CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Insurance Companies and Intermediaries (Insurance Brokers)

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 & CTF, revised these Provisions and Guidelines.

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

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

I NATURE AND LEGAL BASIS OF THE PROVISIONS

The Central Bank of Curaçao and Sint Maarten (hereafter "Central Bank") is committed in the fight against money laundering and terrorist financing. Because of this commitment, and Curaçao and Sint Maarten being a member of both the Financial Action Task Force on Money Laundering (FATF)[1] and the Caribbean Financial Action Task Force (CFATF)[2], a comprehensive framework has been introduced 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 Insurance Companies and Intermediaries (Insurance Brokers) 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;

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

(a) The Code of the Criminal Law (Penal Code) (N.G[3]. 2011, no. 48);
(b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no 65 (N.G. 2010, no 41) (NORUT);
(c) The National Decree containing general measures on the execution of articles 22a, paragraph 2, and 22b, paragraph 2, of the National Ordinance on the Reporting of Unusual Transactions (National Decree penalties and administrative fines for reporters of unusual transactions)(N.G. 2010, no. 71);
(d) The National Ordinance on Identification of Clients when rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no 66 (N.G. 2010, no 40) (NOIS);
(e) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services (National Decree containing general measures on penalties and administrative fines for service providers) (N.G. 2010, no. 70);
(f) Ministerial Decree with general operation of May 21, 2010, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Decree Indicators Unusual Transactions) (N.G. 2010, no. 27);
(g) Ministerial Decree with general operations of March 15, 2010, implementing the National Ordinance on Identification of Clients when Rendering Services (N.G. 2010, no. 11);
(h) Ministerial Decree with general operation of March 15, 2010 for the execution of the NORUT (N.G. 2010, no. 10)
(i) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93)
(j) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74).
(k) National Decree providing for general measures, of August 8th, 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

[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.

supervisors under the National Ordinance on the Identification of Customers when Providing Services); and

(l) National Decree Providing for general measures, of August 8th, 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 the National Ordinance on the Reporting of Unusual Transactions).

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

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

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

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

I.1 Money laundering

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

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

A simple transaction may be just one part of a sophisticated web of complex transactions which are set out and illustrated below. Nevertheless, the basic fact remains that the earliest key stage for the detection of money laundering operations is where the cash first enters the financial system.

Stages of money laundering

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

I.3 Risk-based Approach

Based on the FATF recommendations, particularly those related to (a) customer due diligence (Recommendations 5, 6, 8 and 9), (b) businesses' internal control systems (Recommendation 15), and (c) approach of oversight/monitoring (Recommendation24), insurance companies and intermediaries are allowed to apply a Risk-based Approach ("RBA"). By adopting a RBA, it is possible for insurance companies and intermediaries to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.
This entails that although all clients must be subjected to the minimum due diligence standards outlined in section II.2.A of these Provisions and Guidelines, clients identified by the institution as high risk must be subject to enhanced customer due diligence while low risk clients may be subject to simplified/reduced customer due diligence as outlined in section II.2.A .

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

[4] The full document can 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.4 Sanctions

Insurance companies and intermediaries are required to comply with the compulsory requirements set out in the NORUT and/or NOIS legislations and the provisions and guidelines issued under these laws.

During its on-site examinations, the Central Bank will assess 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 INSURANCE COMPANIES AND INTERMEDIARIES

This Chapter addresses the relevancy to detect and deter money laundering and terrorist financing for insurance companies and intermediaries, followed by a description of some policies and procedures for insurance companies to detect and deter money laundering and terrorist financing. The chapter is concluded with a listing of the information and documentation respective relevant policies and procedures which those institutions must provide to the Central Bank.

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

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, criminals have moved from banks to non-banks, such as insurance companies to launder the proceeds derived from criminal activity.

Although its vulnerability is not regarded to be as high as for other sectors of the financial industry, the insurance business is considered to be a possible target for money launderers and terrorists as they seek to respectively launder their funds derived from criminal activities and finance their terrorist activities.

The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, payments system and contract law.

Examples of the type of life insurance contracts that are vulnerable as a vehicle for laundering money are investment policies, such as:

- unit-linked or with profit single premium contracts;
- purchase of annuities;
- lump sum top-ups to an existing life insurance contract; and
- lump sum contributions to personal pension contracts.

When a life insurance policy matures or is surrendered, funds become available to the policy-holder or other beneficiaries. The beneficiary to the contract may be changed to others - possibly against payment - before maturity or surrender, in order to benefit from any payments that are made by the insurance company and intermediary to the new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions and will often have their origins elsewhere in the financial services system. Because of their investment nature, unit linked policies, sale of second-hand endowment policies and viatical[6] contracts are the contracts which are more subject to abuse.

It is therefore imperative that all insurance companies and intermediaries be constantly vigilant in detecting and deterring criminals from making use of them for money laundering and terrorism financing purposes. Public confidence in insurance companies and intermediaries and hence their stability can be undermined by adverse publicity as a result of the unwittingly use of insurance

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

companies and intermediaries by criminals for the entering of insurance contracts with funds derived from criminal activity.

If insurance companies and intermediaries do not establish and adhere proper policies and procedures, they may unwittingly be used by criminals for the entering into or mediation of contracts from criminal activities and expose themselves to adverse publicity and to losses resulting from fraud.

The NORUT requires that each financial institution rendering financial services, including life insurance companies, report any unusual transactions thereby made or proposed, to the Unusual Transaction's Reporting Center (FIU) without delay. The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties (MOT).
The financial services as mentioned previously are defined in Article 1 of said ordinance and include among others: the entering into a life insurance contract as also the rendering mediation in connection therewith and the distribution on account of a life insurance contract. The act further established an Unusual Transactions Reporting Center to collect process and analyze the obtained information.

These Provisions and Guidelines are aimed at life insurance business which is the predominant type within the insurance sector being used by money launderers.

In this context, the Central Bank urges insurance companies and intermediaries to implement effective policies and procedures to ensure that all (prospective) policyholders are properly identified and that transactions that appear not to be legitimate be discouraged.

Insurance intermediaries (Insurance brokers)
Intermediaries – independent or otherwise – are important for distribution, underwriting and claims settlement. They are often the direct link to the policyholder and therefore, intermediaries must play an important part in anti-money laundering and the prevention of financing of terrorism. The same principles that apply to insurance companies must generally apply to the insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not perform the necessary procedures, or who fails to recognize or report information regarding possible cases of money laundering or the financing of terrorism.

Although insurance intermediaries have their own legal responsibility and obligations (they have to comply with the National Ordinance Identification when Rendering Services, N.G. 2010, no 40), customer due diligence remains the responsibility of the insurance company involved. The intermediaries themselves could have been set up to channel illegitimate funds to the insurers.

II.2 Policy statement

Each insurance company's Supervisory Board of Directors[7] and Management[8] must have issued a formal statement of policy which clearly expresses the institution's commitment to combat the abuse of its facilities, financial products, and services for money laundering and terrorist financing purposes.

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

The policy statement must state the insurance company's intention to comply with current anti-money laundering and terrorist financing legislation and guidelines, in particular the laws and guidelines regarding the identification of customers and the reporting of unusual transactions.

The policy statement[9] 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 subsequently keep adequate records of these 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 policies and procedures by the insurance company'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 employee's awareness and knowledge in the field of money laundering and terrorist financing prevention and detection.

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

[7] See appendix 1 for the definition or explanation or summary.
[8] See appendix 1 for the definition or explanation or summary.
[9] In the design, update and implementation of their policy statement, the Central Bank encourages insurance companies 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", the "Special Recommendations on Terrorist Financing" of the Financial Action Task Force (FATF) and the "Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities" of the International Association of Insurance Supervisors (IAIS). The relevant documents are located at http://www.fatf-gafi.org and at http://www.iaisweb.org

II.2.A Detection and deterrence of money laundering

Pursuant to the NOIS the life insurance companies and intermediaries must ascertain and record the identity of their customers. Furthermore, they must inquire whether or not the party who pays the premium is also the one to whom the distribution will be made.
According to the NOIS, identification must occur in the following cases:

1. When entering into life insurance contracts as referred to in article 1, paragraph 1, sub a of the National Ordinance on the Supervision of the Insurance Industry, and also when rendering mediation in connection therewith at a premium as referred to in article 1, paragraph 1, section c, of mentioned ordinance in excess of the amount stipulated by the Minister. The amount as stipulated by Ministerial Decree (N.G. 2010, no. 11) is fixed at NA*f*. 2.500 per annum if it concerns a periodical premium, and at NA*f*. 5.000 if it concerns a non-recurring premium.

2. When making a distribution on account of a life insurance contract as referred to in article 1, paragraph 1, sub a of the National Ordinance on the Supervision of the Insurance Industry which is in excess of the amount stipulated by the Minister. This amount is fixed at NA*f*. 20.000 by Ministerial Decree (N.G. 2010, no. 11).

Insurance companies and intermediaries 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

Insurance companies and intermediaries have the obligation to determine the true identity of their (prospective) personal and corporate clients/customers [10], before entering into insurance contracts with them. Internal procedures must also clearly indicate for which contracts prospective policyholders or their representatives must identify themselves and which identification documents are acceptable. Insurance companies and intermediaries must develop clear customer acceptance policies and procedures, including a description of the types of customers that are more likely to pose a higher than average risk to the company (refer to appendix 2 for other risk factors). The policy must ensure that transactions will not be conducted, business is not commenced and that insurance contracts are not entered into with (prospective) customers who fail to provide satisfactory evidence of their identity. Insurance companies and intermediaries must not offer insurance to customers or for beneficiaries that obviously use fictitious names or are kept anonymous. The latter being the case with so-called bearer policies.

Customer due diligence measures that must be taken by insurance companies and intermediaries include:

- identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information;
- for all customers, the insurance company and intermediary must determine whether the customer is acting on behalf of another person, and must then take reasonable steps to obtain sufficient identification data to verify the identity of that other person;
- identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurance company and intermediary are satisfied that they know who the beneficial owner is. For legal persons and arrangements this must include

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

insurance companies and intermediaries taking reasonable measures to understand the ownership and control structure of the customer;
- obtaining information on the purpose and intended nature of the business relationship prior to offering their service; and
- conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurance companies' and intermediaries' knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. Thus the efforts to "know your customer" must continue even after the client has been identified.

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

Examples of when this action may be appropriate are when:
(a) a transaction of significance takes place;
(b) a material change takes place in the way the insurance contract is dealt with;
(c) customer documentation standards change substantially, and
(d) the institution becomes aware that it lacks sufficient information about an existing customer.

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

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

If claims, commissions, and other monies are to be paid to persons (including partnerships, companies, etc) other than the policyholder, then the proposed recipients of these monies must be the subjects of identification and verification. The insurance companies and intermediaries must be required to be alert to the implications of the financial flows and transaction patterns of existing policyholders, particularly where there is a significant, unexpected, and unexplained change in the behavior of the policyholders (e.g. claims notifications, early surrender requests and policy alterations, including changes in beneficiaries; see appendix 2 for more triggers). The company must be extra vigilant to the particular risks from the practice of buying and selling second hand endowment policies, as well as the use of single premium unit-linked policies. The company must check any reinsurance or retrocession to ensure the monies are paid to bona fide re-insurance entities at rates commensurate with the risks underwritten. Also, more extensive due diligence must be conducted for high risk customers, including politically exposed persons (PEPs)[11], their families and associates. The institutions' decisions to enter into such business relationships must be taken at their senior management level.

The institution must make reasonable efforts to ascertain that the customer's source of wealth is not from illegal activities. Insurance companies and intermediaries must not accept or maintain a business relationship if they know or must assume that the funds are derived from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations. Additionally, insurance companies and intermediaries are

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

encouraged to conduct enhanced ongoing monitoring on PEPs who hold prominent public functions domestically.

Insurance companies and intermediaries 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.

The required information regarding the customer, the authorized identification documents and the nature of the transaction is legally described and must therefore be adequately documented.

An important objective for insurance companies and intermediaries is to ensure that documents, data or information collected under the customer due diligence process (know your customer policy) is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

The requirement on customer due diligence must apply to all new customers as well as –on the basis of materiality and risk- to existing customers. As to the latter the insurance company and intermediary must conduct due diligence at appropriate times. In insurance, various 'trigger events' occur after the contract date and indicate where due diligence may be applicable. These trigger events include claims notification, surrender requests and policy alterations including changes in beneficiaries.

Hence, the introduction of a checklist for the identification and/or transaction information of customers and a centralized record keeping system must be in place.

Simplified/reduced CDD

1. 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 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 insurance company is allowed to apply simplified or reduced CDD measures when identifying the identity and verifying the identity of the customer.

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.

A). Identification of resident and non-resident personal customers

Pursuant to article 3 of NOIS[12], the identity of a **resident** and a **non-resident** personal customer must be established through one of the following documents:

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

Resident customers

In addition, the identity of a **resident** customer must be verified when a business relationship is established with the customer. The identity of the customer also must be verified when the insurance company and intermediary have doubts about the veracity or adequacy of the identification data obtained from existing customers. Examples include:

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

Non-Resident customers

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

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

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

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

Insurance companies and intermediaries must pay special attention to non-resident clients and understand the reasons for which the client has chosen to enter into an insurance contract in the foreign country.

Non-face-to-face customer

Although a non-face-to-face customer can produce the same documentation as a face-to-face customer, it is more difficult to verify his or her identity. Therefore, in accepting business from non-face-to-face customers an insurance company and an intermediary should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk. Certification by appropriate authorities and professionals of the document must be provided.

Examples of risk mitigating measures:

- Requisition of additional documents complement those which are required for face-to-face- customers;
- Independent contact with the customer by the insurance company or intermediary;
- Third party introduction, e.g. by an intermediary subject to the criteria established in the paragraph " Reliance on intermediaries and third parties"; and
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

B) Identification of corporate customers

Corporate accounts are one of the more likely vehicles to be used for money laundering purposes. Therefore, it is important to identify the nature of the business, account signatories, and the (ultimate) beneficial owner(s) [13]. Insurance companies and intermediaries must also obtain personal information on the managing and/or supervisory directors. Copies of the identification documents of all account signatories, including the directors with signing authority on the corporate client's accounts, must be kept on file. The procedures for the identification of personal customers must be applied for the mentioned account signatures' director(s) and all (ultimate) beneficial owners holding a qualifying interest in the company. Insurance companies and intermediaries must ascertain the identity of corporate customers based on reliable identification documents, with preference for originals and official documents attesting to the legal existence, and structure of a company or legal entity. The identity, existence and nature of the corporate customer must be established with the aid of a certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.

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

The existence and nature of the business must be legally identified for domestic companies through:

- A certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domicile, or with the aid of an identification document to be drawn up by the service provider.
  The extract or the identification document must contain at least the information stipulated by the Minister in Article 6 of the Ministerial Decree (N.G. 2010, no. 11).

Management may require additional information to be provided for these companies such as:

- shareholders' register;
- certificate of incorporation;
- articles of association;
- a list to include full names of all directors, 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 company, together with a designation of the capacity in which they sign;
- financial statements/cash flow statements.

For customers that are legal persons or legal arrangements, insurance companies or intermediaries should:

a. understand the ownership and control structure of the customer and verify that any person purporting to act on behalf of the customer is so authorized, and verify the identity of that person:
b. verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement: and
c. determine who are the natural persons that ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Insurance companies and intermediaries are required to indentify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from reliable sources such that the insurer or intermediary is satisfied that it knows who the beneficial owner is.

Where the above-mentioned requirements are not met, the insurer and intermediary should consider submitting an UTR.

Identification of Politically Exposed Persons

Insurance companies and intermediaries must conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. Insurance companies and intermediaries must implement appropriate risk management systems to determine whether a potential customer, customer or beneficial owner is a politically exposed person (PEP). The institution's decision to enter into business relationships with PEP's must be taken at its senior management level. The institution must make reasonable efforts to ascertain that the PEP 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. Insurance companies and intermediaries must not accept or maintain a business relationship if the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions must obtain senior management's approval to continue the business relationship. Where the financial institution is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring on that relationship.

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

Insurers must include specific clauses in the contracts with their intermediaries. These clauses must include commitments for the intermediaries to perform the necessary customer due diligence measures, granting access to client files and sending (copies of) files to the insurer upon request without delay. The contract could also include other compliance issues such as reporting to the FIU/MOT and insurer in the case of an unusual transaction or activity. It is recommended that insurers use application forms to be filled out by the customers and/or intermediaries that include information on identification of the customer and beneficial owner as well as the method used to verify their identities. Insurers must inform themselves which jurisdictions are considered suitable to rely on business from intermediaries and third parties. The insurer should satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with CDD requirements.

The insurer must undertake and complete its own verification of the customer and beneficial owner if it has any doubts about the third party's ability to undertake appropriate due diligence.

Insurance companies and intermediaries can 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; and
c. obtaining information on the purpose and intended nature of the business relationship.

The following steps must be taken by these companies when relying on intermediaries or other third parties to perform aforementioned elements of the CDD process[14]:

- 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;

[14] In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions, from another financial institution or third party. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers.

- 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, insurance companies and intermediaries must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. A jurisdiction is adequately supervised when its Mutual Evaluation Report[15] discloses less than 10 "Non Compliant or Partially Compliant" ratings regarding the 16 "key and core[16]" FATF Recommendations.

If insurance companies and intermediaries rely on 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.

If the insurance companies and intermediaries rely on other third parties for the complete CDD process (in this case the CDD process has been outsourced) then a written service level agreement is required and must be readily available for the Central Bank when conducting onsite visits.

It should be noted that even though the institution can 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 institution relying on the third party.

Risk-based approach

Risk classification
Insurance companies and intermediaries must develop risk profiles for all their customers to determine which categories of customers expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a customer, must take place after the CDD information mentioned above have been received. The risk profile must comprise minimally the following possible categories: low, medium and high risk. Insurance companies and intermediaries must apply CDD requirements to existing customers and may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, or transaction.

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

(i) Customer risk: It is important for an insurance company and intermediary to assess the type of customer and the nature and scope of the business activities of the customer. The types of customers or business activities that indicate a higher risk include:
    - Politically exposed persons (PEPs) and their families and associates;

[15] 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.
[16] 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*

- Customers engaging in business activities regarded as sensitive, such as pornography, arms trading and the provision of military security services;
- Customers 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;
- Transaction of significance which takes place (from time to time);
- Customers where there is no commercial rationale for a customer making use of the services offered by the insurance company and intermediary that request undue levels of secrecy, or where it appears that an audit trail has been deliberately broken or unnecessarily layered;
- Customer documentation standards change substantially;
- Customers where the beneficial owner of the contract is not known (e.g. certain trusts);
- Customers who are introduced through non face-to-face channels;
- Customers who seek early termination of a product (including during the" free look" period)[17], especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third party;
- Customer who transfer the benefit of a product to an apparently unrelated party;
- Determination of lack of or insufficient information about an existing customer;
- Frequent and unexplained movement of accounts/policies/contracts/funds to different insurance companies or other financial institutions; and
- Significant and unexplained geographic distance between residence or business location of the customer and the location where the product sale took place (or the location of the insurer's representative).

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

- Services to conceal beneficial ownership from competent authorities;
- Transactions or services with no apparent legitimate business, economic, tax, or legal reasons;
- The offer by customers to pay extraordinary fees for services which would not ordinarily warrant such a premium;
- Acceptance of payments or receipts from third parties;
- Acceptance of payments made in cash or endorsed money orders or cashier cheques;
- Acceptance of frequent payments outside of a normal premium policy or payment schedule;

[17] A "free look" provision is a contractual provision, which allows a policy owner or annuitant of a life insurance or annuity contract to examine a contract for a certain number of days and return it for a full refund.

- Acceptance to be used as collateral for a loan and/written in a discretionary or other increased risk trust; and
- Product that allow for assignment without the insurer being aware that the beneficiary of the contract has been changed until such time as a claim is made.

(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;
- 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; and
- Life insurance companies and intermediaries should take into account warnings issued by competent authorities about risks applicable to countries or geographic areas, including the specificity as to the particular risks posed.

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

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

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

Enhanced CDD for high risk categories of customers

Insurance companies and intermediaries must conduct enhanced due diligence in all of the high risk cases/circumstances mentioned under the RBA 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. The institution must make reasonable efforts to ascertain that the

customer's source of wealth or income is not from illegal activities. Insurance companies and intermediaries must not accept or maintain a business relationship if the institution knows or must assume that the funds are derived from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

The insurance company and intermediary must ensure that the identification documents of their 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, insurance companies and intermediaries must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, insurance companies and intermediaries are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically. 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

Life insurance companies and intermediaries 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 important for every insurance company to have adequate procedures for its personnel in place. These procedures must cover:

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

Re.: a) Recognition of unusual transactions[18]

An unusual transaction will often be a transaction which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for the type of policy the customer holds. Therefore, the first key to recognize that a transaction or series of transactions is unusual is to know enough about the customer's business.

The insurance company and intermediary must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose for both the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transaction must, as far as possible, be examined; the findings put in writing, and be available to assist competent authorities and auditors. The insurance company and intermediary should keep the findings of examinations on the background and purpose of complex, unusually large and unusual patterns of transactions available for competent authorities and auditors for at least five (5) years.

In this respect, institution's employees must focus on inquiries and application for an insurance policy, but also on other aspects such as premium payments, request for changes in benefits, beneficiaries, duration of the policy, the acceptance of unfavorable terms on part of the prospective policyholder, local or foreign relationships, the financial profile of the applicant and or its business clients and the applicant's engagement in other business activities, etc.

[18] For specific examples of suspicious transactions please refer to Appendix 2.

Money laundering and terrorist financing are not only realized through new business relationships and transactions. Insurance entities must be alert to the implications of the financial flows and transactions patterns of existing policyholders, particularly where there is significant, unexpected and unexplained change in the behavior of the policyholders' account. Whether a transaction is unusual is determined on the basis of established indicators.

Based on the NORUT objective and subjective indicators have been established by means of which life insurance companies must assess if a customer's transaction qualifies as an unusual transaction. Those indicators are listed in Appendix 3.

All institutions must develop special programs to select objectively defined unusual transactions. Moreover, management must provide its staff with specific guidance and training to recognize and document adequately the unusual transactions based on especially the subjective indicators.

Wire transfer

Internationally, wire transfers are increasingly becoming a method to launder funds from (il)legal sources and illegal activities or to finance terrorism. Life insurance companies must be extremely vigilant when premium payments are made or sums are deposited from accounts with banks outside Curaçao and Sint Maarten. If such funds are accepted, suitable identification of the depositor must be obtained. If another party than the policyholder pays, than knowledge about the source of funds must be required through a "Source of Funds Declaration Form" as presented in Appendix 4 of this guideline.

Insurance companies and intermediaries must include accurate and meaningful originator information (at least the name, address and account number if existent, otherwise a unique reference number) on funds transfers on behalf of their clients within or from Curacao and Sint Maarten and related messages that are sent. In case the insurance company or intermediary receives a fund transferred from a third party to the insurance company or intermediary's client, the insurance company or intermediary must ensure that the fund transfer information is accurate and complete. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds[19]. Insurance companies and intermediaries must observe the latest Interpretative Note to SR VII and apply its relevant parts. Also, further scrutiny is required and reporting to the FIU/MOT[20] must be considered.

Correspondent financial institutions

Particular attention must be paid to correspondent services provided to a financial institution licensed in a jurisdiction where the insurance company and intermediary have no physical presence or is unaffiliated with a regulated financial institution, or where anti-money laundering and antiterrorist financing measures and practices are known to be absent and/or inadequate.

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

- fully understand and document the nature of the respondent financial institution's management and business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

[19] Insurance companies and intermediaries must observe the Interpretative Note to SR VII and apply its relevant parts.

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

- ascertain that the respondent financial institution has effective customer acceptance and know-your-customer (KYC)[21] policies and is effectively supervised; and
- identify and monitor the use of correspondent accounts that may be used as payable-through accounts.

Insurance companies and intermediaries must obtain approval from their senior management before establishing new correspondent relationships. Insurance companies and intermediaries establishing correspondent relationships must communicate their documented anti-money laundering and anti-terrorist financing responsibilities to have a clear understanding as to which institution will perform the required measures. Where a correspondent relationship involves the maintenance of "payable-through accounts", insurance companies and intermediaries must be satisfied that:

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

High-risk and non-cooperative jurisdictions.

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

Countries that have 10 or more "Non Compliant (NC) or Partially Compliant (PC)" ratings of the 16 "key and core" FATF Recommendations in Mutual Evaluation Reports can be considered high risk jurisdictions when they have not shown a high level of commitment to remedy their deficiencies in a reasonable timeframe. The FATF and some FSRBs issue statements on these countries.

Insurance companies and intermediaries must give special attention, especially in underwriting and claims settlement to business relations and transactions with other financial institutions, including intermediaries and individuals, companies and other corporate vehicles, from the high-risk and non-cooperative jurisdictions[22]. If insurance companies and intermediaries find that such a transaction is unusual, this must be reported to the FIU/MOT.

Furthermore, insurance companies and intermediaries 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.

New or developing technologies

New or developing technologies can be used to market insurance products. E-commerce or sales through the internet is an example of this. Although for this type of non-face-to-face business verification may be allowed after establishing the business relationship, the insurance company and intermediary must nevertheless complete verification. The insurance companies and

[21] See Appendix 1 for the definition or explanation or summary.
[22] For an update of high-risk and non-cooperative jurisdictions, insurance companies must consult the FATF-website.

intermediaries need to have policies and procedures in place to address the specific risks associated with non-face-to-face business relationships or transactions.

Foreign branches and subsidiaries
Insurance companies 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. Insurance companies and intermediaries must be 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.
Insurance companies 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.

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

Re.: b) Documentation of unusual transactions

There may be circumstances where an insurance company declines to enter into life insurance contracts with a potential customer or refuse to deal with additional requests made by an existing customer because of serious doubts about the individual's "bona fides" and potential criminal background. While all decisions must be based on normal business criteria and the institution's internal policy to guard against money laundering and terrorist financing, it is important for insurance companies to provide an audit trail for suspicious funds and report all the unusual (intended) transactions as soon as possible to the FIU (MOT).

Re.: c) Reporting of unusual transactions

Insurance companies and intermediaries must have clear procedures which are communicated to their personnel for the reporting of unusual transactions.

Internal reporting
The obligation to report internally, without 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, credit/debit slips, checks and account ledgers records must also be submitted as supplements. Nevertheless, management must stipulate the categories of unusual transactions which must also be brought to their attention. The designated officer(s) must keep an adequate filing system for these records. If internally reported transactions are not reported to the FIU/MOT by the institution, the reasons therefore must be adequately documented and signed off by this officer and/or by management.

External reporting
Insurance companies and intermediaries 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 management for its review for compliance with existing regulations. Copies of these reports must be kept by the reporting institution. If an unusual transaction is not authorized by 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 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 insurance company and its Supervisory Board of Directors, management and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the institution's compliance staff on them;
- the insurance company and its Supervisory Board of Directors, management and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.

Exempt lists
In some jurisdictions the use of an exempt list for the reporting of unusual transactions is permitted. However, the established laws and regulations 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 insurance company must formally designate one or more senior officer(s) to be responsible for the deterrence and detection money laundering and terrorist financing. The compliance officer(s) must be able to act independently. The AML/CFT compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

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

- to verify adherence to the local laws and regulations governing the detection and deterrence of money laundering and terrorist financing;
- to organize training sessions for the staff on various compliance related issues;
- to review compliance with the insurance company's policies and procedures;
- to analyze transactions and verify whether any are subject to reporting according to the indicators as mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- to review all internally reported unusual transactions on their completeness and accuracy with other sources;
- to keep records of internally and externally reported unusual transactions;
- to prepare the external report of unusual transactions;

- to execute closer investigation on unusual or suspicious transactions;
- to remain informed of the 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 effort to combat money laundering and terrorist financing to the (Board of) managing directors, including at least the local managing directors.

The above-mentioned responsibilities must be included in the job description of each designated officer. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities. The officer(s) must have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information.

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

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

- evaluation of the institution's anti money-laundering and counter terrorist financing manual(s);
- customers' file review;
- interviews with employees handling transactions and with their supervisors;
- a sampling of unusual transactions 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 the Supervisory Board of Directors, and to the designated officer(s) with a request to take corrective actions by a certain deadline.

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

Insurance companies and intermediaries 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 establish and adhere to proper policies and procedures to screen their employees on criminal records.

Insurance companies and intermediaries 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 issue and of 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 customer is understood;
- the areas of underwriting of new policies or the modification of existing policies; and
- to keep abreast of 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 customers, irrespective of their level of seniority. Similarly, training must also be provided to existing members of the staff who are dealing directly with the public such as cashiers and agents. Also brokers may receive training. 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 existing 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.

For an insurance company 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

Insurance companies and intermediaries must take into account the characteristics including types of transactions listed in annex 1 to the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing[23]. Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing.

In addition, insurance companies and intermediaries must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals (N.G. 2010, no. 93) and entities as mentioned in or referred to in:

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

- the lists issued by the United Nations[24].
- 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[25] to the FATF document: "Guidance for Financial Institutions in Detecting Terrorist Financing"; and
- the listing[26] of the Office of Foreign Assets Control (OFAC)[27] or of other national authorities;

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

In addition, if an insurance company or an intermediary 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, insurance companies and intermediaries must be vigilant in the abuse of non-profit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII [28] and consider the relevant parts of the FATF document: "Combating the abuse of non-profit organizations, International best practices"[29].

II.3 Record-keeping

Insurance companies and intermediaries must ensure compliance with the record-keeping requirements contained in the relevant money laundering and terrorist financing legislation. Insurance companies and intermediaries must ensure that the investigating authorities must be able to identify a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing and be able to establish a financial profile of the suspect policyholder.

Where appropriate, insurance companies and intermediaries must consider retaining certain records e.g. customer identification and business correspondence, and internal and external reports relative to unusual transactions of clients, for longer periods then required under the relevant money laundering and terrorist financing legislation, rules and regulations.

A document retention policy must 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. 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.

[24] The list can be consulted at http://www.un.org/docs/sc/committees/1267/1267listeng-htm.
[25] The full document can be consulted at http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf
[26] The list can be consulted on FINCEN's website at http://www.treas.gov/offices?enforcement/ofac/sanctions/terrorism.html.
[27] See appendix 1 for the definition or explanation or summary.
[28] Special recommendation VIII refers to measures with respect to vulnerable non-profit organizations.
[29] The full document can be consulted at http://www.fatf-gafi.org/pdf/SR-8NPO/en.pdf

- 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. Moreover, records on identification must be kept at least five years following termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

- Insurance companies and intermediaries 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 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 insurance companies and intermediaries 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 insurance company must be prepared to make available:

- its written and approved policies and procedures on money laundering and terrorist financing prevention;
- the name of each designated officer responsible for the institution's overall money laundering and terrorist financing policies and procedures, and her/his designated job-description;
- records of reported unusual transactions;
- unusual transactions on which closer investigation was required or has been executed;
- the 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 institutions policies and procedures on money laundering and terrorist financing by the internal audit department or the institution's external auditor;
- documents on system tests such as the customers' policies, premium payments overview, duration of policies, purchase sums and other relevant information: and
- required copies of identification documents.

III OFFENCES AND SANCTIONS IN THE NORUT AND THE NOIS

A financial 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 insurance company and intermediary that do not or do 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 insurance company and intermediary that do not or do not timely comply with the obligations imposed by or pursuant to article 2, paragraphs 1, 2, 5, article 3, paragraphs1 through 6, article 5, paragraph 1 through 4, articles 6, 7, 8 and article 11, paragraph 3.

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

III.1 Penalties related to the NORUT and the NOIS

The violation of the obligations imposed by or pursuant to the following articles is subject to a maximum penalty of NA*f.* 500,000.

NORUT

- Article 11[30]
- Article 12, paragraph 2[33]
- Article 13[35]
- Article 22h, paragraph 3[38]

NOIS

- Article 2, paragraph 1, 2[31], and 5[32]
- Article 3[34]
- Article 5, paragraph 1 through 4[36], and 6[37]
- Article 6[39]
- Article 7[40]
- Article 8[41]
- Article 11, paragraph 3[42]

[30] Obligation to report unusual transactions
[31] Obligation to identify the client before rendering any service
[32] Obligation to identify the client before rendering any service
[33] Obligation to provide additional information to the Reporting Center
[34] Obligation to establish the identification of the client
[35] Indication how to report unusual transactions
[36] Obligation to identify the representative
[37] Dispensation or exemption of the Minister under certain conditions
[38] Process of reporting of unusual transaction and additional information
[39] Obligation to document the data received
[40] Obligation of record keeping
[41] Prohibition to render services without identification
[42] Process of identification of clients, reporting of unusual transaction and additional information

Based on abovementioned article 22h, paragraph 3, juncto article 22a, NORUT and article 11, paragraph 3, juncto article 9, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum penalty of NA*f.* 500,000. A list of these requirements is included in Appendix I to the Policy Rule on the violations of the NORUT and NOIS legislations and the AML/CFT provisions and guidelines of the Central Bank. It concerns all the provisions that the (financial) institutions or individuals "**mus**t" comply with.

The Central Bank will indicate in the Decree[43] to impose a penalty the term in which the violator may execute a mandate without a penalty being forfeited.

The amount due may be collected by way of a writ of execution, increased by the costs falling on the collection. The writ of execution shall be served on the violator by means of a bailiff's notification and will produce an entitlement to enforcement[44].

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[45].

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 22h, paragraph 3	- Article 6
	- Article 7
	- Article 8
	- Article 11, paragraph 3

Based on the abovementioned article 22h, paragraph 3, juncto article 22b, NORUT and article 11, paragraph 3, juncto article 9a, NOIS the compulsory requirements in the Provisions and Guidelines are also subject to a maximum administrative fine of NA*f.* 1,000. A list of these requirements is included in Appendix I to this Policy Rule. It concerns all the provisions that the (financial) institutions or individuals "**mus**t" comply with.

Before proceeding to imposing a fine, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a fine, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term[46].

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

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

[43] Decree:"Beschikking" in Dutch
[44] Article 22a, paragraph 3 through 5, NDUT and article 9, paragraph 3 through 5, NDSP
[45] See article 3, paragraph 1 of the NDUT and article 3, paragraph 1 of the NDSP
[46] Article 22b, paragraph 3, ND NORUT and article 9a, paragraph 3, ND PFSP

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

Furthermore, if the supervised (financial) institution or individual does not comply with its obligations, even after an increased penalty or administrative fine, the Central Bank may refer the violation for further investigation to the Public Prosecutor, by providing them with the relative documents[47].

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

Appendix 1: Glossary/Definitions

In this document the following abbreviations and definitions are used.

(Ultimate) beneficial owners
Refers to the natural person(s) who (ultimately) own(s) or controls 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.

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/

Client or customer
Pursuant to article 1, sub c of the NOIS, a client/customer is anyone to whom a service, as defined in article 1 sub b of the NOIS, is rendered.

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 Sint Maarten.

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

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

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

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

Misdemeanour is a minor crime which is punishable.

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

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

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

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

Supervisory Board of Directors
The governing body of an institution, elected by the shareholders, to oversee and supervise the management of the institution's resources and activities. They are ultimately responsible for the conduct of the institution's affairs, and control its direction and, hence its overall policy.

The Unusual Transaction Reporting Center (FIU/MOT)
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.

Third party means an independent separate legal entity or person.

Viatical Contract
A viatical contract is a contract regarding the sale of a life insurance policy to a third party. The owner (viator) of the life insurance policy sells the policy for an immediate cash benefit. The buyer (the viatical settlement provider) becomes the new owner of the life insurance policy, pays future premiums, and collects the death benefit when the insured dies.

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

Appendix 2: **List with examples of suspicious transactions/risks factors to be considered/examples of transactions or trigger events after establishment of the contract**

However, the examples must serve as general indicators which must prompt the institution to closer monitor the client's behavior under the mentioned circumstances. Furthermore, the examples must promote awareness and stimulate the deterrence of money laundering and terrorist financing within the the insurance company.

a. application for a policy from a potential client in a distant place where comparable policy could be provided 'closer to home'

b. application for insurance business outside the policyholder's normal pattern of business

c. introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (e.g. drug trafficking or terrorist activity) are prevalent

d. any request of information or delay in the provision of information to enable verification to be completed

e. any transaction involving an undisclosed party

f. early termination of a product, especially at a loss caused by front end loading, or where cash was tendered and/or the refund check is to a third party

g. a transfer of the benefit of a product to an apparently unrelated third party

h. requests for a large purchase of a lump sum contract where the policyholder's experience is small, regular payments contracts

i. attempts to use a third party to make a proposed purchase of a policy

j. applicant for insurance business shows no concern for the performance of the policy but much concern for the early cancellation of the contract

k. applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by checks or other payment instruments

l. applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency

m. applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify

n. applicant for insurance business appears to have policies with several institutions

o. applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means

p. applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the cash value returned, payable to a third party

q. applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy

r. applicant for insurance business uses a mailbox address outside the insurance supervisor's jurisdiction and where the home telephone has been disconnected, upon verification attempt

Risks factors to be considered

Factors to consider (which are not set out in any particular order of importance and which must not be considered exhaustive) include (where appropriate):

- customer type and background
- geographical origin of customer
- the geographical sphere of the customer's activities
- the nature of the activities
- the means of payment as well as the type of payment (cash, wire transfer, other means of payment)
- the source of funds
- the source of wealth
- the frequency and scale of activity
- the type and complexity of the business relationship
- whether or not payments will be made to third parties
- whether a business relationship is dormant
- any bearer arrangements, and
- suspicion or knowledge of money laundering, financing of terrorism or other crime.

Insurance companies and intermediaries must be aware that for example they are more vulnerable to money laundering if they sell a short term single premium policy than if they sell group pensions to an employer with annuities to be paid after retirement. The former is more sensitive to money laundering and therefore calls for more intense checks on the background of the client and the origin of the premium than the latter. The insurance company and intermediary must also be aware of requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing certain checks, such as sources of wealth.

Examples of transactions or trigger events after establishment of the contract are:

- a change in beneficiaries (for instance, to include non-family members, request for payments to persons other than beneficiaries)
- a change/increase of insured capital and/or of the premium payment (which appears unusual in the light of the income; (several) overpayments of policy premiums after which the policyholder requests that any reimbursement is to be paid to a third party)
- use of cash and/or payment of large single premiums
- requests for prepayment of benefits
- the use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution)

- a change of the type of benefit (lump sum/annuity)(for instance, change of type of payment into lump sum payment)
- early surrender of the policy or change of the duration (where this causes penalties or loss of tax relieve), and
- request for payment of benefits at the maturity date.

Appendix 3: **Life insurance indicators**

Annex C: Indicators services, as referred to in article 1, section a., under 5°, 6° of the NOIS (service providers: insurers and insurance brokers)

a. Taking out an individual life insurance policy

I. REPORTING MANDATORY (objective indicators):

1. A(n) (application for a) life insurance that is reported in connection with money laundering or with the financing of terrorism to the police or the judicial authorities must also be reported to the Reporting Office;
2. The first premium or the single premium is paid cash and is NA*f*. 100,000.00 and higher.

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

1. (Application for) a life insurance in which case there is reason to assume that this can be related to money laundering or the financing of terrorism;
2. Life insurances of which the first premium payment or the single premium is NA*f*. 25,000.00 and higher and which comply with three or more of the following indicators:
   a. the policyholder has his residence outside the Netherlands Antilles;
   b. the policyholder does not state a fixed residence (of his own);
   c. the first premium payment or the single premium deposit takes place from an account at a bank outside the Netherlands Antilles;
   d. the term of the insurance is 3 years or less, unless it is a capital sum insurance for covering pension claims of which the settlement has been established in a pension letter in which it is clearly described that the settlement ensues from an employment relationship;
   e. the premium/single premium payment is more than NA*f*. 250,000.00;
   f. the policyholder has already taken out three or more single premium policies against cash payment at your company or, in the case of intermediaries, through your mediation, in the current calendar year;
   g. payment in small denominations, with uncounted funds, in unusual packing, in foreign currency, with money orders, checks or other negotiable instruments;
   h. there are problems with the identification;
   i. the insurance deviates strongly from what was or may be expected from this policyholder, having taken all circumstances into account (considering income, profession, insurances taken out earlier), in other words, the insurance is unusual for the policyholder;
   j. the policyholder accepts very unfavorable conditions which are not linked to health or age;
   k. a(n) (realistically) insured interest cannot be explained.

b. Settling an individual life insurance policy

I. REPORTING MANDATORY (objective indicators):

1. A payment from a life insurance which, in connection with money laundering or the financing of terrorism, is reported to the police or the judicial authorities, must also be reported to Reporting Office;
2. A payment of NA*f*.100,000.00 and higher on an account at a bank outside the Netherlands Antilles within 5 years after taking out an insurance;
3. A payment of NA*f*. 100,000.00 and higher in connection with the insurance that is transferred within 2 years before the expiration date, the loan or the commutation, or of which the beneficial entitlement is changed within that period (this indicator is not applicable to a transfer to or the beneficial entitlement change in favor of a child or grandchild);
4. A cash payment of NA*f*. 50,000.00 and higher.

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

There is reason to assume that the insurance concerned is related to money laundering or to the financing of terrorism.

Appendix 4: **Source of Funds Declaration Form**[48]

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 insurance company.

2) I ----------declare that the funds totaling NAf[49] _____, to be..... by the undersigned for policy number _____ represents funds obtained by the undersigned from the following source(s):

_____

_____

_____

_____

3) Status

[ ] Resident in Curaçao and Sint Maarten

[ ] Other (specify) _____

[48] The source of funds declaration form must be used when entering into insurance contracts or modifying existing contracts. Where it is reasonable to believe that a prospected customer is connected with illegal activity, or if the customer refuses to sign a "source of funds declaration" and there is no credible explanation to dispel concerns, the insurance company must refuse to execute the requested transaction to insure that the minimum standards are met, but still report it to the Unusual Transactions Reporting Center (FIU/MOT).

[49] Or the equivalent in an other currency

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

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

[ ] Number of a valid identity:

[ ] A valid travel-document or passport: _____

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

5) Consent is hereby provided to this insurance company 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)

Authorized by:

_____
(Name)

_____
(Signature)

[1] This provision is recommended in a pursuit of transparency towards the customer. However, insurance companies and intermediaries may consider excluding this clause from the source of fund declaration form when deemed necessary.