CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Administrators of Investment Institutions and Self-Administered Investment 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 reflect therefore fully the observance of the recommended action plan made by the CFATF.

In the next update 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 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 Administrators of Investment Institutions and Self-Administered Investment 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 Investment Institutions and Administrators (N.G. 2002, no.137), article 9, paragraph 1, and article 18 paragraph 1.

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

a) The Code of Criminal Law (Penal Code) of (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. 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); and
j) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74).

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

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

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

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

- relevant provisions of all the above-mentioned ordinances and decrees; 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

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

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

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

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

I.2 Terrorist financing

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

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

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

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

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), administrators and self-administered investment institutions are allowed to apply a Risk-Based Approach ("RBA"). By adopting a RBA, it is possible for administrators and self-administered investment 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 should be subject to the minimum due diligence standards outlined in section II.2.A of these Provisions and Guidelines, clients identified by the institution as high risk must be subject to enhanced customer due diligence while low risk clients may be subject to simplified/reduced customer due diligence, as outlined in section II.2.A.

Administrators and self-administered investment institutions applying the RBA must document their policies, procedures and controls relative to their applied RBA. Furthermore, the administrators and self-administered investment institutions 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

Administrators and self-administered investment institutions are required to comply with the compulsory requirements set out in the NORUT and/or NOIS and the Provisions and Guidelines under these laws.

The Central Bank will asses during its on-site examination, the supervised 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 ADMINISTRATORS OF INVESTMENT INSTITUTIONS AND SELF-ADMINISTERED INVESTMENT INSTITUTIONS

This chapter addresses the relevancy of the detection and deterrence of money laundering and terrorist financing for administrators and self-administered investment institutions[6]. The due diligence process applicable to the administrators described in this chapter, comprises both the due diligence process relative to their own clients[7] and the clients of an investment institution[8] administered by them. Subsequently, some policies and procedures for administrators and self-administered investment institutions to detect and deter money laundering and terrorist financing are addressed as well as the information and documentation to be collected. The chapter is concluded with a listing of the information and documentation of the respective relevant policies and procedures that the administrators and self-administered investment institutions must provide to the Central Bank.

All administrators and self-administered investment institutions must at all times adhere to the stipulations in these Provisions and Guidelines. In the event that an administrator is entrusted with all or part of the due diligence process of an investment institution, the due diligence performed by the administrator must be regarded as that of the investment institution. Nonetheless, the investment institution (and not the administrator) remains ultimately responsible to ensure adherence to these Provisions and Guidelines. In other words, while an investment institution may rely on an administrator to carry out its anti-money laundering and terrorist financing matters, this does not transfer the ultimate responsibility of the investment institution with respect to compliance with these Provisions and Guidelines to the administrator.

The Central Bank requires all investment institutions that have outsourced their administrative tasks to an administrator, to clearly indicate in an agreement that the administrator will adhere to the laws and regulations related to money laundering and terrorist financing applicable to the investment institution while carrying out its administrative duties for the investment institution. This contract must be signed by both the investment institution and the administrator.

[6] Reference is made to the definition of self-administered investment institutions in the glossary/definition list (Appendix 1)
[7] Reference is made to the definition of a client of an administrator in the glossary/definition list (Appendix 1)
[8] Reference is made to the definition of a client of an investment institution in the glossary/definition list (Appendix 1)

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

The occurrence of money laundering and terrorist financing has over the past years been more evidenced in the traditional banking sector than in the other financial sectors. However, as banks are aggressively taking measures to detect and deter money laundering and terrorist financing, non-bank financial institutions, such as investment institutions, have become increasingly vulnerable to money launderers and terrorists as they seek to respectively launder their funds derived from criminal activities and finance their terrorist activities.

In view of the fact that cash transactions are generally discouraged in the securities industry across jurisdictions, investment institutions are less conducive to the initial placement of criminally derived funds than other types of financial institutions, such as banks. Nonetheless, investment institutions may particularly be misused for money laundering and terrorist financing purposes at the layering and integration stages.

Unlike credit institutions, investment institutions provide a potential avenue which enables money launderers and terrorists to dramatically alter the form of their funds. Such alteration allows conversion of the funds into an entirely different type of assets, namely securities. Given the liquid nature of the participating interests of most investment institutions, the reversal of this conversion may also occur with potentially great frequency, whereby the proceeds from the investment institutions are being placed back into the economy appearing as legitimate funds.

The aforementioned liquid nature of the participating interests of most investment institutions, accompanied by the ability to combine both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of possible investment mediums, and the ease with which transfers can be effected between them, offer money launderers and terrorists attractive ways to respectively integrate criminal proceeds into the economy and finance their illicit operations through investment institutions.

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

In this context, the Central Bank is issuing these Provisions and Guidelines to further promote and maintain the financial stability, soundness and reputation of investment institutions and administrators operating in or from Curaçao and Sint Maarten.

Due to the diversity in the activities of investment institutions and administrators, the nature and scope of their vigilance systems may vary according to the size and complexity of the institutions. Nonetheless, administrators and self-administered investment 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 is further discussed in the next sections.

II.2 Policy statement

The Board of Directors[9] and senior management[10] of an administrator or of a self-administered investment institution must issue a policy statement, which clearly expresses the commitment of the administrator and self-administered investment institution to combat the abuse of their facilities and services for money laundering and terrorist financing purposes. The policy must state the intention of the administrator and self-administered investment institution 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 an administrator or self-administered investment institution which outlines the institution's policies and procedures and must be communicated to the employees of the administrator or self-administered investment institutions.

The policy statement[11] 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 institution's internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness;

- The preparation of an appropriate training program for 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 administrators and self-administered investment institutions to (continuously) observe the relevant standards from international (standard-setting) bodies and ensure that these standards are included in their policy statements.

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

II.2.A Detection and deterrence of money laundering

Administrators and self-administered investment institutions must 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. They must also have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions. These policies and procedures must apply when establishing customer relationships and when conducting ongoing due diligence. Examples of non-face-to-face operations include: business relationships concluded over the internet or by other means such as through the post. Measures for managing the risks must include specific and effective customer due diligence procedures that apply to non-face-to-face customers. These procedures may include: the certification of documents presented; the requisition of additional documents to complement those which are required for face-to-face customers; development of independent contact with the customer; reliance on third party introduction; and the requirement that the first payment be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Foreign branches and subsidiaries

Administrators and self-administered investment 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. Administrators and self-administered investment 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.

Administrators and self-administered investment 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")

Administrators and self-administered investment institutions have the obligation to determine the true identity, including the (ultimate) beneficiaries[12] of their (prospective) clients[13], where applicable, before offering them services. Administrators and self-administered investment institutions are also required to obtain information on the purpose and intended nature of the business relationship with their (prospective) clients being legal entities prior to offering them services. Internal procedures must also clearly indicate which identification documents are required for the acceptance of prospective clients. Before the provision of services to a prospective client, he or she must be duly identified from documents issued by reliable sources, as prescribed in the NOIS. Furthermore, the directors/representatives of the prospective investment institution to be administered by an administrator, must whenever possible, be interviewed personally. The required information regarding the (prospective) client, the authorized identification documents, and the nature of the administrative/investment service(s) to be provided must be adequately described and documented. An important objective for administrators and self-administered investment institutions is to be able to retrieve this information, when needed, without any undue delay. Hence, the implementation of a checklist containing the identification and/or information of clients and a centralized record-keeping system must be in place.

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

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

Administrators and self-administered investment institutions must not accept or maintain a business relationship with a client if they know or must assume that the funds of the client were derived from corruption or misuse of public assets, without prejudice to any obligation they have under criminal law or other laws or regulations.

Furthermore, administrators and self-administered investment institutions are encouraged to perform antecedent screening on persons subject to CDD. This could be done by e.g. searching the internationally accepted authoritative lists on the internet.

CDD to be performed by administrators on their (prospective) clients being administered investment institutions

As indicated in the definition in appendix 1, the term "client" in the context of an administrator of investment institutions, does not only refer to the administered investment institution, hereafter referred to as "investment institution", but also to the applicant upon whose instructions the business relationship with the administrator is established. The applicant who provides the instructions may or may not be the prospective investment institution.

Therefore, the administrator must look beyond the investment institution for due diligence purposes and, depending upon the circumstances, requests proof of identity of any of the following parties:

- the (managing and supervisory) directors of the investment institution;
- any party who provides or will provide instructions to the administrator on behalf of the investment institution;
- in case any of the parties mentioned above is a legal entity, the directors and the ultimate beneficial owners holding a qualifying interest[14] in the legal entity. Please note that a proof of registration of the legal entity with the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation must also be requested.

Pursuant to article 3 of the NOIS, the identity of the above-mentioned parties must be established through one of the following valid documents:

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

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

Face-to-face identification

When conducting face-to-face identification, an administrator must:

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

Non-face-to-face identification

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

Verification of identity

The administrator is required to verify the identity of the individuals subjected to its CDD when the relationship is established with the prospective client. The identity of a resident individual that has previously been subjected to the administrator's CDD must also be verified when the administrator has doubts about the veracity or adequacy of the identification data obtained in the past from this individual.

Examples of verification include:

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

The administrator should complete the verification of the non-resident individuals subjected to its CDD before or during the establishment of the business relationship, provided that:

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

Verification of the existence and nature of the administered investment institution's business

In addition to obtaining the identification documents of the above-mentioned parties associated with the administered investment institution, the administrator must verify the existence and nature of the investment institution's business through reliable identification documents, with preference

for originals and official documents. The existence and nature of a (prospective) investment institution must be legally identified with the aid of a certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation, or with the aid of an identification document to be drawn up by the administrator. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.

Documents regarding the administered investment institution containing at least the following information must be kept on file:

- official name according to its articles of association or similar document[15];
- trade name, if different;
- registered address in full;
- country of incorporation and/or country of seat;
- registration number in the country of incorporation or establishment;
- name of the persons who exercise ultimate effective control in the investment institution; and
- control structure of the investment institution.

The administrator may require additional information to be provided by the investment institutions, such as:

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

In instances that the administrator is unable to comply with the aforementioned CDD requirements, the administrator should not commence a business relationship or perform a transaction for the investment institution. In addition, the administrator should consider filing a report with the Financial Intelligence Unit ("FIU"). The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties ("MOT").

On-going CDD

The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. The on-going due diligence process must also include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the administrator's knowledge of the client, its business and risk profile, and where necessary, the source of funds. In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the FIU. Administrators must apply CDD requirements to existing customers[16] and may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship or transaction.

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

[16] Existing customers as at the date that the national requirements are brought into force.

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

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

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

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

CDD to be performed by administrators and self-administered investment institutions on the (prospective) investors of the (self-) administered investment institutions.

Investment institutions have the obligation to determine the true identity of their (prospective) investors[17], including where applicable the (ultimate) beneficiaries[18] of their investors that are legal entities. The identification of the investors can be either performed by the administrator to which the administrative services pertaining to the investment institution has been wholly or partially outsourced, or by the self-administered investment institution. Administrators and self-administered investment institutions are required to obtain information on the purpose and intended nature of the business relationship with the (prospective) investors. The internal policies and procedures of the administrator and the self-administered investment institution must clearly describe which identification documents are acceptable for the acceptance of investors in the (self-)administered investment institution. Before the provision of services to a prospective investor, identification of the prospective investor must be made from documents issued by reliable sources, as prescribed in the NOIS.

These policies and procedures must also include a description of the types of investor that are likely to pose a higher than average risk to the investment institution. These policies and procedures must ensure that (prospective) investors will not be accepted in case they fail to provide satisfactory evidence of their identity.

Administrators and self-administered investment institutions must also be able to retrieve the information received from investors, when needed, without any undue delay. Hence, the implementation of a checklist containing the identification and/or transaction information of investors and a centralized record-keeping system must be in place.

Administrators and self-administered investment institutions must not accept or maintain a relationship with an investor if they know or must assume that the funds of the investor were derived from corruption or misuse of public assets, without prejudice to any obligation they have under criminal law or other laws or regulations.

Administrators and self-administered investment institutions are required to ensure that documents, data or information collected under the due diligence process relative to the investor is kept up-to-

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

date and relevant by undertaking reviews of existing records, particularly for higher risk categories of investors.

Administrators and self-administered investment institution must take necessary measures in preventing the unlawful use of entities identified as vulnerable, such as charitable or non-profit organizations, to be used as conduits for criminal proceeds or terrorist financing.

Identification and verification of identity for subscription

All (prospective) investors must be duly identified at the time of subscription in the investment institution. For identity purposes, the following categories of investors are distinguished:

A) investor is a financial institution;
B) investor is an individual;
C) investor is a partnership;
D) investor is a corporate entity;
E) investor is a corporation which is a private company; and
F) investor is an institutional investor.

A. Investor is a financial institution

The Minister of Finance grants exemption from the obligation to identify an investor that is a financial institution as referred to in article 2, paragraph 4, subs a and b of the NOIS juncto article 7 of the Ministerial Decree with general operation for the execution of the NOIS, provided that the investor is a(n):

1. an enterprise or institution that possesses a license, as referred to in article 2 of the National Ordinance on the Supervision of Banking and Credit Institutions 1994 (N.G. 1994, no. 4) or an insurance company that possesses a license, as referred to in article 9 of the National Ordinance on the Supervision of the Insurance Industry (N.G. 1990, no. 77), or an investment institution or an administrator that possesses a license, as referred to in article 3, respectively 14 of the National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002. No. 137) or a trust office that possesses a license, as referred to in article 2, second paragraph, of the National Ordinance on the Supervision of Trust Service Providers (N.G. 2003, no. 114) or an insurance broker that is listed in the register, as referred to in article 4 of the National Ordinance on the Insurance Brokers (N.G. 2003, no. 113); or
2. legal person that is affiliated to a stock exchange which is a member of the Fédéracion Internationale des Bourses de Valeurs and which is not established in a country that does not comply with at least 10 of the core recommendations proposed by the Financial Action Task Force (FATF).

Administrators and self-administered investment institutions must document in their records the reason why no further identification documents were requested from the relevant investor, by filing, for example, the documents evidencing that the institutions meet the aforementioned criteria.

Financial institutions that do not meet the aforementioned criteria must be identified in accordance with the provisions outlined below.

B. Investor is an individual

Pursuant to article 3 of the NOIS, the identity of an individual must be established through one of the following valid documents:

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

When conducting face-to-face identification of an investor being an individual, an administrator or self-administered investment institution must:

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

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

The administrator or self-administered investment institution is required to verify the identity of a prospective investor being a natural person. The identity of an investor that has previously been subjected to CDD, must also be verified when the administrator or self-administered investment institution has doubts about the veracity or adequacy of the identification data obtained in the past from this investor. Examples of verification include:

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

C. Investor is a partnership

Where the investor is a partnership, the following information and documentary evidence must be obtained and kept on file:

- a certified extract from the Chamber of Commerce, or similar document being either the original or certified copy of the certificate of establishment or similar document;
- a certified copy of the partnership agreement or Articles of Partnership;
- the identities of all partners having authority to represent the partnership and of all those authorized to issue instructions and represent the investor towards the administrator or self-administered investment institution.

In case the partners are individuals the rules as outlined in these guidelines for investors being individuals must be followed. In case a partner is a corporate entity (partnership, foundation, etc.), the rules as outlined in these Provisions and Guidelines for corporate entities have to be followed.

D. Investor is a corporate entity listed on a stock exchange or a subsidiary of an entity listed on a stock exchange

Where the investor is a corporation which:

- is listed on a stock exchange; or
- is the subsidiary of a company listed on a stock exchange,

the following information is required:

1. a certified extract from the Chamber of Commerce or similar document being either the original or certified copy of the certificate of incorporation or similar document;
2. a list of directors' names, addresses and dates of birth; and
3. identification of all persons representing the investor towards the administrator or self-administered investment institution.

If the investor is listed on a stock exchange which is a member of the Fédéracion Internationale des Bourses de Valeurs and which is not established in a country that does not comply with at least 10 of the core recommendations proposed by the Financial Action Task Force (FATF), as described in article 7 of the Ministerial Decree with general operation for the execution of the NOIS, then only a certified extract from the Chamber of Commerce or similar document must be required.
Documentary evidence must be kept on file as to the listing of the (parent) company. In case of a subsidiary of a company listed on a stock exchange documentary evidence must be kept on file that the investor is a subsidiary of such a listed entity.

In case the representatives towards the administrator or self-administered investment institution are individuals, copies of identification documents have to be obtained in a format as outlined in these guidelines for individual investors. In case the representatives towards the administrator or self-administered investment institution are a corporate entity (such as partnership or foundation), copies of identification documents as outlined in these guidelines for corporate entities have to be obtained.

E. Investor is a corporation which is a private company[19]

Where the investor is a private company the following information must be obtained in addition to the information required for an investor being a company listed on a stock exchange:

- the identity of all directors and all persons authorized to represent the investor towards the administrator or the self-administered investment institution has to be determined in accordance with these guidelines;
- a list of names and addresses of shareholders holding directly or indirectly 25% or more of the issued share capital of the company, and in the case of individual shareholders, their occupations and dates of birth;
- where a significant shareholder (25% or more) is a body corporate and particularly where it appears to be a nominee or "front" company, information must be sought from the company regarding the ultimate beneficial ownership of that particular company. Where the ultimate

[19] A private company is a non-exchange listed company.

beneficial owner(s) is(are) individual(s), identification documents as set out in these guidelines pertaining to individual investors must be obtained.

Administrators and self-administered investment institutions are required to verify the existence and nature of the investor being a private corporate entity. One or more of the following information must in that respect be obtained requested:

- registration number in the country of incorporation or establishment;
- control structure of the investment institution;
- shareholders' register; and
- audited financial statements/cash flow statements.

F. Investor is an institutional investor

Where the investor is an institutional investor e.g. a pension fund, local authority, collective investment scheme or unit trust, endowment fund or charity, the administrator or the self-administered investment institution as the case may be will refer to appropriate sources to check identity depending on the circumstances. Where the investor is a pension fund of a listed company (or its subsidiary), or of a Government agency or local authority, no further steps to verify identity, over and above existing business practice, will normally be required. At all times documentary evidence must be collected and kept on file regarding such institutional investors including documentary evidence of the identity of its representatives, as outlined above for individual investors.

Administrators and self-administered investment institutions which are not able to comply with the aforementioned CDD requirements must not commence a business relationship or perform a transaction for the prospective client. In addition, the administrator and self-administered investment institution must consider filing a report with the FIU.

On-going CDD

The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. The on-going due diligence process must also include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the administrator's or self-administered investment institution's knowledge of the client, its business and risk profile, and where necessary, the source of funds.

In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the Financial Intelligence Unit ("FIU"). Administrators and self-administered investment institutions must apply CDD requirements to existing customers[20] and may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship or transaction.

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

a) a transaction of significance takes place;
b) there is a material change in the way that the account is operated;
c) customer documentation standards change substantially; and
d) the administrator or self-administered becomes aware that it lacks sufficient information about an existing customer.

[20] Existing customers as at the date that the national requirements are brought into force.

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

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

CDD on Politically Exposed Persons

Administrators and self-administered investment institutions must have appropriate risk management in place to determine whether its (proposed) clients are considered political exposed persons ("PEP's) and must conduct enhanced due diligence for PEPs, their families and associates. The institution's decision to enter into business relationships with PEPs 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. Neither an administrator nor a self-administered investment institution must accept or maintain a business relationship if it knows or must assume that the funds are derived from corruption or misuse of public assets. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, administrators and self-administered investment institutions must obtain senior management approval to continue the business relationship. Where administrators and self-administered investment institutions are in a business relationship with a PEP, they must conduct enhanced ongoing monitoring on that relationship.

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

Administrators and self-administered investment institutions may rely on 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;

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

The following steps must be taken by administrators and self-administered investment institutions when relying on intermediaries or other third parties to perform aforementioned elements of the CDD process[21]:

- 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

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

- 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, administrators and self-administered investment institutions must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. A jurisdiction is adequately supervised when its Mutual Evaluation Reports [22] discloses less than 10 "Non Compliant or Partially Compliant" ratings regarding the 16 "key and core[23]" FATF Recommendations.

If administrators and self-administered investment 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 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.

In case the administrators and self-administered investment institutions rely on other third parties for the complete CDD process (in this case the CDD process has been outsourced), than a written contractual arrangement is required and must be readily available for the Central Bank when conducting on-site visits.

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

Furthermore, administrators and self-administered investment institutions are encouraged to perform antecedent screening on persons subject to CDD. This could be done by e.g. searching the internationally accepted authoritative lists on the internet.

Redemptions/Sales

In the case of a redemption or surrender of an investment (wholly or partially), the administrator or self-administered investment institution will be considered to have taken reasonable measures to establish the identity of the investor where payment is made either:

- to the registered owner of the investment by means of a check crossed "Account Payee"; or
- to a bank account held (solely or jointly) in the name of the registered owner of the investment with a financial institution by any electronic means effective to transfer funds.

Bearer shares[24]

Bearer shares confer rights of ownership in an institution upon the physical holder of the shares. Often times the identity of the investor is not recorded when the share is issued and transferred or cannot be obtained by entities subject to customer due diligence obligations and enforcement

[22] 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.

[23] 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*

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

authorities. The high level of anonymity they offer makes them particularly attractive to money launderers and terrorists. For supervised investment institutions in Curaçao and Sint Maarten, the Central Bank discourages the issuance of bearer shares, except for the shares which are listed on public securities exchanges. The financial service providers in Curaçao and Sint Maarten must always know the beneficial owners of bearer shares of companies to whom they render services, which are not listed on a public securities exchange. Certificate of bearer shares must be held in custody by the administrator or self-administered investment institution or a party assigned by the administrator or self-administered investment institution.

Hold mail and c/o Addresses

The investor may at times request the administrator or self-administered investment institution to keep all his mail at the administrator's office for storage or for collection on a later date. Although such a request does not necessarily imply the conduct of money laundering activities, the administrator must closely monitor the activities of such investors.

Source of Funds Declaration Form

As part of the CDD process, administrators and self-administered investment institutions are required to request the (prospective) investors in the investment institutions or their representatives to fill out and sign the Source of Funds Declaration Form[25] enclosed in Appendix 2 to these Provisions and Guidelines for initial investments. With respect to subsequent investments, administrators and self-administered investment institutions are required to request the Source of Funds Declaration Form only for investors that are classified as high risk according to the Risk-based Approach addressed in the next section. The Source of Funds Declaration Forms must be kept on file.

Risk-based Approach

(a) Risk classification

The administrator and self-administered investment institution must develop risk profiles for all their clients, being investment institutions and/or investors, to determine which categories of clients expose the administrator and self-administered investment institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a client, must take place after the CDD information mentioned above has been received. The risk profile must comprise minimally the following possible categories: low, medium and high risk. Administrators and self-administered investment institutions must apply CDD requirements to existing clients and may determine the extent of such measures on a risk- sensitive basis depending on the type of client, business relationship, or transaction.

Administrators and self-administered investment institutions must at least consider the following risk categories while developing and updating the risk profile of a client: (i) client risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk.

(i) Client risk: It is important for an administrator and self-administered investment institution to assess the type of client and the nature and scope of the business activities of the client.

The types of clients or business activities that indicate a higher risk include:

- Politically exposed persons (PEPs) and their families and associates;
- Cash and cash equivalent intensive businesses, such as money remitters, casinos, (internet) gambling businesses;

[25] See Appendix 2.

- Clients engaging in business activities regarded as sensitive, such as pornography, arms trading and the provision of military security services;
- Clients where the structure or nature of the entity or relationship makes it difficult to identify and verify the true owner or controlling interests;
- Charities and non-profit-organizations which are not subject to monitoring or supervision;
- Financial institutions and designated non-financial businesses and professions that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised;
- Clients where there is no commercial rationale for a client making use of the services offered by the administrator and self-administered investment institution that request undue levels of secrecy, or where it appears that an audit trail has been deliberately broken or unnecessarily layered;
- Material change takes place in the way the account is operated;
- Client documentation standards change substantially; and
- Determination of lack of or insufficient information about an existing client.

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

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

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

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

(iv) Delivery Channels Risk: This particular risk category deals with the manner in which the administrator and self-administered investment institution establishes and delivers products and services to its clients. While assessing the vulnerabilities posed by the distribution channels of its products and services, the administrator and self-administered investment 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; and
- Pooled relationships with intermediaries, which due to the anonymity provided by the co-mingling of assets or funds belonging to several clients by the intermediary, tend to be more vulnerable.

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

(a) Enhanced CDD for high risk categories of customers

Administrators and self-administered investment 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.

Administrators and self-administered investment institutions must not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

The Administrators and self-administered investment 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, administrators and self-administered investment institutions must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, administrators and self-administered investment 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[26]" FATF Recommendations in their Mutual Evaluation Report (of the FATF, IMF or FSRB [27]) can be considered high risk jurisdictions when they have not shown a high level of

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

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

[27] FATF Style Regional Body

commitment to remedy their deficiencies in a reasonable timeframe. The FATF and some FSRBs issue statements on these countries.

Administrators and self-administered investment 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. If these business relationships and transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions must, as far as possible, be examined, and written findings must be available for at least five years to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors). If unusual transactions are detected, then these must be reported to the FIU/MOT.

Furthermore, administrators and (self) administered investment 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 administrators and self-administered investment institutions are 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 administrators and (self) administered investment institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that are in compliance 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

Administrators and self-administered investment institutions 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 administrator and self-administered investment institution to have adequate procedures for its personnel in place. These procedures must cover:

a) the recognition of unusual transactions;
b) the acceptance and 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 (self-) administered investment institution's known legitimate business activities. Based on the NORUT legislation, objective and subjective indicators have been established by means of which investment institutions and administrators must assess if a customer's transaction qualifies as an unusual transaction. The indicators for investment institutions and administrators are listed in Appendix 3 and 4, respectively. Furthermore, a list is prepared containing some examples of suspicious investment related transactions which are relevant for administrators and (self-) administered investment institutions and may serve them as guidance in their effort to assess whether certain transactions conducted must be considered unusual. The list is annexed to this guideline (Appendix 5).

Administrators and (self-) administered investment institutions 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. Administrators and (self-) administered investment institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing and keep these findings for at least five years to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors).

In this context, the employees of the administrator or self-administered investment institution must not only focus on the establishment of a relationship, but also on other aspects such as subsequent transactions, the frequency of the transactions, duration of the investments, the acceptance of unfavorable terms on part of the (prospective) investor or (prospective) investment institution, and where applicable, the relationships of the investment institution serviced and/or the investment institution's engagement in other business activities.

Administrators and self-administered investment institutions with advanced computer information systems are encouraged to develop special programs to select objectively defined unusual transactions. Furthermore, management must provide its staff with specific guidelines and training to recognize and document adequately the unusual transactions.

<u>Wire transfer</u>
Internationally, wire transfers are increasingly becoming a method to launder funds from illegal sources and for illegal activities or to finance terrorism. Administrators and self-administered investment institutions must be extremely vigilant when proceeds are transferred from or to accounts with financial institutions licensed in jurisdictions where anti-money laundering measures and practices are known to be absent and/or inadequate.

Based on FATF Special Recommendation (SR) VII [28], administrators and self-administered investment institutions must include accurate and meaningful originator information (at least the name, address and account number) on funds transfers within or from Curaçao and Sint Maarten, and related messages that are 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[29]. Also, further scrutiny is required and reporting to the Unusual Transactions Reporting Center (FIU/MOT)[30] must be considered.

Re. :b) The documentation of unusual transactions

To guard against money laundering and terrorist financing, it is important for administrators and self-administered investment institutions to provide an audit trail for suspicious/unusual funds or transactions. This must be done through documentation of all detected and reported unusual transactions.

Re. :c) Reporting of unusual transactions

Administrators and self-administered investment institutions must have clear procedures which are communicated to their personnel for the reporting of unusual transactions.

There may be circumstances where an administrator or self-administered investment institution declines to establish a business relationship with a potential client or refuses to render additional administrative services to an existing client because of serious doubts about the client's or its representative's "bona fides" and potential criminal background. While all decisions must be based on normal business criteria and the administrator's or self-administered investment institution's internal policy to guard against money laundering and terrorist financing, it is important for the administrator or self-administered investment institution to provide an audit trail for suspicious funds and report all the unusual (intended) transactions as soon as possible to the FIU/MOT.

Internal reporting

The obligation to report internally, without any undue delay, lies on anyone who renders (financial) services by virtue of his profession or in the ordinary course of his business. All transactions as mentioned in the list of indicators of the NORUT must be referred to the designated officer(s), in a format which contains at least the data as stipulated by law.

Whenever available, additional documents such as copies of the identification documents, account statements, checks and account ledgers records must also be submitted as supplements. The designated officer(s) must keep an adequate filing system for these records. If internally reported transactions are not reported to the FIU/MOT by the compliance officer, the reasons therefore must be adequately documented and signed off by this officer and/or by management.

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

[29] Administrators and self-administered investment institutions must observe the Interpretative Note to SR VII and apply its relevant parts.

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

External reporting

Administrators and self-administered investment institutions must cooperate fully with the national law enforcement authorities. A report must be prepared of all unusual transactions by the designated officer(s) for external reporting purposes. The report must be submitted to senior management for review of compliance with existing regulations. The administrator and self-administered investment institution must keep copies of all reports submitted to the FIU/MOT on file. 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 administrator or self-administered investment institution and its directors, officials and employees do not warn their clients when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the compliance staff of the administrator or self-administered investment institution on them;
- the administrator or self-administered investment institution and its directors, officials 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 exempt list for the reporting of unusual transactions is permitted. However, the established laws and regulations, do not allow any exemptions on the reporting obligation of financial service providers.

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

Each administrator and self-administered investment institution must formally designate one or more senior officer(s) to be responsible for the deterrence and detection of money laundering and terrorist financing with 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 policies and procedures of the administrator or self-administered investment institution;
- 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 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 compliance officer(s). The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.

The compliance officer(s) must have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information.

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

Administrators and self-administered investment institutions must maintain an adequately resourced and independent audit function to test compliance (including sample testing) with their policies, procedures and controls. The independent testing must be conducted at least annually by the internal audit department or by an outside independent party such as the external auditor of the administrator or self-administered investment institution. These tests must include:

- evaluation of the anti-money laundering and terrorist financing manual;
- file reviews of the (self-)administered investment institutions;
- 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
- assessment of the adequacy of the record retention system.

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

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

Administrators and self-administered investment institutions 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 company must screen its employees on criminal records.

Administrators and self-administered investment 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 must at least include:

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

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

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

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

In order for an administrator or self-administered investment institution to be able to demonstrate compliance with the aforementioned guidelines with respect to staff training, it must at all times maintain records which 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 on-going training plan.

II.2.B Detection and deterrence of terrorist financing

Administrators and self-administered investment institutions must take into account the characteristics including types of transactions listed in the annex 1 to the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing"[31]. Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing. In addition, administrators and self-administered investment 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 or referred to in:

- Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- annex 2[32] of the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing";
- the listing[33] of the Office of Foreign Assets Control (OFAC)[34] or of other national authorities; and
- the lists issued by the United Nations[35].

Supervised institutions must continuously compare the names in 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 to the FIU/MOT and the Central Bank immediately.

In addition, if an administrator and self-administered investment 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, administrators and self-administered investment institutions must be vigilant in the abuse of non-profit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII [36] and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices[37].

[31] The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
[32] The full document can be consulted located at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf.
[33] The list is located on FINCEN's website at
http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html.
[34] See appendix 1for the definition or explanation or summary.
[35] The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.
[36] Special recommendation VIII refers to measures with respect to vulnerable nonprofit organizations.
[37] The full document can be consulted at http://www.fatf-gafi.org/pdf/SR-8NPO/en.pdf.

II. 3 Record-keeping

Administrators and self-administered investment institutions must ensure compliance with the record-keeping requirements contained in the relevant money laundering and terrorist financing legislation. The investigating authorities need to ensure a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing.
Where appropriate, administrators and self-administered investment institutions must consider retaining certain records e.g. customer identification, account files, and 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 weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. However, when practicable, the following document retention terms are suggested:

- All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction takes place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior.
- Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued.
- Administrators and self-administered 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 administrators and self-administered investment institutions must be prepared to provide information or documentation on their money laundering and terrorist financing policies and deterrence and detection 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 administrator or self-administered investment institution must be prepared to make available 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 his/her designated job-description;
- records of reported unusual transactions;
- unusual transactions on which closer investigation was required;
- completed source of funds declarations;
- schedule of the training provided to the institution's personnel regarding money laundering and terrorist financing;

- assessment reports on the institution's policies and procedures on money laundering and terrorist financing by the internal audit department or the institution's external auditor; and
- documents on system tests such as the customers' transactions data and files, overview of the origin and destination of wire-transfers and other transfers to and from the accounts, and other relevant information; and
- required copies of identification documents.

III OFFENCES AND SANCTIONS IN THE NORUT AND THE NOIS

An administrator or self-administered investment institution that does not comply with the compulsory AML/CTF 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 administrator and self-administered investment 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 the administrator and self-administered investment 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 amount of a penalty 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.

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[38]
- Article 12, paragraph 2[41]
- Article 13[43]
- Article 22h, paragraph 3[46]

NOIS

- Article 2, paragraph 1, 2[39], and 5[40]
- Article 3[42]
- Article 5, paragraph 1 through 4[44], and 6[45]
- Article 6[47]
- Article 7[48]
- Article 8[49]
- Article 11, paragraph 3[50]

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

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

The Central Bank will indicate in the Decree[51] to impose a penalty the term in which the violator can execute a mandate without a penalty being forfeited.

The amount due can be collected by way of a writ of execution, increased by the costs falling on the collection. The writ of execution shall be served on the violator by means of a bailiff's notification and will produce an entitlement to enforcement[52].

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[53].

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 abovementioned article 22h, paragraph 3, NORUT and article 11, paragraph 3, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum administrative fine of NA*f.* 1,000. A list of these requirements is included in Appendix I to 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 the intention to impose a penalty, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term[54].

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

The Central Bank will refer an offence for criminal investigation or prosecution to the law enforcement in circumstances where the offender emphatically refuses to comply with the compulsory requirements set out in the NORUT and/or NOIS.
In case of violation of or acting contrary to the provisions in the relevant articles mentioned in article 23 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

[51] Decree:"Beschikking" in Dutch
[52] Article 22a, paragraph 3 through 5, NDUT and article 9, paragraph 3 through 5, NDSP
[53] See article 3, paragraph 1 of the NDUT and article 3, paragraph 1 of the NDSP
[54] Article 22b, paragraph 3, NORDUT and article 9a, paragraph 3, NDSP

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 onsite 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[55].

[55] Article 4, paragraph 3, of the NDUT and NDSP, respectively

Appendix 1: Glossary /Definitions

In this document the following abbreviations and definitions are used:

Bearer shares
Shares issued in bearer form. Contrary to registered shares, the ownership of the bearer shares is not registered in a register maintained by the issuing entity. A bearer share is owned by the person who possesses it and the transfer takes place by the physical handing over of the security.

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

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

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

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

Client or customer or investor
In general sense, a client (customer) is defined in article 1, sub c of the NOIS, as anyone to whom a service, as defined in article 1, sub b of the NOIS is rendered.
More specifically, a client or customer of an investment institution or administrator is respectively defined as follows:

Client/investor of an Investment Institution: the participant who or which owns participating interests in the investment institution, as defined in article 1 (d) of the National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137).

Client of an Administrator: the investment institution to which the administrator provides administrative services. The term "client" in the context of an administrator does not only refer to the administered investment institution but also to the applicant upon whose instructions the business relationship with the administrator is established. The administrative services are described in article 1 (g) of the National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137).

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

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

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

Identify means to establish the identity of someone.

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

Misdemeanour is a minor crime which is punishable

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

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.

Self-administered investment institution
An investment institution whose administrative services, particularly its transfer agency services and/or investor relation services, have not been outsourced to a third party. These administrative services are performed by the investment institution's own staff.

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

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

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

Third party means an independent separate legal entity or person.

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: The Source of Funds Declaration Form

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 investment institution/the administrator.

2) ……I declare that the funds totaling _____, which

are used to purchase shares/ units/ interest in _____
(name of investment institution) represent funds obtained by the undersigned from the following source(s):

3) Consent is hereby given to this investment institution or administrator to disclose this transaction to those institutions which are legally entitled to receive the information contained here in.

Customer's name

Customer's address

Customer's Signature

Appendix 3: Indicators for Investment 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 to the police or the judicial authorities must also be reported to the Reporting Office.

B. Cash transactions:

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

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

A. *Probable money laundering transactions:*

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

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

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

a) transaction atypical of investor;
b) investor asks for a check in the name of a third party in the event of total or partial sale of his investment in the investment institution;
c) checks endorsed to the investor for the payment of the purchase of an investment in the investment institution by the investor;
d) identification problems;
e) unusual pattern of purchase(s) and sale(s) by the investor of investments in the investment institution;
f) unusual condition offer.

*C. Giro-based transactions of NA*f*. 5,000,000.00 and higher that comply with two or more of the following indicators:*

a) identification problems;
b) unusual pattern of purchase(s) and sale(s) by investor of investments in the investment institution;
c) transactions atypical of investor;
d) unusual condition offer;
e) payment of an investment in the investment institution takes place by means of several successive payments instead of one payment;
f) payment of the proceeds of complete or partial sale of an investment has to take place in several successive transactions at the request of the investor;
g) proceeds of the investment in the event of complete or partial sale are not transferred to the investor's own account;
h) transfer of the proceeds of the complete or partial sale of the investment in the investment institution without stating the beneficiary or under a code name;
i) transfer to the investment institution for the payment of the investment without stating the principal, or under a code name.

D. *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: Indicators for Administrators

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 terrorist activities to the police or the judicial authorities must also be reported to the Reporting Office.

B. Cash transactions:

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

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

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

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

B. Dodging the marginal amount:

Preference of the investment institution or investor for transactions under the marginal amount in which case there is reason to assume that it/he wants to avoid reporting in doing so.

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

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

a. no explainable legal objective or no visible relation with (business) operations;
b. transactions atypical of the investment institution;
c. transactions atypical of the investor;
d. checks endorsed to the investment institution;
e. checks endorsed to the investor for the payment of the sale of an investment in the investment institution by the investor;
f. identification problems;
g. investor asks for a check in the name of a third party in the event of a complete or partial sale of his investment in the investment institution;

h. unusual pattern of purchase(s) and sale(s) by the investor of investments in the investment institution;
i. unusual number of accounts;
j. unusual condition offer.

D. Giro-based transactions:

1. Transactions of NA*f*. 10,000,000.00 and higher that comply with two or more of the following indicators:
a. identification problems;
b. unusual pattern of purchase(s) and sale(s) by the investor of investments in the investment institution;
c. transaction atypical of investor;
d. transaction atypical of investment institution;
e. unusual condition offer;
f. payment of an investment in the investment institution takes place by means of several successive payments instead of one payment;
g. payment of the proceeds of complete or partial sale of an investment has to take place in several successive transactions, whether or not to the same beneficiary, at the request of the investor;
h. proceeds of the investment in the event of a complete or partial sale are not transferred to the investor's own account;
i. transfer of the proceeds of the complete or partial sale of the investment in the investment institution without stating the beneficiary, or under a code name;
j. transfer to the investment institution for the payment of the investment without stating the principal, or under a code name.

Appendix 5: Examples of unusual investment related transactions

The examples mentioned below may apply to both administrators and self-administered investment institutions. The administrators and self-administered investment institutions must be extra vigilant for the unusual transactions mentioned below. A client that displays the behavior mentioned below, is not necessarily involved in money laundering or terrorist financing activities. However, the examples must serve as general indicators which must prompt the administrator or self-administered investment institution to closer monitor the client's behavior. Furthermore, the examples must promote awareness and stimulate the deterrence of money laundering and terrorist financing within the administrator or self-administered investment institution.

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

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

c) Buying and selling of the shares in an investment institution with no discernible purpose or in circumstances which appear unusual.

d) A client whose approach to investment risk and return is unusual. The client may be willing to take significantly more risk than the normal investor for the same expected rate of return.

e) A client who churns its investments or indulge in early surrender of his or her participating interests into the investment institution despite penalties or exit charges.

f) A number of purchased transactions by the same counterparty in small amounts relating to the same security, which are then sold in one transaction, the proceeds being credited to an account different from the original account.

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

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

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

j) The use by a client of a securities brokerage firm as a place to hold funds that are not being used to trade in securities.

k) A client who deals with a securities broker only in cash or cash equivalents rather than through banking channels.

l) A client who prefers to use a securities broker's client money account as a bank account and who instructs a broker to perform certain duties on his or her behalf, such as wire transfers and safe deposits in the broker's own name.

m) The entry of matching buys and sells in particular securities ("wash trading"), creating the illusion of trading. Such wash trading does not result in a bona fide market position, and might provide "cover" for a money launderer or terrorist.

n) Wash trading through multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts. Transfers of positions between accounts that do not appear to be commonly controlled also could be a warning sign.

o) Third party payments in case of subscriptions and or redemptions.

The following activities must require extra care by particularly administrators

In addition to the above-mentioned examples, administrators in particular must be alert for the following activities exhibited by their administered investment institutions that may be related to money laundering and terrorist financing activities.

a) Frequent and excessive switching of administrators by the investment institution.

b) The administered investment institution issues bearer shares.

c) Bearer or unregistered securities/near-cash instruments are offered in settlement of transactions.

d) The investment institution that is being administered is not regulated by any supervisory authority.