the Trust Deed.

Where the trust is identified as a bare or fixed trust, it is the settlor that must be identified as the person exercising effective control over the trust and the trustees as the ultimate beneficiaries of the trust. Therefore, CDD measures as previously described must be applied to both the trustee, being the ultimate beneficiary, and the settlor of the trust.

Where the trust is identified as a discretionary trust, the ultimate beneficiary is not previously established. In such a case, a distinction must be made between applicable CDD measures at time of establishing the trust and CDD measures applicable at the time of appointment of beneficiaries of the trust. When the trust is established and thereby the client relationship is created, in case of a discretionary trust, CDD measures apply to the settlor of that trust. As soon as the beneficiaries of the trust are appointed, the company (trust) service provider is required to perform proper CDD on the beneficiary (ies).

Reliance on intermediaries or other third parties to perform some of the elements of the due diligence process

Company (trust) service providers may rely on intermediaries or other third parties to introduce business or perform the following elements of the CDD process:

a. identification and verification of the customer's identity;

b. identification and verification of the beneficial owner; and

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

If company (trust) service providers rely on intermediaries or other third parties to perform some of the elements of the CDD process[21] or to introduce business, they must take the following steps:

- immediately obtain from the third party the necessary information concerning the performed elements of the CDD process;

[20] See Appendix 1 for the definition or explanation or summary.

[21] In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another financial institution or third party.

- take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay, however, not longer than within a timeframe of 2 working days;
- satisfy themselves that the third party is AML/CFT regulated and supervised (in accordance with FATF Recommendation 23, 24 and 29), and has measures in place to comply with the required CDD requirements;

In addition, in case of reliance on foreign third parties, company (trust) service providers must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. A jurisdiction is adequately supervised when its Mutual Evaluation Report[22] discloses less than 10 "Non Compliant or Partially Compliant" ratings regarding the 16 "key and core[23]" FATF Recommendations.

If company (trust) service provider rely on intermediaries or other third parties to perform elements of the CDD process, a service level agreement will be required in case the complete CDD process has been outsourced to an intermediary or third party. The service level agreement must be readily available for the Central Bank when conducting on-site visits. In case only one or two elements of the due diligence process is/are performed by an intermediary or third party (like for example identifying the client and verifying the copy of a passport) then a service level agreement is not required.

It should be noted that even though acompany (trust) service provider may rely on other third parties for part of the CDD process or the process may be outsourced, the ultimate responsibility for customer identification and verification remains with the company (trust) service provider relying on the third party.

Risk-based Approach

(a) Risk classification

A company (trust) service provider must develop risk profiles for all its customers to determine which categories of clients expose it to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a client, must take place after the CDD information mentioned above has been obtained. The risk profile must comprise minimally the following possible categories: low, medium and high risk. Company (trust) service providers must apply CDD requirements to existing clients and may determine the extent of such measures on a risk sensitive basis depending on the type of client, business relationship, or transaction.

Company (trust) service providers must at least consider the following risk categories while developing and updating the risk profile of a client: (i) customer risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk.

(i) Customer risk: It is important for a company (trust) service provider to assess the type of client and the nature and scope of the business activities of the client. The types of clients or business activities that indicate a higher risk include:

- Politically exposed persons (PEPs) and their families and associates;
- Cash and cash equivalent intensive businesses, such as money remitters, casinos, (internet) gambling businesses;
- Clients engaging in business activities regarded as sensitive, such as pornography, arms trading and the provision of military security services;
- Clients where the structure or nature of the entity or relationship makes it difficult to identify and verify the true owner or controlling interests;
- Charities and non-profit-organizations which are not subject to monitoring or supervision;
- Financial institutions and designated non-financial businesses and professions that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised;
- Clients where there is no commercial rationale for them making use of the services offered by the company (trust) service provider that request undue levels of secrecy, or where it appears that an audit trail has been deliberately broken or unnecessarily layered;
- Transaction of significance takes place (from time to time);
- Material change takes place in the way the account is operated;
- Client documentation standards change substantially; and
- Determination of lack of or insufficient information about an existing client.

(ii) Products/services risk: An effective risk assessment must also include determining the potential risk presented by products and services offered by the company (trust) service provider. A key element is the establishment of the existence of a legitimate business, economic, tax or legal reason for the client to make use of the products/services offered by the company (trust) service provider. Determining the risks of products and services must include the consideration of factors such as:

- Private banking activities;
- Ability to make payments to or receive payments from unassociated or unknown third parties;
- Services where the receipt and transmission of cash proceeds are possible;
- Services to conceal beneficial ownership from competent authorities;
- Transactions or services with no apparent legitimate business, economic, tax, or legal reasons; and
- The offer by clients to pay extraordinary fees for services which would not ordinarily warrant such a premium.

(iii) Country or Geographic Risk: Country risk provides useful information as to potential money laundering and terrorist financing vulnerabilities. The following countries and territories are regarded as high risk countries and territories:

- Countries subject to sanctions and embargoes issued by e.g. the United Nations and the European Union;
- Countries identified by FATF and FATF-style regional bodies as lacking appropriate AML/CFT laws, regulations and other measures; and
- Countries identified by credible sources, such as FATF, FATF-style regional bodies, IMF and the World Bank, as providing funding or support for terrorist activities, or as having designated terrorist organizations operating within them.

(iv) Delivery Channels Risk: This particular risk category deals with the manner in which the company (trust) service provider establishes and delivers products and services to its clients. While assessing the vulnerabilities posed by the distribution channels of its

products and services, the company (trust) service provider must at least consider the following factors:

- The use of third parties introducers and intermediaries to conduct (some of the) elements of the client due diligence process that do not meet all of the criteria mentioned under section II.2.A above relative to reliance on third parties;
- The establishment of the relationship with the client remotely (non-face to face);
- The control of the relationship or transactions remotely (e.g. straight-through processing of transactions);
- Pooled relationships with intermediaries, which due to the anonymity provided by the co-mingling of assets or funds belonging to several clients by the intermediary, tend to be more vulnerable.

The weight assigned to these risk categories (individually or in combination) in assessing the overall risk exposure may vary from one company (trust) service provider to another. The company (trust) service provider must make its own determination as to the assignment of the risk weights.
The result of the risk assessment of a particular client, as evidenced by the risk profile, will determine if additional information needs to be requested, if the obtained information needs to be verified, and the extent to which the resulting relationship will be monitored.

Enhanced CDD for high risk categories of customers
Company (trust) service providers must conduct enhanced due diligence in all of the high risk cases/circumstances mentioned above and in any other high risk cases/circumstances identified by the company (trust) service providers, according to their risk assessment framework. The company (trust) service provider's decision to enter into or to continue business relationships with such clients must be taken at its senior management level.

Company (trust) service providers must not accept or maintain a business relationship if the company (trust) service provider knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

The company (trust) service provider must ensure that the identification documents of its high risk categories of customers are at all times valid.

Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, company (trust) service providers must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, company (trust) service providers are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.

High-risk and non-cooperative jurisdictions.
Jurisdictions are considered as high-risk and non-cooperative when they have detrimental rules and practices in place which constitute weaknesses and impede international co-operation in the fight against money laundering and terrorism financing.

Countries that have 10 or more "Non Compliant(NC) or Partially Compliant (PC)" ratings of the 16 "key and core[24]" FATF Recommendations in their Mutual Evaluation Report (of

[24] The core Recommendations are: Recommendations 1, 5, 10 and 13 and Special Recommendations II and IV

the FATF, IMF or FSRB [25]) can be considered high risk jurisdictions when they have not showed a high level of commitment to remedy their deficiencies in a reasonable timeframe. The FATF and some FSRB's do issue statements on these countries.

Company (trust) service providers are required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations including the high-risk and non-cooperative jurisdictions. The same holds for the customers. Company (trust) service providers must exercise special care when their customers have business relations in those countries. If these business relationships and transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions must, as far as possible, be examined, and written findings must be available for at least five years to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU/MOT and auditors). If unusual transactions are detected, then these must be reported to the FIU/MOT.

Furthermore, company (trust) service providers must continuously consult the FATF's, CFATF's and/or the Central Bank's website for the most recent version of the FATF and the CFATF Public Statements moreover, the related FATF documents on the High-risk and non-cooperative jurisdictions.

Simplified/reduced CDD

The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless, there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances the company (trust) service provider is allowed to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

Examples of customers where the risk may be lower include:

(a) Financial institutions that are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those requirements;
(b) Public companies that are subject to regulatory disclosure requirements. This refers to companies that are listed on a securities exchange or in comparable situations; or
(c) Government administrations or enterprises.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

The key Recommendations are: Recommendations 3, 4, 23, 26, 35, 36 and 40 and *Special Recommendations I, III and V*

[25] FATF Style Regional Body

II.2.A.1. Recognition, documentation and reporting of unusual transactions

Company (trust) service providers are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is therefore important for every company (trust) service provider to have adequate procedures for its personnel in place. These procedures must cover:

a) the recognition of unusual transactions;
b) the documentation of unusual transactions; and
c) the reporting of unusual transactions.

Re.: a) Recognition of unusual transactions

An unusual transaction will often be a transaction which is inconsistent with an international company's known legitimate business activities. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the client's or its representative's "bona fides" and potential criminal background.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which company (trust) service providers must assess if a customer's transaction qualifies as an unusual transaction. Those indicators are listed in Appendix 3. Furthermore, in the enclosed appendix 4 to these provisions and guidelines, some examples of unusual activities/behavior by international companies are outlined. These examples may serve company (trust) service providers as guidance in their effort to assess whether certain transactions conducted may be considered unusual.

Company (trust) service providers are required to pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Company (trust) service providers are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing and keep these findings for at least five years to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors).

In this context, the employees of the company (trust) service provider that is a legal person or the company (trust) service provider that is a natural person must not only focus on the establishment of a relationship, but also on other aspects such as subsequent transactions, the frequency of the transactions, duration of existence of the international company, and where applicable, the relationships of the international company serviced and/or engagement by the international company in other business activities.

Company (trust) service providers with advanced computer information systems are encouraged to develop special programs to select objectively defined unusual transactions. Furthermore, the company (trust) service provider must provide its staff with specific guidance and training to recognize and document adequately the unusual transactions.

<u>Wire transfer</u>
Internationally, wire transfers are increasingly becoming a method to launder funds from illegal sources and for illegal activities or to finance terrorism. Company (trust) service providers must be extremely vigilant when proceeds are transferred from or to accounts with

financial institutions licensed in jurisdictions where anti-money laundering measures and practices are known to be absent and/or inadequate.

Based on FATF Special Recommendation (SR) VII[26], company (trust) service providers must include accurate and meaningful originator information (at least the name, address and account number if existent, otherwise a unique reference number) on funds transfers on behalf of their clients within or from Curaçao and Sint Maarten and related messages that are sent. In case the company (trust) service provider receives a fund transferred from a third party to the company (trust) service provider's client, the company (trust) service provider must ensure that the fund transfer information is accurate and complete. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds[27]. Company (trust) service providers must observe the latest Interpretative Note to SR VII and apply its relevant parts. The full text of the note may be consulted on FATF's website at: http://www.fatf-gafi.org. Also, further scrutiny is required and reporting to the FIU/MOT[28] must be considered.

Misuse of technological development

For electronic services, company (trust) service providers could refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003. Company (trust) service providers are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

Re.: b) The documentation of unusual transactions

To guard against money laundering and terrorist financing, it is important for company (trust) service providers to provide an audit trail for suspicious/unusual funds or transactions. This must be done through documentation of all detected and reported unusual transactions.

Re.: c) Reporting of unusual transactions

Company (trust) service providers must have clear procedures which are communicated to their personnel for the reporting of unusual transactions.

There may be circumstances where a company (trust) service provider declines to establish a business relationship with a potential client or refuses to render additional trust services to an existing client because of serious doubts about the client's or its representative's "bona fides" and potential criminal background. While all decisions must be based on normal business criteria and the company (trust) service provider's internal policy to guard against money laundering and terrorist financing, it is important for the company (trust) service provider to provide an audit trail for suspicious activities and report all the (intended) unusual activities to the FIU/MOT without delay.

[26] In October 2001, the FATF issued eight Special Recommendations on Terrorist Financing. Special recommendation VII refers to measures with respect to wire transfers.

[27] Company (trust) service must observe the Interpretative Note to SR VII and apply its relevant parts.

[28] See appendix 1 for the definition or explanation or summary.

Internal reporting

The individual transaction or series of transactions which qualify as unusual must be reported internally without undue delay. All transactions as mentioned in the ministerial decree regarding the Indicators for Unusual Transactions must be referred to the designated officers in a format which contains at least the data as stipulated by law.

Whenever available, additional documents such as copies of the identification documents, account statements, checks and account ledgers records must also be submitted as supplements. Management may choose to require that some categories of unusual transactions be drawn to its attention. The designated officer(s) must keep an adequate filing system for these records.

If internally reported transactions are not reported to the FIU/MOT by the compliance officer or the person responsible for the compliance function, the reasons therefore must be adequately documented and signed off by this person and/or by management.

External reporting

Company (trust) service providers must cooperate fully with the national law enforcement authorities. The designated officers must prepare a report of all unusual transactions for external reporting purposes. Copies of these reports must be kept by the reporting company (trust) service providers on file. For company (trust) service providers being legal persons, the report must be submitted to senior management for its review for compliance with existing regulations.

If an unusual transaction is not authorized by senior management to be incorporated in the report to the FIU/MOT all documents relevant to the transaction including the reasons for non-authorization must be adequately documented, signed off by the designated officer and senior management and kept by the reporting company (trust) service providers.
Taking into account the above mentioned procedure for external reporting, the compliance officer(s) should be able to act independently.

The following must also be addressed in the Policy Statement referred to in section II.2 of these provisions and guidelines:

- the company (trust) service provider and, in case it is a legal entity, also its directors, officials and employees must not warn their clients when information about them is being reported to the FIU/MOT, or on internal inquiries being made by (the compliance staff of) company (trust) service provider on them; and
- the company (trust) service provider and, in case it is a legal entity, its directors, officials and employees must follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.

Exempt lists

In some jurisdictions the use of exempt list for the reporting of unusual transactions is permitted. However, the established laws and regulations, do not allow any exemptions on the reporting obligation of financial service providers.

II.2.A.2 The appointment of one or more compliance officer(s)

Each company (trust) service provider must formally designate one or more officer(s) at management level[29], responsible for the deterrence and detection of money laundering and terrorist financing. If the company (trust) service provider is a natural person, this natural person must be entrusted with the compliance function.

The compliance officer or the aforementioned natural person must be responsible for at least the following:

- to verify adherence to the local laws and regulations governing the detection and deterrence of money laundering and terrorist financing;
- if the company (trust) service provider has a staff, to organize training sessions for the staff on various compliance-related issues;
- to review compliance with the policy and procedures of the company (trust) service provider;
- to analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- to review all internally reported unusual transactions for their completeness and accuracy with other sources;
- to keep records of internally and externally reported unusual transactions;
- to prepare the external report of unusual transactions;
- to execute closer investigation on unusual of suspicious transactions;
- to remain informed of the local and international developments on money laundering and terrorist financing and, where applicable, to make suggestions to management for improvements; and
- to periodically report information on the institution's effort to combat money laundering and terrorist financing to the (Board of) managing directors, including at least the local managing directors.

The above-mentioned responsibilities must be included in the job description of the designated officer entrusted with the company (trust) service provider's anti-money laundering and terrorist financing matters. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities. The officer(s) must have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information.

II.2.A.3 A system of independent testing of the policies and procedures

Company (trust) service providers must maintain an adequately resourced and independent audit function to test compliance (including sample testing) with their policies, procedures and controls. The independent testing must be conducted at least annually by the internal

[29] Management level is considered a position whereby the compliance officer has:
1 unlimited access to all relevant information for the execution of his/her task;
2 authority to analyze cases independently; and
3 authority to report to the unusual transactions center (MOT).

audit department or by an outside independent party, such as the external auditor of the company (trust) service provider.

These tests must include amongst other:

- evaluation of the anti-money laundering and counter terrorist financing manual;
- file review of the international companies to which trust services are provided;
- interviews with employees who handle transactions and with their supervisors;
- sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- assessment of the adequacy of the record retention system.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or to the Board of Directors, and to the designated officer(s) with a request to take prompt corrective actions by a certain deadline.

II.2.A.4 Screening of employees / Appropriate training plans and programs for personnel

Company (trust) service providers must ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. Each company (trust) service provider that has a staff must screen its employees on criminal records.

Company (trust) service providers must develop training programs and provide (ongoing) training to all personnel who handle transactions that may be qualified as unusual or suspicious based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2010, no. 27).

Training must at least address the following:

- creating awareness by the employee of the money laundering and terrorist financing issue, the need to detect and deter money laundering and terrorist financing, the laws and regulations in this respect and the reporting requirements;
- the detection of unusual transactions or proposals, and the procedures to follow after identifying these;
- making sure that the need to verify the identity of the client is understood; and
- the developments in the area of money laundering and terrorist financing.

As far as new employees are concerned, training must be provided to all new employees dealing with clients, irrespective of their level of seniority. Similarly, training must also be provided to existing members of the staff (such as account and assistant account managers) who are dealing directly with clients. These persons are the first point of contact with potential money launderers and terrorists and their efforts are therefore vital to the organization's strategy in curtailing money laundering and terrorist financing.

A higher level of instruction covering all aspects of money laundering and terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

It will also be necessary to make arrangements for refreshment training at regular intervals to ensure that the staff members do not forget their responsibilities and that they are updated on current and new developments in the area of money laundering and terrorist financing techniques, methods and trends. The training must include a clear explanation of all aspects of the laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. This might be best achieved by an annual review of the instructions for recognizing and reporting of unusual transactions.

Company (trust) service providers that are natural persons must also at regular intervals be trained in the area of AML/CFT to remain abreast of the developments in these areas.

In order for a company (trust) service provider to be able to demonstrate that it has complied with the aforementioned guidelines with respect to training, it must at all times maintain records which include:

- details of the content of the training programs provided (for company (trust) service providers that are legal persons) or training programs followed (for company (trust) service providers that are natural persons);
- the names of the person(s) who have received the training;
- the date on which the training was provided;
- the results of any testing carried out to measure the participants' understanding of the money laundering and terrorist financing requirements; and
- an on-going training plan.

II.2.B Detection and Deterrence of Terrorist Financing

Company (trust) service providers must take into account the characteristics including types of transactions listed in annex 1 to the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing"[30]. Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing.

In addition, company (trust) 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 or referred to in:

- Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- annex 2[31] of the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing";
- the listing[32] of the Office of Foreign Assets Control (OFAC)[33] or of other national authorities; and
- the lists issued by the United Nations.[34]

[30] The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
[31] The full document can be consulted located at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
[32] The list is located on FINCEN's website at http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html.
[33] See appendix 1 for the definition or explanation or summary.

Supervised company (trust) service providers must continuously match their clients' database with the names on the above-mentioned lists. If a company (trust) service provider encounters a match, it must freeze the asset of the client and inform the Central Bank immediately.

In addition, company (trust) service providers must be vigilant in the abuse of non-profit organizations for terrorist financing. They must observe the FATF's Special Recommendation (SR) VIII[35] and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices"[36].

If company (trust) service providers suspect or have reasonable grounds to suspect that funds of the international company and/or its related party are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, they must report promptly their suspicion to the FIU/MOT. Reference is made to the Ministerial Decree N.G. 2010, no. 27.

II.3 Record-keeping

Company (trust) service providers must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. Company (trust) service providers must ensure that the investigating authorities must be able to identify a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing.
Where appropriate, company (trust) service providers must consider retaining certain records e.g. customer identification, account files, business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations.

A document retention policy must include the following:

- All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction takes place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior.

- Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued.

- Company (trust) service providers must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities.

In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority, they must be retained until it is confirmed by these parties that the case has been closed.

---

[34] The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.
[35] Special recommendation VIII refers to measures with respect to vulnerable non-profit organizations.
[36] The full document can be consulted at http://www.fatf-gafi.org/pdf/SR-8NPO/en.pdf.

II.4 Examination by the Central Bank

All company (trust) service providers must be prepared to provide information or documentation on their money laundering and terrorist financing policies and deterrence and detection procedures to the on-site examiners of the Central Bank before or during an examination and upon the Central Bank's request during the year. The company (trust) service provider must be prepared to make available at least the following items:

- its written and approved policies and procedures on money laundering and terrorist financing prevention;
- the name of each designated officer responsible for the company (trust) service provider's overall money laundering and terrorist financing policies and procedures and his/her designated job-description;
- records of reported unusual transactions;
- unusual transactions on which closer investigation was required;
- completed source of funds declarations;
- schedule of the training provided to the institution's personnel regarding money laundering and terrorist financing;
- assessment reports on the institution's policies and procedures on money laundering and terrorist financing by the internal audit department or the institution's external auditor;
- documents on system tests such as the clients' transactions data and files, overview of the origin and destination of wire-transfers and other transfers to and from the accounts, and other relevant information; and
- required copies of identification documents.

III OFFENCES AND SANCTIONS IN THE NORUT AND THE NOIS

A company (trust) service provider that does not comply with the compulsory AML/CFT requirements is committing an offence, which is an unlawful and punishable act. The way in which an offence is punished depends on the severity of the offence committed. Offences are subdivided in: misdemeanours and felonies.

In accordance with article 22a, paragraph 1 and article 22b paragraph 1 of the NORUT, the Central Bank has the authority to impose a penalty or an administrative fine on the company (trust) service provider that does not or does not timely comply with the obligations imposed by or pursuant to article 11, article 12 paragraph 2, article 13, and article 22h, paragraph 3.

Pursuant to article 9, paragraph 1 and article 9a paragraph 1, of the NOIS the Central Bank has the authority to impose a penalty or an administrative fine on the company (trust) service provider that does not or does not timely comply with the obligations imposed by or pursuant to article 2, paragraphs 1, 2, 5, article 3, paragraphs1 through 6, article 5 paragraph 1 through 4, articles 6, 7, 8 and article 11, paragraph 3.

The amount of a penalty or fine for the various offences is specified in the National Decree Penalties and Fines Reporters Services Unusual Transactions (ND PFRUT) (NG 2010 no. 71) and the National Decree Penalties and Fines Service Providers (ND PFSP) (NG 2010 no. 70). The Central Bank will report an offence to be criminally investigated or prosecuted by the law enforcement in circumstances where the offender emphatically refuses to comply with the NORUT and/or NOIS.

NORUT

- Article 11[37]
- Article 12, paragraph 2[40]
- Article 13[42]
- Article 22h, paragraph 3[45]

NOIS

- Article 2, paragraph 1, 2[38], and 5[39]
- Article 3[41]
- Article 5, paragraph 1 through 4[43], and 6[44]
- Article 6[46]
- Article 7[47]
- Article 8[48]
- Article 11, paragraph 3[49]

[37] Obligation to report unusual transactions
[38] Obligation to identify the client before rendering any service
[39] Obligation to identify the client before rendering any service
[40] Obligation to provide additional information to the Reporting Center
[41] Obligation to establish the identification of the client
[42] Indication how to report unusual transactions
[43] Obligation to identify the representative
[44] Dispensation or exemption of the Minister under certain conditions
[45] Process of reporting of unusual transaction and additional information
[46] Obligation to document the data received
[47] Obligation of record keeping
[48] Prohibition to render services without identification
[49] Process of the identification of clients, reporting of unusual transaction and additional information

III.1 Penalties related to the NORUT and the NOIS

The violation of the obligations imposed by or pursuant to the following articles is subject to a maximum penalty of NA*f.* 500,000.
Based on abovementioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum penalty of NA*f.* 500,000. A list of these requirements is included in Appendix I to this Policy Rule. It concerns all the provisions that the (financial) institutions or individuals "**mus**t" comply with.

The Central Bank will indicate in the Decree[50] to impose a penalty the term in which the violator can execute a mandate without a penalty being forfeited.
The amount due can be collected by way of a writ of execution, increased by the costs falling on the collection. The writ of execution shall be served on the violator by means of a bailiff's notification and will produce an entitlement to enforcement[51].

III.2 Administrative fines related to the NORUT and the NOIS

The violation of the obligations imposed by or pursuant to the following articles is subject to a maximum administrative fine of NA*f.* 1,000[52].

NORUT

- Article 11
- Article 12, paragraph 2
- Article 13
- Article 20, paragraph 2
- Article 22h, paragraph 3

NOIS

- Article 2, paragraph 1, 2, and 5
- Article 3
- Article 5, paragraph 1 through 4, and 6
- Article 6
- Article 7
- Article 8
- Article 11, paragraph 3

Based on the abovementioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum administrative fine of NA*f.* 1,000. A list of these requirements is included in Appendix I to the Policy Rule on the violations of the NORUT and NOIS legislations and the AML/CFT provisions and guidelines of the Central Bank. It concerns all the provisions that the (financial) institutions or individuals "**mus**t" comply with.

Before proceeding to imposing a penalty, the Central Bank shall inform the (financial) institution or individual in writing of the intention to impose a penalty, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term[53].

[50] Decree:"Beschikking" in Dutch
[51] Article 22a, paragraph 3 through 5, NORUT and article 9, paragraph 3 through 5, NOIS
[52] See article 3, paragraph 1 of the ND PFRUT and article 3, paragraph 1 of the NP PFSP
[53] Article 22b, paragraph 3, ND NORUT and article 9a, paragraph 3, ND PFSP

III.3 Referral for criminal investigation in accordance with the NORUT/NOIS

The Central Bank will refer an offence for criminal investigation or prosecution to the law enforcement in circumstances where the offender emphatically refuses to comply with the compulsory requirements set out in the NORUT and/or NOIS.

In case of violation of or acting contrary to the provisions in the relevant articles mentioned in article 23 of the NORUT, or violation of regulations set by or pursuant to the relevant articles mentioned in article 10 of the NOIS, and the compulsory requirements in the Provisions and Guidelines the Central Bank may immediately refer the violation to the Public Prosecutor for further (criminal) investigation and prosecution. An example of a case where the Central Bank may immediately refer the violation to the Public Prosecutor for further (criminal) investigation and prosecution is that the Central Bank, during an on-site examination, takes notice of serious or grave violation of the NORUT, NOIS or the Provisions and Guidelines.

Furthermore, if the supervised (financial) institution or individual does not comply with its/his obligations, even after an increased penalty or administrative fine, the Central Bank can refer the violation for further investigation to the Public Prosecutor, by providing them with the relative documents[54].

[54] Article 4, paragraph 3, of the ND PFRUT and ND PFSP, respectively

Appendix 1: **Glossary/Definitions**

In this document the following abbreviations and definitions are used:

Board of Directors
The governing body of an institution, elected to oversee and supervise the operation and activities of the institution. The Board of Directors is ultimately responsible for the conduct of the institution's affairs, and controls its direction and, hence its overall policy.

Caribbean Financial Action Task Force (CFATF)
The CFATF is an organization of 29 states of the Caribbean basin, which have agreed to implement common countermeasures to address the problem of criminal money laundering. CFATF was established as a result of meetings convened in Aruba in May 1990 and in Jamaica in November 1992. The CFATF maintains a website at: http://www.cfatf.org/

Certify means to declare formally that a certain stated fact is true.

Client or customer
In general sense, a client or customer is defined in article 1, sub c of the NOIS, as anyone to whom a financial service, as defined in article 1, sub b of the aforementioned ordinance is rendered. More specifically, a client or customer of a company (trust) service provider is defined as follows:

Client of Company (trust) service provider: the client of a company (trust) service provider is in accordance with the NOST an international company. Ex article 1 paragraph d of the NOST, an international company is defined as a legal person which has its registered office or its actual place of business in Curaçao or Sint Maarten and which has been granted dispensation from the provisions of articles 9 - 15 of the National Ordinance on Foreign Exchange Transactions.

Company (trust) service provider
A company (trust) service provider is a person authorized to provide trust services pursuant to article 2 of the NOST. The trust services regulated by the NOST are defined in article 1 paragraph, 1 of the NOST. According to the stipulations of the NOST, a company (trust) service provider can be a natural person, a partnership or a legal entity.

Financial Action Task Force on Money Laundering (FATF)
The FATF is an inter-governmental body established in 1989, and whose purpose is to develop and promote policies to combat money laundering and terrorist financing. It has 34 member countries and two regional organizations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drugs Control and Crime Prevention and the CFATF. The FATF maintains a website at: http://www.fatf-gafi.org/

Felony refers to a serious offence committed for which the lawbreaker will be tried, judged and sentenced by a court in Curaçao or Sint Maarten.

High-risk and non-cooperative jurisdictions are jurisdictions that have detrimental rules and practices in place which constitute weaknesses and impede international co-operation in the fight against money laundering and terrorism financing.

Identify means to establish the identity of someone.

Know Your Customer (KYC)
The objective of KYC policies and procedures of investment institutions or administrators is for them to know the client with whom they are dealing. Sound KYC policies and procedures are critical in protecting the safety and soundness of the institutions and the financial system.

Misdemeanour is a minor crime which is punishable.

NOIS
The National Ordinance on the Identification when Rendering Services includes provisions on the identification of clients when rendering services.

Nominee shareholder service
A shareholder service account set up by a person (adviser) for the purpose of holding and or administrating assets (funds) on behalf of other persons (their client).

Office of Foreign Assets Control (OFAC)
Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

Politically exposed persons (PEPs)
As defined in *Customer due diligence for banks* (Basel publication 85- October 2001), politically exposed persons (PEPs) are individuals who are or have been entrusted with promoting public functions, including heads of states or of governments, senior politicians, senior government, judicial or military officials, senior executives or publicly owned corporations and important political party officials.

Qualifying Interest
A qualifying interest is a direct or indirect holding equal to or exceeding 25% of the nominal capital of the legal entity.

Senior Management
Comprises the individuals entrusted with the daily management of the operations to achieve the institution's objectives.

Source of funds refers to the activity that generated the funds for a client to be deposited into an account. This may include e.g. salary bonuses, earned income, interest and dividend payment.

Source of wealth refers to the activity that generates or which have generated an individual's net financial position.

Third party means an independent separate legal entity or person.

Trust
A trust is a legal arrangement created *inter vivos* or on death by a settler or grantor, whereby assets are placed under the control of a person, known as the trustee, for the benefit of

another person(private trust), known as the beneficiary, or for a specified purpose (public trust). The following types of trusts are broadly identified:

- **Bare trust / Fixed trust**: In a Bare/Fixed trust property is vested in the trustee by the settler, for the benefit of the beneficiary. There are no complicated rules as to how the trustee may decide who benefits from the trust or indeed what the trust property actually is. The bare trust can also be described as a fixed trust because the beneficiaries' interests are clearly defined.
- **Discretionary trust**: In a Discretionary trust, trustees have the power to distribute the property as they think fit in accordance with the rules set out in the Trust Deed.

Verify means to confirm; to establish the truth, accuracy or reality of something.

The Unusual Transaction Reporting Center (MOT/FIU)
Pursuant to article 11 of the National Ordinance on the reporting of Unusual Transactions, any (legal) person who provides a financial service is obliged to inform the MOT "Meldpunt Ongebruikelijke Transacties" of an unusual transaction which is contemplated or has taken place.

(Ultimate) beneficial ownership
Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

Appendix 2: The Source of Funds Declaration Form

To: (name of ultimate beneficial owner of the international company)

Time: _____

Date: _____

1) I, _____ understand that I am making this declaration for my own protection as well as for the protection of the company (trust) service provider that provides trust services to the international company I (co-)own.

2) I declare that the funds totaling _____, which have been used to purchase interest in _____ (name of international company) represent funds obtained by the undersigned from the following source(s):

_____

_____

_____

_____

3) The undersigned is aware that the information contained in this Source of Funds Declaration Form may be disclosed to those institutions which are legally entitled to the information contained here.[55]

_____
Ultimate Beneficial Owner's name

_____
Ultimate Beneficial Owner's address

_____
Ultimate Beneficial Owner's Signature

[55] This provision is recommended in a pursuit of transparency towards the customer. However, company (trust) service provider may consider excluding this clause from the Source of Funds Declaration Form when deemed necessary.

Appendix 3: Indicators for Company (trust) service providers

Indicators services, as referred to in article 1, section a., under 14º of the NORUT, (company (trust) service providers)

I. REPORTING MANDATORY (objective indicators):

A. Transactions that are reported to the police or the judicial authorities:

Transactions that are reported in connection with money laundering or the financing of terrorism to the police or the judicial authorities must also be reported to the Reporting Office.

B. Cash transactions:

All cash transactions of NA*f*. 10,000.00 and higher or the equivalent thereof in foreign currency in which case the provider of management services is directly or indirectly involved.

II. REPORTING MANDATORY, IF THE PERSON WHO IS OBLIGED TO REPORT CONSIDERS THAT THE FOLLOWING SITUATIONS ARE APPLICABLE (subjective indicators):

A. Probable money laundering transactions or the financing of terrorism:

Transactions in which there is reason to assume that they could be related to money laundering or to the financing of terrorist activities or other criminal activities.

B. Transactions in which checks, traveler's checks or similar instruments of payment are involved:

Transactions by a client of NA*f*. 100,000.00 and higher, including the purchasing or cashing of checks, traveler's checks or similar instruments of payment (hereafter 'checks') which comply with two or more of the following indicators:

a. no explainable objective or no visible relation with (business) operations;
b. transaction atypical of client;
c. incoming flow consists of many small amounts and outgoing check(s) with large amounts, or vice versa, which flow does not fit within the profile of the client;
d. endorsed in client's name;
e. conspicuous number of accounts;
f. conspicuous turnover or conspicuous changes in the account balance which cannot be reasonably explained, considering the activities of the client;
g. unusual condition offer.

C. Giro-based transactions:

Transactions of NA*f*. 1,000,000.00 and higher that comply with two or more of the following indicators:

a) identification problems;
b) conspicuous number of accounts;
c) no explainable objective or no visible relation with the profile of the client;

d) transaction atypical of client;
e) unusual condition offer;
f) conspicuous turnover or conspicuous changes in the account balance which cannot be reasonably explained, considering the activities of the client;
g) incoming flow consists of many small amounts and outgoing flow of large amounts, or vice versa, which flow does not fit within the activities of the client;
h) in the transaction, a security deposit or third-party account is used;
i) incoming transaction without any statement of the principal or under a code name;
j) the basis of the transaction is not documented or the transaction lacks a valid legal title;
k) the transaction runs via the client's bank account, but is at the expense and risk of a third party ("fiduciary" use of the account).

D. Dodging the marginal amount:

Preference of the client for transactions under the marginal order amount in which case there is reason to assume that he wants to avoid reporting in doing so.

Appendix 4: Examples of unusual transactions related to the provision of trust services to international companies

Company (trust) service providers must be extra vigilant for the unusual transactions mentioned below. A client that displays the behavior mentioned below is not necessarily involved in money laundering or terrorist financing activities. However, the examples must serve as general indicators which must prompt the company (trust) service provider to closer monitor the client's behavior under the mentioned circumstances. Furthermore, the examples must promote awareness and stimulate the deterrence of money laundering and terrorist financing within the company (trust) service provider.

a) Large or unusual settlements of transactions in cash or bearer forms, such as travelers' cheques.

b) Individual or corporate clients located in poorly regulated or uncooperative jurisdictions with undisclosed ownership.

c) Client introduced by an overseas bank, an affiliate or other client both of which are based in countries where production of drugs or drug trafficking may be prevalent.

d) Any transaction in which the counterparty to the transaction is unknown or where the nature, size or frequency appears unusual.

e) A client whose source of funds is not clear and who refuses to provide satisfactory identification documents and explanations.

f) Accounts which are said to be "trust" or fiduciary accounts for which there is no trust deed or supplemental documentation.

g) A client moving property through different globally incorporated foreign companies.

h) A client using legal structures to issue loans to themselves.

i) A client using legal structures to buy real estate at a value below the economic value.

j) Faking certain performances to justify higher turnover.

k) The purchase of winning lottery tickets by the international company.

l) Turnover of the international company appears to be unrealistically high (considering industry international company operates in).

m) Frequent and/or unexplained change of beneficiary.

n) Beneficiary does not have any apparent connection to the settler.

o) Client has unexplained urgency to carry out a certain transaction.

p) Unexplained requests for anonymity.

q) Transaction is unnecessarily complicated and client can not explain setup (and reason for complicated setup) of the transaction (splitting or concentrating amounts).

r) A client that makes multiple transactions just below legal threshold ("smurfing").

s) Sudden activation of dormant company for unexplained reasons.

In addition to the above-mentioned examples, company (trust) service providers must be particularly alert for frequent and excessive switching of company (trust) service provider by the international company, as this may be an indication that the international company is laundering money.