CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Credit Institutions

November 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 therefore fully reflect 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 "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 Credit Institutions 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 Banking and Credit Institutions 1994 (N.G. 1994, no. 4), article 21, paragraph 2, section e.

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 the 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 penalties and administrative fines for reporters of unusual transactions (N.G. 2010 no. 70));
(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. 71);
(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 operation of March 15, 2010, for the execution of the NOIS (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);
(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

[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.

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 are 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; and
- 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 will be 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

During the three stages of money laundering, numerous transactions may be 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 terrorism.

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

I.3 Risk-based Approach

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), credit institutions are allowed to apply a Risk-Based Approach ("RBA"). By adopting a RBA, it is possible for the credit institutions 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 must be subjected 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 while low risk clients may be subject to simplified/reduced customer due diligence as outlined in section II.2.A.

Credit institutions applying the RBA must document their policies, procedures and controls relative to their applied RBA. Furthermore, they must, on an on-going, basis monitor the effective operation of the policies, procedures and controls concerning their RBA and, when needed, make the necessary amendments to these policies, procedures and controls.

[4] The full document can be consulted at **http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf**.

[5] The list can be consulted at http://www.un.org/sc/committees/1267/consolist.shtml..

I.4 Sanctions

Credit institutions are required to comply with the compulsory requirements set out in the NORUT and/or NOIS legislations and the provisions and guidelines issued under these laws. Breaches of the obligations set out under aforesaid regulations are subject to sanctions by the Central Bank.

During its on-site examinations, the Central Bank will assess the supervised financial institutions' compliance with these Provisions and Guidelines and all other Anti Money Laundering (AML) and Combating 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 CREDIT INSTITUTIONS

This chapter addresses the relevancy of the detection and deterrence of money laundering and terrorist financing for credit institutions, followed by a description of some policies and procedures for credit institutions to detect and deter money laundering and terrorist financing. The chapter concludes with a listing of the information and documentation of the relevant policies and procedures that those institutions must provide to the Central Bank.

II.1 The relevancy of the detection and deterrence of money laundering and terrorist financing for credit institutions

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 obvious in the traditional banking sector than in other (financial) sectors.

However, non-bank financial institutions, such as insurance companies and investment institutions have become increasingly vulnerable to money launderers and terrorists who seek, to launder their funds derived from criminal activities and finance their terrorist activities respectively. Still, credit institutions, which include banks, remain prone to be used by criminals to launder their illicitly obtained funds.

The integrity of the financial sector of Curaçao and Sint Maarten, which includes credit institutions, heavily depends on the perception that it functions within a framework of high legal, professional, and ethical standards. A reputation for integrity is a valuable asset of a credit institution. However, public confidence in credit institutions and, hence their stability can be undermined by adverse publicity as a result of their unwitting use by criminals for money laundering and terrorist financing purposes.

If credit institutions do not establish and adhere to proper policies and procedures, they may unwittingly be used by criminals and become involved in money laundering and terrorist financing activities which will negatively affect their reputation and operations.

It is therefore imperative that all credit institutions continue to be vigilant in detecting and deterring criminals from engaging in any form of money laundering and terrorist financing.

In this context, the Central Bank is issuing these Provisions and Guidelines to further promote and maintain the financial stability, soundness, and reputation of credit institutions and the financial sector of Curaçao and Sint Maarten. These Provisions and Guidelines serve as a tool for further implementation of the NOIS and the NORUT legislations.

All credit institutions 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 topic is discussed further in the next sections.

II.2 Policy statement

Each credit institution's Board of Supervisory Directors[6] and senior management[7] must issue a policy statement that clearly expresses the credit institution's commitment to combat the abuse of its facilities, financial products, and services for money laundering and terrorist financing purposes.

This policy statement is a "Best Practice" statement of a credit institution's Board of Supervisory Directors and Senior Management which outlines the institution's policies and procedures and must be communicated to its employees.

The policy statement must state the institution'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.

The policy statement must cover also the following items.

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

- The appointment of one or more compliance officer(s) at management level responsible for ensuring day-to-day compliance with these procedures. The officer(s) must have the authority to investigate unusual transactions extensively;

- A system of independent testing of the policies and procedures by the credit institution's internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness; and

- The preparation of an appropriate training plan for and training of personnel to increase employees' awareness and knowledge in the area of money laundering and terrorist financing prevention and detection.

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

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

II.2.A. Detection and deterrence of money laundering

Credit institutions have the obligation to identify their (prospective) personal or corporate clients[8] before rendering them financial services. Management must maintain an information program to inform those clients of the objectives of the relevant anti-money laundering legislation and inherent requirements for credit institutions. Also, internal procedures must clearly indicate for which financial services clients or their representatives must be identified and which identification documents are acceptable.

The legally allowed client identification documents and the nature of the transaction are prescribed in the NOIS legislation[9]. The required information must be updated regularly and adequately documented. Credit institutions 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 accounts or business relationships. An important objective for credit institutions is to be able to retrieve this information, without any undue delay. Hence, the Central Bank requires the credit institution to implement a checklist containing identification and/or transaction information and to maintain a centralized record keeping system to retain copies.

Foreign branches and subsidiaries

Credit institutions 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. Credit institutions 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.
Credit institutions 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)

Credit institutions must develop clear customer acceptance policies and procedures, including a description of the categories of customer likely to pose a higher than average risk to the credit institution. The policy must ensure that transactions will not be conducted, business is not commenced and that accounts are not opened with (prospective) customers who fail to provide satisfactory evidence of their identity.

Credit institutions 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 service.

The source of funds declaration form must be used in the opening of accounts and/or the transferring of funds, and when accepting funds from occasional customers and non-correspondent banks.

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

Where it is reasonable to believe that a requested transaction is connected with criminal activity or if the client refuses to sign a "source of funds declaration", and there is no credible explanation to dispel concerns, the credit institution must refuse to execute the requested transaction to ensure that the minimum standards are met, but still report it to the Unusual Transactions Reporting Center (FIU/MOT).

The efforts to "know your customer" must continue even after the client has been identified.
Ongoing due diligence must include also the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, his or her business and risk profile, and where necessary, the source of funds. If doubts arise relating to the identity of the client after the client has been accepted and accounts have been opened, 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 Financial Intelligence Unit (FIU). The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties (MOT).

Examples of when this action may be appropriate are when:

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

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

Credit institutions are required to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

Moreover, credit institutions must apply CDD requirements to existing customers on the basis of materiality and risk and must conduct due diligence on such existing relationships at appropriate times.

For identification purposes, the credit institution must distinguish the following customers and their transactions:

(a) transactions (including the opening of an account) with (prospective) account holders based on a permanent relationship;
(b) transactions with non-account holders or occasional customers;
(c) non-account holders' requests for provision of safekeeping custody services; and
(d) occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII.

(a) Transactions with (prospective) account holders

Before rendering a (financial) service the credit institution has to identify its customers.

Identification of resident and non-resident personal customers

Pursuant to article 3 of the NOIS legislation, the identity of **resident** and **non-resident** personal customers must be established through one of the following valid documents:

- a driver's license;
- an identity card;
- a travel-document or passport; or
- any other document designated by the Minister of Finance.

Resident customers

In addition, the identity of a **resident** individual customer must be verified when a business relationship is established with the customer. The identity of the customer also must be verified when the credit institution has doubts about the veracity or adequacy of the identification data obtained from existing customers. Examples 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; and
- requesting a copy of utility bill.

Non-Resident customers

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

- existing banking relationships of the prospective customer;
- international or home country telephone directory;
- personal reference by a known account holder;
- embassy or consulate in home country of address provided by the prospective client;
- comparison of signature if a personal account check is tendered to open the account; and
- if provided, cross reference of address printed on personal check to permanent address provided by client on standard application form.

Credit institutions must pay special attention to non-resident customers and understand the reasons why the customer has chosen to open an account in Curaçao or Sint Maarten.

Non face-to-face clients/certification

At times a credit institution may establish a business relationship with a non-resident client or conduct transactions on behalf of a non-resident client with which no face -to- face contact has been established. Examples of non-face-to-face operations include business relationships concluded over the internet or by other means, such as through the post; services and transactions over the internet including trading in securities by retail investors over the internet or other interactive computer services; use of ATM machines; telephone banking; transmission of instructions or applications via facsimile or similar means, and making payments and receiving cash withdrawals as part of electronic point-of-sale transactions using prepaid or re-loadable or account-linked value cards.

For **non-resident** clients a copy of the identification document is sufficient, under the condition that the relevant document is accompanied by a certified extract of the civil registry of births, marriages and deaths of the place of residence of the party or that the document is certified by a notary public, embassy or consulate. The name, address and telephone number of the notary public, embassy or consulate including the name and contact details of the officer who signed for certification must be clearly indicated. Furthermore, the identification document may be sent via electronic mail under the condition that a certified copy is received within 14 days of the receipt of the electronic version by the credit institution. The submitted copy of the identification document, including the photograph, must be clearly legible.

It should be noted that if face-to-face contact has been established by the credit institution with a (prospective) non-resident client, then the aforementioned certification requirement is not necessary.

Credit institutions are required to 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.

Measures for managing the risks must include specific and effective CDD procedures that apply to non-face-to-face customers. Examples of such procedures include the certification of documents presented, the request of additional documents to complement those required for face-to-face customers; independent contact with the customer, third party introduction and requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Identification of Politically Exposed Persons

Credit institutions 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 PEP's 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. Credit institutions 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, financial institutions must obtain senior management approval to continue the business relationship. Where the financial institution is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship. Credit Institutions must implement appropriate risk management systems to determine whether a potential customer, customer or beneficial owner is a politically exposed person (PEP).

Identification of corporate customers

Corporate accounts are one of the more likely vehicles to be used for money laundering purposes. Therefore, it is important to identify the nature of the business, account signatories, and the (ultimate) beneficial owner(s)[10]. Credit institutions also must obtain personal information on the managing and/or supervisory directors. Copies of the identification documents of all account signatories, including the directors without signing authority on the corporate client's accounts, must be kept on file. The procedures for the identification of personal customers must be applied for the mentioned account signatures' director(s) and all (ultimate) beneficial owners (UBO) holding a qualifying interest in the company. Credit institutions must ascertain the identity of corporate customers based on reliable identification documents, with preference for originals and official documents attesting to the legal existence, and structure of a company or legal entity. The identity, existence and nature of the

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

corporate customer must be established 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. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.

Management may require additional information from these companies, such as:

- shareholders' register;
- certificate of incorporation;
- articles of association;
- a list to include full names of all directors (including supervisory directors, if applicable), 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 company, together with a designation of the capacity in which they sign; and
- business plan/cash flow statements.

Identification in case of representation
Pursuant to article 5 of the NOIS legislation, a credit institution is bound to establish the identity of the individual appearing before it on behalf of a customer or on behalf of a representative of a customer, before it proceeds to render the financial service. If the customer acts for a third party or that third party also acts for another third party, the credit institution must be bound to also establish the identity of each third party. Thus, when customers are represented by a company (trust) service provider and this company (trust) service provider opens an account with a credit institution on behalf of its customer, that customer must be duly identified through one or more of the ways indicated above.

Identification of clients with nominee accounts[11]
All credit institutions that provide nominee services 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 mentioned previously.

Beneficial owner declaration
A credit institution must have each corporate account holder complete and sign for each account a beneficial owner declaration form as presented in Appendix 2 for all accounts.

Anonymous accounts or accounts in fictitious names
Anonymous accounts or accounts in fictitious names are **prohibited**. Credit institutions are required to maintain numbered accounts in such a way that full compliance can be achieved with the FATF Recommendations. For example, the credit institution 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.

(b) Transactions with non-account holders or occasional customers

Transactions undertaken by a credit institution for non-account holders will be classified as an incidental service. These services involve mainly cash or transfer transactions. Management's responsibility is to make the staff aware of the arrangements or procedures in place. Identification will be necessary for all transactions and for the amounts above the limits established by the Minister

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

of Finance, as referred to in the 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).

(c) Non account holders' requests for provision of safekeeping custody services

Particular precaution needs to be taken in relation to requests to hold boxes, parcels, and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification procedures set out under section II.2.A must be followed. Where the credit institution is unable to comply with the customer due diligence (CDD) requirements set out under section II.2.A, it must consider making an unusual transaction report to the FIU/MOT.

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

Credit institutions 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.

The following steps must be taken by credit institutions when relying on intermediaries or other third parties to perform aforementioned elements of the CDD process[12]:

- immediately obtain from the third party the necessary information concerning the elements of the CDD process;
- 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; and
- 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, credit intuitions must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT regulated and supervised. A jurisdiction is adequately regulated and supervised when its) Mutual Evaluation Report[13] discloses less than 10 "Non Compliant or Partially Compliant" ratings regarding the 16 "key and core[14]" FATF Recommendations.

If credit institutions 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

[12] 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. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers.

[13] Countries could refer to reports, assessments or reviews concerning AML/CFT that are published by the FATF, CFATF or other FATF-style regional bodies (FSRBs), the IMF or World Bank.

[14] The core Recommendations are: Recommendations 1, 5, 10 and 13 Special Recommendations II and IV
The key Recommendations are: Recommendations 3, 4, 23, 26, 35, 36 and 40 *Special Recommendations I, III and V*

outsourced to an intermediary or third party. 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. If the credit institution relies on intermediaries or other third parties for the complete CDD process (in this case the CDD process has been outsourced) then a written service level agreement is required and must be readily available for the Central Bank when conducting on-site visits.

It should be noted that even though the credit institution may rely on intermediaries or other third parties for part of the CDD process or that the process may be outsourced, the ultimate responsibility for customer identification and verification remains with the credit institution relying on the third party.

Timing of verification

Credit institutions may complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, provided that:

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

If verification is completed after the establishment of the business relationship the reasons for this must be documented.

Risk-based Approach

Risk classification

The credit institution must develop risk profiles for all its customers to determine which categories of customers expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a customer, 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. Credit institutions must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, or transaction.

The credit institutions must at least consider the following risk categories while developing and updating the risk profile of a customer: (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 credit institution to assess the type of customer and the nature and scope of the business activities of the customer. The types of customers 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;
    - Customers engaging in business activities regarded as sensitive, such as pornography, arms trading and the provision of military security services;
    - Customers whose 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;
- Customers where there is no commercial rationale for a customer making use of the services offered by the credit institution 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;
- Customer documentation standards change substantially; and
- Determination of lack of or insufficient information about an existing customer.

(ii) Products/services risk: An effective risk assessment must also include determining the potential risk presented by products and services offered by the credit institution. A key element is the establishment of the existence of a legitimate business, economic, tax or legal reason for the customer to make use of the products/services offered by the credit institution.

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 improperly beneficial ownership from competent authorities;
- Transactions or services with no apparent legitimate business, economic, tax, or legal reasons;
- The offer by customers to pay extraordinary fees for services which would not ordinarily warrant such a premium;
- Incoming wire transfers that are not accompanied by complete originator information;
- Back-to-back loans.

(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 a having designated terrorist organizations operating within them.

(iv) Delivery Channels Risk: This particular risk category deals with the manner in which the credit institution establishes and delivers products and services to its customers. While assessing the vulnerabilities posed by the distribution channels of its products and services, the credit institution must at least consider the following factors:

- The use of third parties introducers and intermediaries to conduct (some of the) elements of the customer 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 customer remotely (non-face to face);
- The control of the relationship or transactions remotely (e.g. straight-through processing of transactions); and
- Pooled relationships with intermediaries, which due to the anonymity provided by the co-mingling of assets or funds belonging to several customers 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 credit institution to another. The credit institution must make its own determination as to the assignment of the risk weights. The result of the risk assessment of a particular customer, 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.

(a) Enhanced CDD for high risk categories of customers

Credit institutions must conduct enhanced due diligence in all of the high risk cases/circumstances mentioned above and in any other cases/circumstances identified by the institution, according to its risk assessment framework. The institution's decision to enter into or to continue business relationships with such customers must be taken at its senior management level. Credit institutions must not accept or maintain a business relationship if they know or must assume that the funds are derived from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

Credit institutions 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, credit institutions must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, credit institutions are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.

(b) 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" FATF Recommendations in Mutual Evaluation Reports can be considered high risk jurisdictions when they have not shown a high level of commitment to remedy their deficiencies in a reasonable timeframe. The FATF and some FSRBs issue statements on these countries.

Credit institutions are required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations including high-risk and non-cooperative jurisdictions. The same holds for the customers; banks 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 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, (financial) institutions 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.

(c) 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, circumstances may arise 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 credit institution is allowed to apply simplified or reduced CDD measures when establishing the identity and verifying the identity of the customer and the beneficial owner.

Examples of customers (transaction or products) where the risk may be lower include:

(a) financial institutions subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and supervised for compliance with those requirements;
(b) public companies subject to regulatory disclosure requirements, i.e., companies that are listed on a stock exchange or comparable situations; and
(c) government administrators or enterprises.

Where credit institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that are compliant with and have effectively implemented the FATF Recommendations. Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

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

Credit institutions are not only required to adhere to the stipulations of the identification regulations, but are also required to detect and report either proposed or completed unusual transactions. Therefore, it is important for every institution to have in place adequate procedures for its personnel.

Mentioned procedures must cover:

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

(a) Recognition of unusual transactions

An unusual transaction will often be a transaction inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the customer's business. In this context, employees of credit institutions must not only focus on financial statements of the client, but also on aspects, such as the client's local or foreign relationships and the financial profile of the client, and the client's engagement in other business activities.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which credit institutions must assess if a customer's transaction qualifies as an unusual transaction. Those indicators are listed in Appendix 3. Institutions with an advanced computer information system may develop special programs to select objectively defined unusual transactions.
However, management must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions.

In order to implement the FATF recommendation 11, credit institutions must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Credit institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. Furthermore, credit institutions are required to keep such findings available for competent authorities and auditors for at least five years.

Credit institutions are required to aggregate and monitor balances and activities in customer accounts and apply consistent CDD measures on a fully consolidated worldwide basis, regardless of the type of accounts, such as on- or off balance sheet, and assets under management.

<u>Wire transfer</u>
Internationally, wire transfers are increasingly being used to launder funds from illegal sources and for illegal activities or to finance terrorism. Credit institutions must be extremely vigilant before accepting funds from non-account holders and non-correspondent banks for transfer to equally unknown parties. If such funds are accepted, suitable identification of the non-account holders and knowledge of the source of funds must be required through a source of funds declaration form as presented in Appendix 4.

Based on FATF Special Recommendation (SR) VII,[15] credit institutions must include accurate and meaningful originator information (at least the name, address, and account number) regarding funds transfers within or from Curaçao and Sint Maarten, and on related messages sent. The information must remain with the transfer or related message through the payment chain.

If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds. Credit institutions 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://ww.fatf-gafi.org**. Also, further scrutiny is required and reporting to the Unusual Transactions Reporting Center (FIU/MOT) must be considered.

Correspondent banking

Credit institutions are not permitted to enter into, or continue, correspondent banking relationships with shell banks. Credit institutions are required to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

Particular attention must be paid to correspondent services (such as correspondent banking services) provided to a financial institution licensed in a jurisdiction where the credit institution has no physical presence or is unaffiliated with a regulated bank, or where anti-money laundering and anti-terrorist financing measures and practices are known to be absent and/or inadequate.

In addition, the credit institutions' policies and procedures regarding the opening of correspondent accounts must at least require the following actions:

- fully understand and document the nature of the respondent bank's management and business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- ascertain that the respondent bank has effective customer acceptance and know-your-customer (KYC)[16] policies and is effectively supervised; and identify and monitor the use of correspondent accounts that may be used as payable-through accounts credit institutions must obtain approval from senior management before establishing new correspondent relationships; and
- assess the respondent institution's AML/CFT controls, and ascertain whether or not they are adequate and effective.

Credit institutions establishing correspondent relationships must communicate their documented anti-money laundering and anti-terrorist financing responsibilities to have a clear understanding as to which institution will perform the required measures.

Where a correspondent relationship involves the maintenance of "payable-through accounts", credit institutions must be satisfied that:

(a) their customer (the respondent financial institution) has performed all the normal CDD obligations on those of its customers that have direct access to the accounts of the correspondent financial institution; and
(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

[15] In October 2001, the FATF agreed on eight Special Recommendations on Terrorist Financing. Special recommendation VII pertains to wire transfers.
[16] See Appendix 1 for the definition or explanation or summary.

Misuse of technological development
For electronic services, credit institutions could refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003. Credit institutions 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.

(b) The documentation of unusual transactions

To guard against money laundering and terrorist financing, credit institutions must set forth their findings relative to suspicious/unusual funds or transactions in writing. Such findings must be kept for at least five years and made available for competent authorities and auditors.

(c) Reporting of unusual transactions

Credit institutions must have clear procedures which are communicated to their personnel for the reporting of unusual transactions.

There may be circumstances where a credit institution declines to open an account for a potential new customer or refuses to deal with a request made by a non-account holder because of serious doubts about the individual's bona fides and potential criminal activity. Credit institutions must base such decisions on normal commercial criteria and internal policy. According to article 11 of the NORUT, anyone who renders financial services by virtue of his profession in the ordinary course of his business, must be bound to report any unusual (intended) transaction thereby made or proposed to the FIU/MOT without delay.

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 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) must be referred to the designated officers in the format(s) approved by management. However, management may choose to require that some categories of unusual transactions be drawn to their attention. Whenever available, additional documents, such as copies of the identification documents, credit/debit slips, checks, and account ledger records also must be submitted as supplements. The designated officers must keep an adequate filing system of these records.

If internally reported transactions are not reported to the FIU/MOT by the institution, the reasons must be adequately documented and signed off by the compliance officer and/or by management.

External reporting
The designated officers must prepare a report of all unusual transactions for external reporting purposes. The report must be submitted to senior management for its review for compliance with existing regulations. Copies of these reports must be kept by the reporting institution.

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 institution.

Taking into account the above-mentioned procedure for external reporting, the compliance officer(s) should be able to act independently.
Management must establish a policy to ensure that:

- the credit institution and its supervisory directors, senior management, and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the institution's compliance staff on customers; and
- the institution and its supervisory directors, senior management, and employees 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 an exempt list for the reporting of unusual transactions is permitted. However, the established laws and regulations in Curaçao and Sint Maarten do not allow any exemptions concerning the reporting obligation of credit institutions.

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

Each credit institution must formally designate one or more senior officer(s) at management level responsible for the detection and deterrence of money laundering and terrorist financing. The compliance officer(s) must be able to act independently. The AML/CFT compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

The compliance officer(s) must be assigned at least the following responsibilities:

- to verify the adherence to the local laws and regulations governing the detection and deterrence of money laundering and terrorist financing;
- to organize training sessions for the staff on various compliance-related issues;
- to review compliance with the institution's policy and procedures;
- 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 of unusual or suspicious transactions;
- to remain informed of the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- to periodically report information on the institution's efforts 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 each designated officer entrusted with the AML/CFT matters. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.

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

Independent testing of the adequacy of the functioning of the credit institution's policies and procedures must be conducted at least annually by an adequately resourced internal audit department or by an outside independent party, such as the institution's external auditors.

These tests must include at least:

- an evaluation of the institution's anti money-laundering and counter terrorist financing manual(s);
- customers' file review;
- interviews with employees who handle transactions and with their supervisors;
- a 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
- an 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 Supervisory 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

Credit institutions 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 credit institution must establish and adhere to proper policies and procedures in screening its employees for criminal records.

Credit institutions 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 includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the institution's policies against money laundering and terrorist financing. Training must at least address the following topics:

(a) New employees

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer(s) must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They must be made aware of the existing internal policies, procedures, and external regulations concerning money laundering, terrorist financing, and the reporting requirements. They must receive an explanation of the vigilance policies and systems, including particular emphasis on customer identification, suspicious activity, and reporting requirements.

(b) Cashiers/foreign exchange operators/advisory staff

Staff members dealing directly with the public are the first point of contact with potential money launderers. Therefore, their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. These members must be aware of the organization's reporting system for such transactions. Training must be provided on the KYC principle, on how to detect unusual transactions or proposals, and on the procedures to follow after identifying such transactions.

(c) Personnel involved with account opening/new client

Staff members who are in a position to handle account opening, or to accept new clients, must receive the training set out under (b) above. In addition, the need to verify the identity of the customer must be understood, and training must be provided in the organization's account opening and customer verification procedures. These staff members must be aware that unusual transactions must be reported whether the funds are accepted or not. Staff members must also know what procedures to follow in this respect.

(d) Supervisors and Managers

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.

(e) Ongoing training

Refreshment training at regular intervals must be arranged to ensure that the staff remembers its responsibility and be kept informed of current and new developments regarding domestic and/or international money laundering and terrorist financing techniques, methods, and trends. The training must include a clear explanation of all aspects of laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification, due diligence, and unusual transactions reporting in Curaçao or Sint Maarten. This might be best achieved through a semi-annual review of the instructions for recognizing and reporting of unusual transactions.

For a credit institution to demonstrate compliance with the aforementioned guidelines with respect to staff training, it must at all times maintain records that include:

- details of the content of the training programs provided;
- the names of the staff members who have received the training;
- the date on which the training was provided;
- the results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- an ongoing training plan.

II.2.B Detection and deterrence of Terrorist Financing

Credit institutions must take necessary measures to prevent the unlawful use of entities identified as vulnerable, such as charitable or nonprofit organizations as conduits for criminal proceeds or terrorist financing.

Credit institutions must take into account the characteristics including types of transactions listed in the annex 1 to the FATF document entitled "Guidance for Financial Institutions in Detecting Terrorist Financing".[17] Those characteristics and transactions could be cause for additional scrutiny and could indicate funds involved in terrorist financing. In addition, credit institutions must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in:

- the list issued by the United Nations;[18]
- 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[19] to the FATF document" Guidance for Financial Institutions in Detecting Terrorist Financing"; and
- the listing[20] of the Office of Foreign Assets Control (OFAC)[21] or of other national authorities.

Supervised institutions must continuously compare the names in their client database with the names on the above-mentioned lists. If a supervised institution encounters a match, it must freeze the asset of the client, and report the occurrence to the FIU/MOT and the Central Bank immediately.

[17] The full document can be consulted at **http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.**
[18] The list can be consulted at **http://www.un.org/docs/sc/committees/1267/1267listeng-htm**.
[19] The full document can be consulted at **http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.**
[20] The list can be consulted at FINCEN's website at
http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html.
[21] See Appendix 1 for the definition or explanation or summary.

In addition, if a credit institution suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, it must report promptly its suspicion to the FIU/MOT. Reference is made to the Ministerial Decree N.G 2010, no. 27.

Moreover, credit institutions must be vigilant in the abuse of nonprofit organizations for terrorist financing. They must observe the FATF's Special Recommendation (SR) VIII[22] and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices[23].

II.3 Record-keeping

Credit institutions must ensure compliance with the record-keeping requirements in the relevant money laundering and terrorist financing legislation. Credit institutions must ensure that investigating authorities be able to identify a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing.

Where appropriate, credit institutions 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 longer periods then 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 took 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.

- Credit institutions 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, the records must be retained until it is confirmed by these parties that the case has been closed.

[22] Special recommendation VIII refers to measures with respect to vulnerable nonprofit organizations.
[23] 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 credit institutions must be prepared to provide information or documentation on their money laundering and terrorist financing policies and detection and deterrence procedures to the examiners of the Central Bank before or during an on-site examination and upon the Central Bank's request during the year. The credit institution 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 institution's overall money laundering and terrorist financing policies and procedures and her/his designated job description;
- records of reported unusual transactions;
- unusual transactions which required closer investigations;
- 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 customers' transactions data and files, other relevant information such as Swift daily-overview, nostro-account reconciliations, list of clients that make use of deposit boxes, and non-account holders transactions; and
- required copies of identification documents.

During on-site examinations, the Central Bank will assess the supervised financial institution's compliance with these provisions and guidelines and all other Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) legal obligations. In case of non-compliance, sanctions will be applied.

III OFFENCES AND SANCTIONS IN THE NORUT AND THE NOIS

A credit institution 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 a credit institution 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 a credit institution 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 penalty amount 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.

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.

NORUT

- Article 11[24]
- Article 12, paragraph 2[27]
- Article 13[29]
- Article 22h, paragraph 3[31]

NOIS

- Article 2, paragraph 1, 2[25], and 5[26]
- Article 3[28]
- Article 5, paragraph 1 through 4[30],
- Article 6[32]
- Article 7[33]
- Article 8[34]
- Article 11, paragraph 3[35]

Based on abovementioned article 22h, paragraph 3, juncto article 22a, NORUT and article 11, paragraph 3, juncto article 9, NOIS the compulsory requirements in the Provisions and Guidelines

[24] Obligation to report unusual transactions
[25] Obligation to identify the client before rendering any service
[26] Obligation to identify the client before rendering any service
[27] Obligation to provide additional information to the Reporting Center
[28] Obligation to establish the identification of the client
[29] Indication how to report unusual transactions
[30] Obligation to identify the representative
[31] Process of reporting of unusual transaction and additional information
[32] Obligation to document the data received
[33] Obligation of record-keeping
[34] Prohibition to render services without identification
[35] Process of identification of clients, reporting of unusual transaction and additional information

are also subject to a maximum penalty of NA*f.* 500,000. 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.

The Central Bank will indicate in the Decree[36] to impose a penalty the term in which the violator may 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 of 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[37].

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[38].

NORUT	*NOIS*
- Article 11	- Article 2, paragraph 1, 2, and 5
- Article 12, paragraph 2	- Article 3
- Article 13	- Article 5, paragraph 1 through 4
- Article 22h, paragraph 3	- Article 6
	- Article 7
	- Article 8
	- Article 11, paragraph 3

Based on the abovementioned article 22h, paragraph 3, juncto article 22b, NORUT and article 11, paragraph 3, juncto article 9a, 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 this Policy Rule. It concerns all the provisions that the (financial) institutions or individuals "**mus**t" comply with.

Before proceeding to imposing a fine, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a fine, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term[39].

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 in which 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 NORUT, or violation of regulations set by or pursuant to the relevant articles mentioned in article 10 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.

---

[36] Decree:"Beschikking" in Dutch

[37] Article 22a, paragraph 3 through 5, NORUT and article 9, paragraph 3 through 5, NOIS

[38] See article 3, paragraph 1 of the ND PFRUT and article 3, paragraph 1 of the NP PFSP

[39] Article 22b, paragraph 3, ND NORUT and article 9a, paragraph 3, ND PFSP

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 onsite-examination, takes notice of serious or grave violation of the NORUT, NOIS or the Provisions and Guidelines.

Furthermore, if a supervised (financial) institution or an individual does not comply with its or 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[40].

[40] 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.

Bearer securities
Securities instruments issued in bearer form. They comprise bearer bonds and bearer stock certificates. Contrary to registered securities, the ownership of the bearer security is not registered in a register maintained by the issuing entity. The bearer security is owned by the person who possesses it, and the transfer takes place by physically handing over this security.

Board of Supervisory Directors
The governing body of an institution, elected by the shareholders, to oversee and supervise the management of the institution's resources and activities. It 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, that 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
Pursuant to article 1, sub c of the NOIS, a client/customer is anyone to whom a financial service, as defined in article 1, sub b of the NOIS, is rendered.

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

Financial Action Task Force on Money Laundering (FATF)
The FATF is an intergovernmental body established in 1989, whose purpose is to develop and promote policies to combat money laundering and terrorist financing. The FATF 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 Drug Control and Crime Prevention and the CFATF. The FATF maintains a website at: **http://www.fatf-gafi.org/**

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.

Holding a qualifying interest
Holding a qualifying interest is understood to be both a direct and an indirect holding that is:
the *Ultimate Beneficial owner owning 25% or more of the nominal capital of the institution* (financial interest equal to or exceeding 25%), also *to exercise directly or indirectly the voting rights in the enterprise or institution equal to or exceeding 25%* (controlling interest equal to or exceeding 25%).

Identify means to establish the identity of someone.

Know Your Customer (KYC)
The objective of KYC policies and procedures for credit institutions is for them to know the customer 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 account
An account set up by a person (adviser) for the purpose of holding and or administering assets (funds) on behalf of other persons (his or her clients).

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 of publicly owned corporations, and important political party officials.

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. earned income, interest and dividend payment.

Third party means an independent separate legal entity or person.

Ultimate beneficial owner
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 or arrangements. Ultimate Beneficial owner owning 25% or more of the nominal capital of the institution (financial interest equal to or exceeding 25%), also to exercise directly or indirectly the voting rights in the enterprise or institution equal to or exceeding 25% (controlling interest equal to or exceeding 25%).

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.

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

Appendix 2: Ultimate Beneficial Owner Declaration Form
Notice:

This declaration aims at retaining the identity of the beneficial owner by virtue of the present regulations in Curaçao and Sint Maarten

Name of client _____

Client reference number _____

The undersigned hereby declares
(mark with a cross where applicable)

☐ as client of the credit institution (1)
(natural person)

☐ as representative of the client
(legal entity)

☐ that he/she is the beneficial owner of the assets to be deposited with or held by the bank

☐ that the following natural person(s) is/are the ultimate beneficial owner(s) of the assets to be deposited with or held by the credit institution (1)

Personal data:

Full name _____

Address _____

Date of birth _____ Place of birth _____

Nationality _____

Attached: copy of personal identity document ☐ passport ☐ id. Card

The undersigned confirms that all due diligence has been exercised in ascertaining the identity of the abovementioned listed beneficial owner(s) of above company. Additionally, the undersigned declares that he/she will inform the credit institution[41] without delay of any change concerning the identity of these ultimate beneficial owner(s).

Date _____
Name _____
Signature _____

[41] In case of a bank, type the word bank. In case of another type, specify the type of credit institution

Appendix 3: Indicators services, as referred to in article 1, section a., under 1º, 2º, 3º, 4º, 7º and 8º of the NORUT (service providers: credit institutions and others (*))

For all the indicators, the following shall apply:
- mandatory reporting of transactions or intended transactions;
- applicable to all said amounts is: NA*f.* or the equivalent thereof in foreign currency.

credit institutions and others

I. MANDATORY REPORTING (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:

1. Transactions of NA*f.* 250,000.00 and higher;
2. Transactions of NA*f.* 20,000.00 and higher in which case exchange takes place in larger denominations;
3. Transactions of NA*f.* 20,000.00 and higher in which exchange takes place in another currency;
4. Transactions of NA*f.* 20,000.00 and higher regarding purchasing or cashing by client of checks, traveler's checks or similar instruments of payment;
5. Transactions of NA*f.* 20,000.00 and higher in which securities are involved;
6. Transactions of NA*f.* 20,000.00 and higher that comply with two or more of the following indicators:
   a. uncounted;
   b. in foreign currency;
   c. not deposited on own account;
   d. transfer to foreign account.

C. Giro-based transactions

Transactions by non-accountholders of NA*f.* 20,000.00 and higher intended for foreign countries.

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:

Transactions in which case there is reason to assume that they could be in connection with money laundering or the financing of terrorism.

B. New accounts:

1. Accounts in which case two or more of the following indicators have been complied with:
   a. non-residents;
   b. identification problems;
   c. unusual condition offer;
   d. conspicuous number of accounts.

C. Transactions in which loans are involved:

Transactions of NA*f.* 250,000.00 and higher concerning an issued or intended loan that comply with two or more of the following indicators:
a. no explicable objective or no visible relation with (business) operations;
b. securities that are held by the credit institution or by third parties, the origin of which cannot be verified or that do not correspond with (business) operations of the client;
c. security deposits by third parties that do not have any visible relation with the client;
d. use does not correspond with the objective of the loan granted;
e. unexpected and inexplicable redemption of a (problem) loan;
f. incoming flow consists of many small amounts from unknown third parties or without an indication of the principal.

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

Transactions of NA*f.* 100,000.00 and higher, including the purchase or cashing by client of checks, traveler's checks or similar instruments of payment that comply with two or more of the following indicators:
a. from or to foreign countries;
b. no explicable objective or no visible relation with (business) operations;
c. transaction atypical of client;
d. incoming flow consists of many small amounts and outgoing flow of large amounts, or vice versa;
e. endorsed in client's name;
f. conspicuous number of accounts;
g. client acts as a straw man;
h. conspicuous turnover or conspicuous changes in the account balance;
i. unusual condition offer.

E. Transactions in which securities are involved:

Transactions with securities of NA*f.* 20,000.00 and higher including the physical surrender or delivery of securities that comply with two or more of the following indicators:
a. from or to foreign countries;
b. identification problems;
c. unusual condition offer;
d. transaction atypical of client;
e. client acts as a straw man;
f. client is nervous for no demonstrable reason;
g. client is accompanied and monitored;
h. no explainable objective or no visible relation with (business operations;
i. client has not been to office earlier;
j. incoming flow consists of many small amounts and outgoing flow of large amounts or vice versa.

F. Cash transactions:

1. Preference of the client for transactions under the marginal amount in which case the reason is to assume that he wants to avoid reporting;
2. Transactions of NA*f.* 20,000.00 and higher that comply with two or more of the following indicators:
   a. identification problems;
   b. unusual condition offer;

c. transaction atypical of client;
d. small denominations;
e. unusual packing;
f. frequent deposits by non-account holder;
g. client is nervous for no demonstrable reason;
h. client is accompanied and monitored;
i. client acts as a straw man;
j. no explainable objective or no visible relation with (business operations;
k. conspicuous turnover or conspicuous changes in the account balance;
l. incoming flow consists of many small amounts and outgoing flow of large amounts or vice versa.
m. client delivers uncounted funds without these being related to the (business) operations;
n. amount is not deposited by client on his own account or the account of the employer;
o. amount is deposited in favor of an account at a bank abroad.

3. Transactions of NA*f.* 5,000.00 and higher in which case funds are made available at a financial institution in or outside the Netherlands Antilles for a non-accountholder that comply with two or more of the following indicators:
   a. no explainable objective or no visible relation with (business) operations;
   b. identification problems;
   c. transaction atypical of client;
   d. client is nervous for no demonstrable reason;
   e. client is accompanied and monitored;
   f. client acts as a straw man.

G. Giro-based transactions

1. Transactions of NA*f.* 1,000,000.00 and higher that comply with two or more of the following indicators:
   a. from or to foreign countries;
   b. identification problems;
   c. conspicuous number of accounts;
   d. no explainable objective or no visible relation with (business) operations;
   e. transaction atypical of client;
   f. unusual condition offer;
   g. conspicuous turnover or conspicuous changes in the account balance;
   h. incoming flow consists of many small amounts and outgoing flow of large amounts or vice versa.
   i. not on client's own account.

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

* Anyone with a license or dispensation, based on the Banking and Credit System Supervision National Ordinance 1994, is included here.

Indicators services, as referred to in article 1, section a., under 9°, (credit card transactions) NORUT (service providers: i.a. credit card companies and credit institutions)

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 must also be reported to the Reporting Office.

B. Deposit by client:

Cash deposit by the client in Curaçao or Sint Maarten in favor of a credit card account of NA*f.* 5,000.00 and higher.

C. Use of credit cards:

Using the credit card in connection with transactions of NA*f.* 20,000.00 and higher in or from Curaçao and Sint Maarten.

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 terrorism.

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

Appendix 4: Source of Funds Declaration Form[42]

To: (Institution's name and address)

---------- Time: ----------

---------- Date:----------

----

1) I ----------understand that I am making this declaration for my own protection as well as for the protection of the credit institution.

2) I declare that the funds totaling NAf[43] _____ , to be deposited by the undersigned on account number _____, represents funds obtained by the undersigned from the following source (s):

_____

_____

_____

_____

This deposit includes drafts, wire transfers, exchange of currency, etc.

Sections 3 and 4 need only be completed by nonbank customers.

3) Status

[ ] resident of Curaçao or Sint Maarten

[ ] Other (specify) _____

[42] The source of funds declaration form must be used in the opening of accounts and/or the transferring of funds, and when accepting funds from noncustomers and non correspondent banks. Where it is reasonable to believe that a requested transaction is connected with criminal activity or if the client refuses to sign a "source of funds declaration", and there is no credible explanation to dispel concerns, the credit institution must refuse to execute the requested transaction to insure that the minimum standards are met, but still report it to the Unusual Transactions Reporting Center (FIU/MOT).

[43] Or the equivalent in another currency

4) Legally accepted customers identification documents (Article 3 of the National Ordinance on the Identification when rendering Services)

[ ] Number of a valid driver's license: _____

[ ] Number of a valid identity card _____

[ ] A valid travel document or passport: _____

[ ] Another document to be designated by the Minister: _____

5) The undersigned is aware that the information contained in this source of fund declaration form may be disclosed to those institutions which are legally entitled to the information contained here.*

_____
(Customer's name)

_____
(Customer's address)

_____
(Customer's signature)

Authorized by:

_____
(Name)

_____
(Signature)

* This provision is recommended in a pursuit of transparency towards the customer. However, credit institutions may consider excluding this clause from the source of fund declaration form when deemed necessary.