CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Money Transfer Companies

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 reflect therefore fully the observance of the recommended action plan made by the CFATF.

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

I. NATURE AND LEGAL BASIS OF THE PROVISIONS

The Central Bank of Curaçao and Sint Maarten (hereafter "Central Bank") is committed in 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 Money Transfer Companies 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
- Regulations for Foreign Exchange Transactions Curaçao and Sint Maarten (N.G. 2010, no. 112), article 21, paragraph 1.

Laws or executive decrees

The laws or executive decrees relating to money laundering and terrorist financing are:

(a) The Code of the Criminal Law (Penal Code) (N.G2. 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.71);
(d) The National Ordinance on Identification of Clients when rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no 66 (N.G. 2010, no 40) (NOIS);
(e) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on penalties and administrative fines for service providers) (N.G. 2010, no.70);
(f) Ministerial Decree with general operation of May 21, 2010, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Decree Indicators Unusual Transactions) (N.G. 2010, no. 27);
(g) Ministerial Decree with general operations of March 15, 2010, implementing the National Ordinance on Identification of Clients when Rendering Services (N.G. 2010, no.11);
(h) Ministerial Decree with general operation of March 15, 2010 for the execution of the NORUT (N.G. 2010, no.10)
(i) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no.93)
(j) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74);
(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 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 which are set out and illustrated below. Nevertheless the basic fact remains that 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"[3] 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 client's database with the names on the United Nations list[4].

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), money transfer companies are allowed to apply a Risk-based Approach ("RBA"). By adopting a RBA, it is possible for money transfer companies 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 subjected to enhanced customer due diligence as outlined in section II.2.A.

3 The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
4 The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.

Money Transfer Companies (MTC) 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.

I.4 Sanctions

MTC 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. During its on-site examination, 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.

I I PROVISIONS AND GUIDELINES ON THE DETECTION AND DETERRENCE OF MONEY LAUNDERING AND TERRORIST FINANCING FOR MONEY TRANSFER COMPANIES

This Chapter addresses the relevancy of the detection and deterrence of money laundering and terrorist financing for Money Transfer Companies, followed by a description of some policies and procedures for money transfer companies 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 which those institutions must provide to the Central Bank.

II.1 The relevancy of the detection and deterrence of money laundering and terrorist financing for money transfer companies

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

However, non-bank financial institutions, such as Money Transfer Companies, hereafter "MTC", have become increasingly vulnerable to money launderers and terrorists who seek, to launder their funds derived from criminal activities and finance their terrorist activities.

The integrity of the financial sector of Curaçao and Sint Maarten which among others includes MTC depends heavily 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 MTC. However, public confidence in MTCs and hence their stability can be undermined by adverse publicity as a result of the unwittingly use of these companies by criminals for money laundering and terrorist financing purposes.

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

It is therefore imperative that all MTCs continue to be vigilant in 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 MTCs and the financial sector of Curaçao and Sint Maarten.

All MTCs must exercise due diligence by ensuring that at least they have in place policies and procedures including a policy statement covering certain aspects relevant to the detection and deterrence of money laundering and terrorist financing. This is further discussed in the next sections.

II.2 Policy statement

Each MTC's, Board of Supervisory Directors [5] and senior management [6], must issue a policy statement that expresses the commitment to combat the abuse of its facilities, product and services for money laundering and terrorist financing purposes. The policy statement must state the company's intention to comply with current anti-money laundering and terrorist financing legislation and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions.

This policy statement is a statement of "Best Practice" of the Board of Supervisory Directors and Senior Management of a MTC 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 the clients and transactions;

- The appointment of one or more compliance officers 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 MTC internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness;

- 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 MTCs to (continuously) observe the relevant standards from international (standard-setting) bodies and ensure that these standards are included in their policy statements.

5 See Appendix 1 for the definition or explanation or summary.
6 See Appendix 1 for the definition or explanation or summary.

II.2.A Detection and deterrence of Money Laundering

MTCs may only offer their money transfer services to natural persons and have the obligation to identify those (prospective) personal clients[7] before rendering them money transfer 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 financial institutions. Also, internal procedures must clearly indicate that clients or their representatives must identify themselves and which identification documents are acceptable.

The legally allowed client identification documents and the nature of the transaction are prescribed in the NOIS[8]. The required information must be regularly updated and adequately documented. MTC must have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, and their retention period. An important objective for a MTC is to be able to retrieve this information, without any undue delay. Hence, the Central Bank requires the MTC to implement a checklist containing identification and/or transaction information and to maintain a centralized record keeping system to retain copies. The MTC must ensure that the identification documents are valid at all times. Reference is in this respect made to also article 3, paragraph 3 of the NOIS.

Foreign branches and subsidiaries

MTCs 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. MTC 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.

MTCs 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.

Moreover, MTCs are required to maintain a current list of its agents and all their branches and subsidiaries (both locally and abroad). Mentioned list must be made available to the Central Bank.

Customer Due Diligence (CDD)

MTC's must develop clear customer policies and procedures with regards to rendering money transfer services, including a description of the types of customers that are likely to pose a higher than average risk to the company. The policies must ensure that transactions will not be conducted, business is not commenced with (prospective) customers who fail to provide satisfactory evidence of their identity. Anonymous transfers and fictitious names must be prohibited.

7 See Appendix 1 for the definition or explanation or summary.
8 See Appendix 1 for the definition or explanation or summary.

MTC 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 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. If doubts arise relating to the identity of the client after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the Financial Intelligence Unit. The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties (MOT).

The required information regarding the client and the allowed identification documents with regards to money transfer services is legally prescribed and must be updated regularly and adequately documented. An important objective for a MTC is to be able to retrieve this information, without any undue delay. Hence, the implementation of a checklist containing identification and/or transaction information and a centralized record-keeping system must be in place. The efforts to "know your customer" must continue once the client has been identified and becomes a regular client. For identity reasons each MTC will distinguish the following customers and their transactions:

- Transactions with "prospective" regular personal customers based on a regular relationship;
- Transactions with occasional personal customers;
- Occasional transactions that are wire transfers in the circumstances covered by the FATF's Interpretative Note to SR VII.

A MTC must establish the identity of each customer which contemplated or actually performed a money transfer transaction.

MTCs 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.

A MTC must apply CDD requirements to existing customers[9] on the basis of materiality and risk and must conduct due diligence on such existing relationships at appropriate times.

A) Transactions with regular customers

Identification of regular resident and non-resident personal customers

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

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

9 Existing customers as of the date that the national requirements are brought into force.

Resident customers

In addition the identity of a **resident** individual customer can be verified by checking a local telephone directory and/or seeking confirmation of identity or activities at other local financial institutions. Management may require additional information to be submitted, such as:

- checking a local telephone directory;
- verifying occupation and name of employer; and
- requesting a copy of utility bill.

Non-resident customers

A MTC must also pay special attention to non-resident customers and understand the reasons for which the customer uses the company's money transfer services. Verification of the identity of **non-resident** clients must be obtained as soon as reasonably practicable by reference to one or more of the following, as deemed practical and appropriate:

- international or home country telephone directory;
- embassy or consulate in home country of address provided by the prospective client;

Identification in case of representation

Pursuant to article 5 of the NOIS, a MTC is bound to establish the identity of the individual appearing before him on behalf of a customer or on behalf of a representative of a customer, before it proceeds to render the money transfer services. If the customer acts for a third party or that third party also acts for another third party, the MTC must be bound to also establish the identity of each third party.

B) Transactions with occasional customers

Transactions processed by a MTC for occasional customers will be classified as an incidental service. Management's responsibility is to make the staff aware of all the relevant current arrangements or procedures. The procedure for the identification of regular personal customers must also be applied for the identification of occasional personal customers. Identification will be necessary for all transactions and for the amounts above the limits established by the Minister of Finance, as referred to in the Ministerial Decree as published in the N.G. 2010, no.11.

C) Non face-to-face clients

MTCs are not permitted to process payment instructions provided by non-face-to-face customers/business relation.

Where the MTC 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.

Risk-based approach

Risk classification
A MTC 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 received.

A MTC must at least consider the following risk categories while developing and updating the risk profile of a customer: (i) customer risk, and (ii) country or geographic risk.

(i) Customer risk: It is important for a MTC to assess the type of customer. The types of customers that indicate a higher risk include:
- Politically exposed persons (PEPs) and their families and associates;
- Transaction of significance takes place (from time to time);
- Material change takes place in the client's transactional behavior.

(ii) 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 that have designated terrorist organizations operating within them.

The weight assigned to these risk categories (individually or in combination) in assessing the overall risk exposure may vary from one MTC to another. The MTC 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.

Enhanced CDD for high risk categories of customers

A MTC 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. MTCs should conduct extensive due diligence for high risk customers, including PEPs, their families and associates. The company should make reasonable efforts to ascertain that its customer's source of wealth is not from illegal activities and where appropriate, review its regular customer's character, and of the type of transactions this customer would typically conduct. The institution's decision to provide money transfer services to such customers must be taken at its senior management level. A MTC must not accept or provide money transfer services if the institution knows 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.

AMTC must ensure that the identification documents of its 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, a MTC must regularly review at least its more important customers to detect if an existing customer may have become PEP. Additionally, MTCs are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.

Furthermore, MTCs must implement appropriate risk management systems to determine whether a potential customer, customer or beneficial owner is a politically exposed person (PEP).

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

MTCs are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is therefore important for every a MTC to have adequate procedures for its personnel in place. These procedures must cover:

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

Re.: a) Recognition of unusual transactions

An unusual transaction will often be a transaction which is inconsistent with a customer's known legitimate business or personal activities. Therefore, the first key to recognize that a transaction or series of transactions is unusual is to know enough about the customer's source of income. Based on the NORUT, objective and subjective indicators have been established by means of which MTC must assess if a customer's transaction qualifies as an unusual transaction. Those indicators are listed in Appendix 2.

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 the adequately documenting of unusual transactions.

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

Wire transfer

Wire transfers are increasingly used for laundering funds from illegal sources. A MTC must be extremely vigilant in accepting funds from its customers for transfer.

Based on FATF's Special Recommendation (SR) VII[10], MTCs must include accurate and meaningful originator information (at least the receivers and senders name and address) on funds transfers

10 In October 2001, the FATF agreed on eight Special Recommendations on Terrorist Financing. Special recommendation VII pertains to wire transfers.

within or from Curaçao and Sint Maarten, and possible related messages that are sent, and the information must remain with the transfer or related message through the payment chain.

A beneficiary MTC must be required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by at least name and address of originator. The lack of this information (at least name and address of originator) may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit. In some cases, the beneficiary MTC should consider restricting or even terminating its business relationship with financial institutions that fail to meet SRVII standards.

MTCs must give special attention to transactions involving recipients and senders of funds from high-risk and non-cooperative jurisdictions, being countries that, according to the criteria of FATF, do not apply sufficient anti-money laundering measures and procedures in combating the financing of terrorism. In addition the MTCs' policies and procedures must at least require the company to ascertain that the respondent foreign MTC has effective customer and know-your-customer (KYC) [11] policies with respect to rendering money transfer services, and is effectively supervised.

Furthermore, MTCs 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.

Misuse of technological development

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

Re.: b) The documentation of unusual transactions

To guard against money laundering and terrorist financing, MTCs 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.

Re.: c) Reporting of unusual transactions

MTCs must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. 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 any undue delay. All transactions as mentioned in the Ministerial Decrees containing general measures regarding the Indicators for unusual transactions must be referred to the designated officers, in the format(s) approved by management. Nevertheless, management must stipulate the categories of unusual transactions which must also be brought to its attention whenever

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

available, additional documents such as copies of the identification documents, checks and account ledgers records must also 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 compliance officer, the reasons therefore must be adequately documented and signed off by this 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 MTC.

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 MTC.

Taking into account the above-mentioned procedure for external reporting, the compliance officer(s) should be able to act independently.

Management must establish policies to ensure that:

- a MTC 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 them;
- a MTC and its Supervisory Directors, senior management and employees follow the instructions from the FIU/MOT to the extent that it carries out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.

Exempt lists

In some jurisdiction 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 on the reporting obligation of financial service providers.

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

Each MTC must formally designate one or more officer(s) at management level responsible for the deterrence and detection 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 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 policies and procedures;
- to analyze transactions and verify whether any are subject to reporting according to the indicators as mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- to review all internally reported unusual transactions on their completeness and accuracy with other sources;
- to keep records of internally and externally reported unusual transactions;
- to prepare the external report of unusual transactions;
- to execute closer investigation on unusual or suspicious transactions;
- to remain informed of the relevant developments regarding local and international 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. 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 a MTC'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 MTC external auditors. These tests include amongst others:

- evaluation of the MTC anti money-laundering and anti-terrorist financing manuals;
- review of copies of customers' identification documents;
- interviews with employees who handle transactions and with their supervisors;
- sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- assessment of the adequacy of the record retention system.

The scope of the testing and of the results must be documented, with any deficiencies being reported to senior management and/or to the Board of Supervisory Directors, and to the designated officers with a request for a response indicating corrective action taken or to be taken and a deadline for doing so.

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

MTCs must ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are adhered to. Each MTC must establish and adhere to proper policies and procedures to screen its employees on criminal records.

MTCs 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 for the MTC 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 for reporting of 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/advisory staff

Staff members dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore 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 unusual transactions, and that those transactions need to be reported whether the funds are accepted or not. They must also know what procedures to follow in this respect. Training must be provided on the KYC principles, on how to detect unusual transactions or proposals, and on the procedures to follow after identifying these. The need to verify the identity of the customer must be understood, and training must be provided in the organization's customer verification procedures.

(c) 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.

(d) On-going training

It is necessary to arrange for refreshment training at regular intervals to ensure that the staff remembers its responsibility and to 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 the laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. This might be best achieved through amongst others at least a semi-annual review of the instructions for recognizing and reporting of unusual transactions.

For a MTC 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 staff 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 the money laundering; and terrorist financing requirements; and

- an ongoing training plan.

II.2.B Detection and deterrence of Terrorist Financing

MTCs must take into account the relevant characteristics including types of transactions listed in the annex 1 to the FATF document:"Guidance for Financial Institutions in Detecting Terrorist Financing"_[12] Those characteristics and transactions could be cause for additional scrutiny and could indicate funds involved in terrorist financing. In addition, MTCs must take into account other available information including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in:

1. the list issued by the United Nations;[13]
2. the annex to the National decree freezing assets from Taliban cs and Osama bin Laden cs as lastly amended (N.G. 2010, no. 93);
3. annex 2[14] to the FATF document" Guidance for Financial Institutions in Detecting Terrorist Financing"; and
4. the listing[15] of the Office of Foreign Assets Control (OFAC)[16] or of other national authorities.

Supervised institutions must continuously match their clients' 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.

If a MTC 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 National Decree containing general measures for indicators on terrorist financing N.G 2010, no. 27.

II.3 Record-keeping

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

Where appropriate, MTCs 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 than required under the relevant money laundering and terrorist financing legislation, rules and regulations.

A document retention policy must include the following:

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

12 The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
13 The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.
14 The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
15 The list can be consulted at FINCEN's website at
http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html.
16 See Appendix 1 for the definition or explanation or summary.

- Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driver's licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued. Moreover, records on identification must be kept at least five years following termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

- MTCs must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities.

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

II.4 Examination by the Central Bank

All MTC 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 MTC must be prepared to make available:

- its written and approved policies and procedures on money laundering and terrorist financing prevention;
- the name of each designated officer responsible for the MTC'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;
- schedule of the training provided to the company's personnel regarding money laundering and terrorist financing;
- assessment report on the company's policies and procedures on money laundering and terrorist financing by the internal audit department or the company's external auditor; and
- documents on system tests such as the customers' transactions data and listings of regular customers and occasional customers.

During the on-site examinations, the Central Bank will assess the institutions' 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 MTC that does not comply with the compulsory AML/CFT requirements is committing an offence, which is an unlawful and punishable act. The way in which an offence is punished depends on the severity of the offence committed. Offences are subdivided in: misdemeanours and felonies.

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

Pursuant to article 9, paragraph 1 and article 9a paragraph 1, of the NOIS the Central Bank has the authority to impose a penalty or an administrative fine on the MTC 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 on the non-compliance penalties and administrative penalties for reporters of 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[17]
- Article 12, paragraph 2[20]
- Article 13[22]
- Article 22h, paragraph 3[25]

NOIS

- Article 2, paragraph 1, 2[18], and 5[19]
- Article 3[21]
- Article 5, paragraph 1 through 4[23], and 6[24]
- Article 6[26]
- Article 7[27]
- Article 8[28]
- Article 11, paragraph 3[29]

17 Obligation to report unusual transactions
18 Obligation to identify the client before rendering any service
19 Obligation to identify the client before rendering any service
20 Obligation to provide additional information to the Reporting Center
21 Obligation to establish the identification of the client
22 Indication how to report unusual transactions
23 Obligation to identify the representative
24 Dispensation or exemption of the Minister under certain conditions
25 Process of reporting of unusual transaction and additional information
26 Obligation to document the data received
27 Obligation of record keeping
28 Prohibition to render services without identification
29 Process of the identification of clients reporting of unusual transaction and additional information

Based on above-mentioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum penalty of NA*f.* 500,000. A list of these requirements is included in Appendix I to the Policy Rule on the violation 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[30] to impose a penalty the term in which the violator may execute a mandate without a penalty being forfeited.

The amount due may be collected by way of a writ of execution, increased by the costs falling on the collection. The writ of execution shall be served on the violator by means of a bailiff's notification and will produce an entitlement to enforcement[31].

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.* 1000[32].

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, and 6
- Article 20, paragraph 2	- Article 6
- Article 22h, paragraph 3	- Article 7
	- Article 8
	- Article 11, paragraph 3

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

Before proceeding to imposing a penalty, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a penalty, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term[33].

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

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

30 Decree:"Beschikking" in Dutch
31 Article 22a, paragraph 3 through 5, NORUT and article 9, paragraph 3 through 5, NOIS
32 See article 3, paragraph 1 of the ND PFRUT and article 3, paragraph 1 of the ND PFSP
33 Article 22b, paragraph 3, of the NORUT and article 9a, paragraph 3, ND PFSP

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. An example of a case where the Central Bank may immediately refer the violation to the Public Prosecutor for further (criminal) investigation and prosecution is that the Central Bank, during an on-site examination, takes notice of serious or grave violation of the NORUT, NOIS or the Provisions and Guidelines.
Furthermore, if the supervised (financial) institution or individual does not comply with its 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[34].

34 Article 4, paragraph 3, of the ND PFRUT and NP PFSP, respectively

Appendix 1: Glossary/Definitions

In this document the following abbreviations and definitions are used.

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, which have agreed to implement common countermeasures to address the problem of criminal money laundering. CFATF was established as a result of meetings convened in Aruba in May 1990 and in Jamaica in November 1992. The CFATF maintains a website at: http://www.cfatf.org/

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

Client or customer
Pursuant to article 1, sub c of the NOIS, a client/customer is anyone to whom a 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/or Sint Maarten.

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

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

Identify means to establish the identity of someone.

Know Your Customer (KYC)
The objective of KYC policies and procedures of MTC is for them to know the customer with whom they are dealing, especially their regular customers. Sound KYC policies and procedures are critical in protecting the safety and soundness of the MTC and the financial system.

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

Misdemeanour is a minor crime which is punishable.

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 state or of governments, senior politicians, senior government, judicial or military officials, senior executives or publicly owned corporations and important political party officials.

Senior Management
Comprises the individuals entrusted with the daily management of the operations to achieve the MTC objectives.

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: Indicators services, as referred to in article 1, section a., under 10º NORUT, (service providers: money transfer companies)

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. Cash transactions:

Transactions of NA*f*. 5,000.00 and higher in which case the funds are made available in the form of circulating currency, in checks or by means of a credit or debit card, or are made payable in the form of circulating currency, in checks or by deposit on an account.

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 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 3: Source of Funds Declaration Form[35]

To: (Institution's name and location)

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

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

---

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

2) I declare that the funds totaling NAf[36] _____ , represents funds obtained by the undersigned from the following source:

_____

_____

_____

_____

Sections 3 and 4 need only be completed by non-bank customers.

3) Status

[ ] Resident of Curaçao or Sint Maarten

[ ] Other (specify) _____

4) Legally accepted customers identification documents (Article 3 of the National

_____

[35] The source of funds declaration form must be used in 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 MTC 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 (MOT).

36 Or the equivalent in an other currency

Ordinance on the Identification when rendering Services, 1996)

[ ] 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) 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.37

_____
(Customer name)

_____
(Customer address)

_____
(Customer Signature)

Authorized by:

_____
(Name)

_____
(Signature)

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