

**BANK VAN DE NEDERLANDSE ANTILLEN**  
**(Central Bank)**

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

April 2009

---

NETHERLANDS ANTILLES

## TABLE OF CONTENTS

<b>I</b>	<b>INTRODUCTION .....</b>	<b>3</b>
I.1	Money Laundering .....	3
I.2	Terrorist Financing .....	4
I.3	Legal basis .....	4
<b>II</b>	<b>PROVISIONS AND GUIDELINES ON THE DETECTION AND DETERRENCE OF MONEY LAUNDERING AND TERRORIST FINANCING FOR INSURANCE COMPANIES AND INTERMEDIARIES .</b>	<b>6</b>
II.1	The relevancy of the detection and deterrence of money laundering and terrorist financing for insurance companies and intermediaries.....	6
II.2	Policies and procedures for insurance companies to deter and detect money laundering and terrorist financing .....	8
II.2.1	Policy statement.....	8
II.2.2	The implementation of a formal system of internal control to identify (prospective) clients and deter, detect and report unusual transactions and keep adequate records of the clients and transactions .....	8
II.2.2.1	Information and internal control measures.....	9
II.2.2.2	Internal control policy with respect to unusual transactions .....	13
II.2.3	The appointment of one or more compliance officer(s).....	16
II.2.4	An independent testing system of the policies and procedures .....	17
II.2.5	Screening of employees / Appropriate training plans and programs for personnel.....	17
II.3	Examination by the Bank van de Nederlandse Antillen .....	18
Appendix 1:	Glossary/Definitions.....	20
Appendix 2:	List with examples of suspicious transactions/risks factors to be considered/examples of transactions or trigger events after establishment of the contract .....	22
Appendix 3:	Life insurance indicators .....	24
Appendix 4:	Source of Funds Declaration.....	26

## I INTRODUCTION

The Netherlands Antilles is committed in the fight against money laundering and terrorist financing. Because of this commitment, and being a member of both the Financial Action Task Force on Money Laundering (FATF)<sup>1</sup> and the Caribbean Financial Action Task Force (CFATF)<sup>2</sup>, the Netherlands Antilles has introduced a comprehensive framework to prevent and combat money laundering and terrorist financing.

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

- a) The National Ordinance on the amendment of the Code of Criminal law (penalization of terrorism, terrorist financing and money laundering)(N.G.<sup>3</sup>. 2008, 46);
- b) The National Ordinance on the Reporting of Unusual Transactions (MOT) (N.G. 1996, no. 21);
- c) The National Ordinance on Identification of Clients before Rendering Financial Services “LIF”) (N.G. 1996, no. 23);
- d) Ministerial Decrees and National decrees containing general measures issuing the indicators for reporting of unusual transactions relating to money laundering and terrorist financing;
- e) National decrees freezing assets Taliban cs and Usama bin Laden cs;
- f) National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74).

These laws and decrees are the basis for further actions by the Netherlands Antillean financial sector to detect and deter money laundering and terrorist financing. Furthermore, the latest laws and decrees represent the implementation of the original 40 FATF recommendations to combat money laundering as issued in 1990 and lastly revised in 2003<sup>4</sup>.

After the September 11 terrorism attacks, the FATF extended its mandate with the combating of the financing of terrorism. In October 2001, the FATF issued 8 special recommendations on terrorist financing<sup>5</sup>. In 2004 the ninth special recommendation on terrorist financing was issued by the FATF.

These Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing issued by the Bank aim to achieve compliance with the FATF 40 recommendations of 2003 and the nine special recommendations on terrorist financing.

### 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. This gives rise to three common factors:

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

<sup>1</sup> See appendix 1 for the definition or explanation or summary.

<sup>2</sup> See appendix 1 for the definition or explanation or summary.

<sup>3</sup> N.G.: National Gazette, official national publication.

<sup>4</sup> The 40 recommendations can be found on the FATF website at: <http://www.fatf-gafi.org>.

<sup>5</sup> The 8 recommendations can be found on the FATF website at: <http://www.fatf-gafi.org>.

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:  
This is the first stage of the money laundering process when illegal monies are introduced in 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:  
Separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- 3) Integration:  
The provision of apparent legitimacy to criminally derived wealth. 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 terrorist or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offence. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.

To help financial institutions identify financing of terrorism, the FATF issued a publication: “Guidance for Financial Institutions in Detecting Terrorist Financing”<sup>6</sup> 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 Bank instructed the supervised institutions to continuously match their client base with the names on the United Nations’ list<sup>7</sup>.

### **I.3 Legal basis**

These provisions and guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing are issued by the Bank van de Nederlandse Antillen (hereinafter “the Bank”) pursuant to the following legal provisions:

- The National Ordinance on the Supervision of Banking and Credit Institutions (N.G. 1994, no. 21), article 21 paragraph 2 section e for credit institutions;

<sup>6</sup> The full document can be consulted at <http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf>.

<sup>7</sup> The list can be consulted at <http://www.un.org/docs/sc/committees/1267/1267listeng-htm>.

- The National Ordinance Insurance Supervision (N.G. 1990, no. 77), article 31 paragraph 1 for insurance companies;
- The National Ordinance on Investment Institutions and Administrators (N.G. 2002, no. 137), article 9 paragraph 1, and article 18 paragraph 1 for investment companies respectively administrators;
- The National Ordinance on Foreign Exchange Traffic (N.G. 1981, no. 67) for money remitters;
- The National Ordinance on the Insurance Brokerage Business, article 6 paragraph 1b (N.G. 2003, no. 113).

The aim of the provisions and guidelines is to contribute to an adequate implementation by all supervised (financial) institutions of:

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

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

The provisions and guidelines apply to the following type of financial institutions:

- Credit institutions
- Insurance Companies
- Investment institutions
- Administrators of Investment institutions
- Money transfer companies
- Insurance Brokerage Business

## 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 should provide to the Bank van de Nederlandse Antillen (hereinafter “the 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 policyholder 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 insurer 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<sup>8</sup> contracts are the contracts which are more subject to abuse.

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

---

<sup>8</sup> See appendix 1 for the definition or explanation or summary.

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

If insurance companies 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 activity and expose themselves to adverse publicity and to losses resulting from fraud.

The National Ordinance on the Reporting of Unusual Transactions (N.G.<sup>9</sup>1996, no. 21) requires that each financial institution that renders financial services including life insurance companies, should report any unusual transactions thereby made or proposed, to the Unusual Transaction's Reporting Center (MOT)<sup>10</sup> without delay. 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 (MOT) to collect, process and analyze the obtained information.

These provisions and guidelines are primarily aimed at life insurance business which is the predominant type within the insurance sector being used by money launderers. There is no reporting duty yet for the non-life sector. This does however, not change the fact that non-life insurers should be aware of the fact that their institution could be used for money laundering purposes, e.g. illegally obtained funds may be used to purchase assets which are deliberately written off in order to receive 'clean' money from an insurer. Insurance companies should take all necessary steps to prevent this.

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

The National Committee against Money Laundering "CIWG" is preparing draft legislation to include the broad insurance sector. New indicators will be developed in due time.

#### 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 should play an important part in anti-money laundering and the prevention of financing of terrorism. The same principles that apply to insurance companies should 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 financial services, N.G. 1996, no 23), 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.

---

<sup>9</sup> N.G.: National Gazette, official national publication.

<sup>10</sup> See appendix 1 for the definition or explanation or summary.

## **II.2 Policies and procedures for insurance companies to deter and detect money laundering and terrorist financing**

### **II.2.1 Policy statement**

Each insurance company's Supervisory Board of Directors<sup>11</sup> and Management<sup>12</sup> should 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 the purpose of money laundering and terrorist financing.

This policy statement is a statement of "Best Practice" of the Supervisory Board of Directors and Management of an insurance company which outlines the institution's policies and procedures.

The statement should 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<sup>13</sup> should amongst others also cover:

- 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) should have the authority to investigate unusual transactions extensively;
- A system of independent testing of procedures by the insurance company's internal audit personnel, compliance department, or by a competent external source;
- Screening of and 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.

### **II.2.2 The implementation of a formal system of internal control to identify (prospective) clients and deter, detect and report unusual transactions and keep adequate records of the clients and transactions**

Pursuant to the National Ordinance on Identification of clients when Rendering Financial Services (N.G. 1996, no. 23) the life insurance companies and intermediaries must ascertain and

---

<sup>11</sup> See appendix 1 for the definition or explanation or summary.

<sup>12</sup> See appendix 1 for the definition or explanation or summary.

<sup>13</sup> In the design, update and implementation of their policy statement, the 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>

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 LIF, 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 the above-mentioned ordinance in excess of the amount stipulated by the Minister. The amount as stipulated by Ministerial Decree (N.G. 1998 no.19) is fixed at NAf. 2.500,- per annum if it concerns a periodical premium, and at NAf. 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 NAf. 20.000,- by Ministerial Decree (N.G. 1998 no. 19).

### II.2.2.1 Information and internal control measures

Insurance companies and their intermediaries have the obligation to determine the true identity of their (prospective) personal and corporate clients/customers<sup>14</sup>, before entering into insurance contracts with them.

Internal procedures should also clearly indicate for which contracts prospective policyholders or their representatives must identify themselves and which identification documents are acceptable. Insurance companies should 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 should ensure that transactions, should under no circumstance be conducted with customers who fail to provide proof of their identity. As a matter of principle, insurers should 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 should be taken by insurers include:

- identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
- for all customers, the insurer should determine whether the customer is acting on behalf of another person, and should 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 insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include insurers 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; 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 insurer's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

---

<sup>14</sup> See appendix 1 for the definition or explanation or summary.

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 should be the subjects of verification.

The insurance companies and intermediaries should 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 surrenders request and policy alterations, including changes in beneficiaries; see appendix 2 for more triggers). The company should 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 should 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 should be conducted for high risk customers, including politically exposed persons (PEPs)<sup>15</sup>, their families and associates. The institutions decisions to enter into such business relationships should be taken at its senior management level. The institution should make reasonable efforts to ascertain that the customer's source of wealth is not from illegal activities. Insurance companies should not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

Insurance companies should 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 should therefore be adequately documented.

An important objective for insurance companies 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 should apply to all new customers as well as –on the basis of materiality and risk- to existing customers. As to the latter the insurer should 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 should be in place.

#### Reliance on intermediaries and third parties

Insurers should include specific clauses in the contracts with their intermediaries. These clauses should 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 MOT and insurer in the case of a suspicious transaction or activity. It is recommended that insurers use application forms to be filled out by the customers and/or intermediaries that

---

<sup>15</sup> See appendix 1 for the definition or explanation or summary.

include information on identification of the customer and beneficial owner as well as the method used to verify its identity. Insurers should inform themselves which jurisdiction are considered suitable to rely on business from intermediaries and third parties.

The insurer should 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.

The ultimate responsibility for customer identification and verification remains with the insurer relying on third parties. It should be emphasized to intermediaries and third parties the importance of knowing their customer and the consequences of assisting in money laundering and financing of terrorism.

### A) Identification of personal customers

Pursuant to article 3 of the National Ordinance on the Identification when Rendering Financial Services (N.G. 1996, no. 23) (LIF)<sup>16</sup>, the identity of a **resident** and a **non-resident** personal customer shall be established through one of the following documents:

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

In case of a **non-resident** customer, a copy of aforementioned documents is acceptable, provided that the relevant documentation will be accompanied by a certified extract of the civil registry of births, deaths and marriages of the place of residence of the customer.

In addition, the identity of a **resident** customer may be verified by reviewing the local telephone directory and seeking confirmation of identity or activities with other institutions.

Management may require additional information to be submitted, such as:

- telephone number;
- occupation and name of employer (if self employed, description of the occupation);
- reference letter;
- name and address of references;
- copy of a utility bill;

Verification of the identity of **non-resident** clients should 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,

---

<sup>16</sup> See appendix 1 for the definition or explanation or summary.

- if provided, cross reference address printed on personal check to permanent address provided by client on standard application form.

Insurance companies should 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.

## **B) Identification of corporate customers**

It is important to identify the nature of the business, its directors (supervisory and managing directors), account signatures and the (ultimate) beneficiaries. In this respect the amount of coverage may also be important. The procedures for the identification of personal customers should be applied for the company directors and all owners and (ultimate) beneficial owners<sup>17</sup> holding a qualifying interest in the company.

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 shall contain at least the information stipulated by the Minister in Article 6 of the Ministerial Decree with General Operations for the execution of National Ordinance Identification when Rendering Financial Services.

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

- shareholder's 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.

### Record keeping

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

Where appropriate, insurance companies should consider retaining certain records e.g. customer identification and business correspondence, for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations.

---

<sup>17</sup> See appendix 1 for the definition or explanation or summary.

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:

1. All necessary records on transactions, both domestic and international, should 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.
2. 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 should be kept for at least five years after the account is closed.

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

### **II.2.2.2 Internal control policy with respect to unusual transactions**

Life insurance companies 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 should cover:

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

#### **Re.: a) Recognition of unusual transactions<sup>18</sup>**

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 insurer should 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 should, as far as possible, be examined, the findings established in writing, and be available to assist competent authorities and auditors. In this respect, institution's employees should 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 accepting 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.

Money laundering and terrorist financing are not only realized through new business relationships and transactions. Insurance entities should 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.

---

<sup>18</sup> For specific examples of suspicious transactions please refer to Appendix 2.

Whether a transaction is unusual is determined on the basis of established indicators.

Based on the National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21), 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 should develop special programs to select objectively defined unusual transactions. Moreover, management must provide its staff with specific guidelines and training to recognize and document adequately the unusual transactions based on especially the subjective indicators.

#### International 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 should be extremely vigilant when premium payments are made or sums are deposited from accounts with banks outside the Netherlands Antilles. If such funds are accepted, suitable identification of the depositor should be obtained. If another party than the policyholder pays, than knowledge about the source of funds should be required through a "Source of Funds Declaration Form" as presented in Appendix 4 of this guideline.

#### Non-cooperative countries and territories (NCCTs)

Insurance companies should 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 "non-cooperative countries and territories" (NCCTs)<sup>19</sup>, being countries that, according to the criteria of the FATF do not apply sufficient anti-money laundering measures, and procedures in combating the financing of terrorism. If insurance companies and intermediaries find that such a transaction is unusual, this should be reported to the MOT.

#### 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 insurer should nevertheless complete verification. The insurers need to have policies and procedures in place to address the specific risks associated with non face-to-face business relationships or transactions.

#### Terrorist financing

Insurance companies should take into account the characteristics including types of transactions listed in the annex 1 to the FATF document "Guidance for Financial Institutions in Detecting terrorist Financing"<sup>20</sup>. Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing.

---

<sup>19</sup> For an update of listed NCCTs, insurance companies should consult the FATF-website at: <http://www.fatf-gafi.org/NCCT-en.htm>

<sup>20</sup> The full document can be consulted at <http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf>.

In addition, insurance companies should take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in:

- the annex to the National Ordinance on Freezing the assets of Taliban of Afghanistan c.s. and Usama Bin Laden c.s. of 2002 (N.G. 2002, no. 27);
- annex 2<sup>21</sup> to the FATF document : "Guidance for Financial Institutions in Detecting Terrorist Financing";
- the listing<sup>22</sup> of the Office Of Foreign Assets Control (OFAC)<sup>23</sup> or of other national authorities;
- the lists issued by the United Nations<sup>24</sup>.

In addition, insurance companies should be vigilant in the abuse of non-profit organizations for terrorist financing. The institutions should observe the FATF's Special Recommendation (SR) VIII<sup>25</sup> and consider the relevant parts of the FATF document: "Combating the abuse of non-profit organizations, International best practices"<sup>26</sup>.

If an insurance company 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 should report promptly its suspicion to the Unusual Transaction Reporting Center (MOT).

#### **Re.: b) Acceptance and 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 Unusual Transactions Reporting Center (MOT).

#### **Re.: c) Reporting of unusual transactions**

Insurance companies should 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 National Ordinance on the Reporting of Unusual

---

<sup>21</sup> The full document can be consulted at <http://www.fatf-gafi.org/pdf/GuidFITFOI/en.pdf>

<sup>22</sup> The list can be consulted on FINCEN's website at <http://www.treas.gov/offices/enforcement/ofac/sanctions/terrorism.html>.

<sup>23</sup> See appendix 1 for the definition or explanation or summary.

<sup>24</sup> The list can be consulted at <http://www.un.org/docs/sc/committees/1267/1267listeng-htm>.

<sup>25</sup> Special recommendation VIII refers to measures with respect to vulnerable non-profit organizations.

<sup>26</sup> The full document can be consulted at <http://www.fatf-gafi.org/pdf/SR-8NPO/en.pdf>

Transactions, should 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 should also be submitted as supplements. Nevertheless, management should stipulate the categories of unusual transactions which must also be brought to their attention. The designated officer(s) should keep an adequate filing system for these records.

If internally reported transactions are not reported to the Unusual Transactions Reporting Center (MOT) by the compliance officer, the reasons therefore should be adequately documented and signed off by this officer and/or by management.

### External reporting

Insurance companies should cooperate fully with the national law enforcement authorities. A report should be prepared of all unusual transactions by the designated officer(s) for external reporting purposes. The report should be submitted to management for their review for compliance with existing regulations, and their authorization for submission to the Unusual Transactions Reporting Center (MOT). Copies of these reports must be kept by the reporting institution.

If an unusual transaction is not authorized by management to incorporate in the report to the Unusual Transactions Reporting Center (MOT), all documents relevant to the transaction including the reasons for non-authorization should be adequately documented, signed off by the designated officer and management and kept by the reporting institution.

Management should 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 Unusual Transactions Reporting Center (MOT), or on internal inquiries being made by the institutions compliance staff on them;
- the insurance company and its Supervisory Board of Directors, management and employees follow the instructions from the Unusual Transactions Reporting Center (MOT) to the extent that they carry out further investigation or review. The same holds for inquiries made 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 of the Netherlands Antilles do not allow any exemptions on the reporting obligation of financial service providers.

## **II.2.3 The appointment of one or more compliance officer(s)**

Each insurance company should formally designate one or more senior officer(s) to be responsible for money laundering and terrorist financing deterrence and detection, with at least the following responsibilities:

- to organize training sessions for the staff on various compliance related issues;
- to review compliance with the insurance company's policy 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 prepare periodic information on the institutions' efforts in combating money laundering and terrorist financing.

The above mentioned responsibilities should be included in the job description of each designated officer. The job description should be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.

#### **II.2.4 An independent testing system of the policies and procedures**

Independent testing of the adequate working of the policies and procedures should be conducted at least annually by the internal audit department or by an outside party such as the institution's external auditors. These tests may include:

- evaluation of the institution's anti money-laundering and anti-terrorist financing manual(s);
- customer's file review;
- interviews with employees who handle 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;
- a test of the validity and reasonableness of the judgments used when exempting from reporting to the Unusual Transactions Reporting Center (MOT); and
- assessment of the adequacy of the record retention system.

The scope of the testing and the testing results should be documented, with any deficiencies being reported to management and/or the Supervisory Board of Directors, and to the designated officer(s) with a request for a response to take prompt corrective actions in the future by a certain deadline.

#### **II.2.5 Screening of employees / Appropriate training plans and programs for personnel**

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

Insurance companies should at a minimum develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions.

Training should 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 internal and external 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 should be provided to all new employees dealing with customers, irrespective of their level of seniority. Similarly, training should 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 should 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 their responsibilities and that they are updated on current and new developments in the area of money laundering and terrorist financing techniques, methods and trends. The training should include a clear explanation of all aspects of the Netherlands Antillean laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. This might be best achieved by a semi-annual review of the instructions for recognizing and reporting of unusual transactions.

In order for an insurance company to be able to demonstrate that it has complied with the aforementioned guidelines with respect to staff training, it should 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 delivered;
- 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.3 Examination by the Bank van de Nederlandse Antillen**

All insurance companies should be prepared to provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the Bank before or during an examination and upon the Bank's request during the year. The insurance company should be prepared to make available:

- its written and approved policy 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 deterrence and detection procedures, and her/his designated job-description;
- records of reported unusual transactions;
- unusual transactions on which closer investigation was required or a source of funds declaration has been executed;
- schedule of the training provided to the institution's personnel regarding money laundering and terrorist financing;
- the assessment report on the institutions policies and procedures on money laundering and terrorist financing by the internal audit department or the institution's external auditor; and
- documents on system tests such as the customers' policies, premium payments overview, duration of policies, purchase sums and other relevant information.

**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.

**The Caribbean Financial Action Task Force (CFATF)**

The CFATF is an organization of twenty-six 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 LIF, a client/customer is anyone to whom a financial service, as defined in article 1 sub b of the LIF, is rendered.

**The 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 29 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/>

**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 owing 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 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.

**LIF**

The National Ordinance on the Identification when Rendering Financial Services (N.G. 1996, no. 23) includes provisions on the identification of clients when rendering financial services.

**Management**

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

**Office of Foreign Assets Control (OFAC)**

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

**Politically exposed persons (PEPs)**

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

### **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 (MOT)**

Pursuant to article 11 of the National Ordinance on the reporting of Unusual Transactions (N.G. 1996, no. 21), 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.

### **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.

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

- 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 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 want 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 cheque 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 use 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 should 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.

Insurers should 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 insurer should 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****A. The entering into of an individual life insurance contract.**

For all indicators, the following shall apply:

All amounts stated shall be NAf., or the equivalent thereof in foreign currency.

**I. REPORTING MANDATORY:**

1. (An application for) a life insurance reported to Police or Justice in relation to money laundering, shall also be reported to the Reporting Center;
2. The initial premium or the purchase sum is paid in cash and exceeds NAf. 100,000.-.

**II. REPORTING MANDATORY IF THE PERSON LIABLE FOR REPORTING CONSIDERS THAT THE FOLLOWING SITUATIONS APPLY:**

1. (An application for) a life insurance whereby there is cause to presume that same may relate to money laundering and or terrorist financing;
2. Life insurances for which the initial premium payment or the purchase sum exceeds NAf. 25,000.- and which meet three or more of the following indicators:
  - a. the policyholder has his residence outside the Netherlands Antilles;
  - b. the policyholder reports no (private) permanent residence;
  - c. the initial premium payment or purchase sum deposit is effected from an account with a bank outside the Netherlands Antilles;
  - d. the duration of the insurance is 3 years or less, unless it concerns capital assurance for the covering of pension claims, the scheme of which has been laid down in a pension letter, clearly stating that the scheme is based on employment;
  - e. the premium/purchase sum payment amounts to more than NAf. 250,000;
  - f. the policyholder already has effected three or more single-premium insurances with your company against cash payment in the current calendar year or, in the case of brokers, has effected same through your mediation ;
  - g. payment in small denominations, with uncounted money in unusual packaging, in foreign currency by postal orders, checks or other valuable;
  - h. there are problems with identification;

- i. the insurance deviates considerably from what was expected or might have been expected from this policy-holder, taking into consideration all circumstances (reckoning with income, occupation, insurances concluded earlier), in other words the insurance is unusual for the policyholder;
- j. the policyholder accepts very unfavorable terms that are not connected with health or age;
- k. an (actual) insured interest cannot be explained.

**B. The completion of an individual life insurance contract**

For all indicators, the following shall apply:

All amounts stated shall be NAf., or the equivalent thereof in foreign currency.

**I. REPORTING MANDATORY:**

- 1. Any payment from life insurance, related to money laundering, reported to Police or Justice, shall also be reported to the Reporting Center;
- 2. Any payment in excess of NAf. 100,000.- into an account with a bank outside the Netherlands Antilles within 5 years from the insurance having been entered into;
- 3. Any payment of over NAf. 100,000.- related to the insurance, transferred within 2 years prior to the expiration date of the insurance, its use as collateral security or the surrendering of its policy or the beneficiary of which insurance was changed within that period (this indicator shall not apply in respect of a transfer to, or of the party benefited being changed to, a child or a grandchild);
- 4. Any cash payment in excess of NAf. 50,000.-.

**II. REPORTING MANDATORY IF THE PERSON LIABLE FOR REPORTING CONSIDERS THAT THE FOLLOWING SITUATIONS APPLY:**

- 1. There is cause to presume that the insurance concerned is related to money-laundering and or terrorist financing

**Appendix 4: Source of Funds Declaration<sup>27</sup>**

To: (Institution's name and location)

----- Time: -----  
----- Date:-----  
-----

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

2) I declare that the currency totaling \_\_\_\_\_, to be..... by the undersigned for policy number \_\_\_\_\_ represents funds obtained by the undersigned from the following source:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3) Status

Antillean resident

Dutch resident

Other (specify) \_\_\_\_\_

<sup>27</sup> The source of funds declaration should be used when entering into insurance contracts or modifying existing contracts. Where it is reasonable to believe that a prospect 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 should refuse to execute the requested transaction to insure that the minimum standards are met, but still report it to the Unusual Transactions Reporting Center (MOT).

4) Legally accepted customers identification documents (Article 3 of the National Ordinance on the Identification When rendering Financial Services, 1996)

- Number of a valid driver's license: \_\_\_\_\_
- Number of a valid identity card issued by the local authorities: \_\_\_\_\_
- A valid travel-document or passport: \_\_\_\_\_
- Another document to be designated by the Minister: \_\_\_\_\_
- Other (specify): \_\_\_\_\_

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.

\_\_\_\_\_  
(Customers name)

\_\_\_\_\_  
(Customers address)

\_\_\_\_\_  
(Signature)

**Authorized by:**

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Signature)