# BANK OF GUYANA

# Guideline for

# Insurance Companies and Intermediaries

# on

# Anti-Money Laundering and Countering the

# Financing of Terrorism

**Date issued**
March 26, 2013

**Dates Amended**
29 April 2019
17 March 2023

**TABLE OF CONTENTS**

**ABBREVIATIONS**

| | |
|---|---|
| AML | Anti-Money Laundering |
| AML/CFT | Anti-Money Laundering and the Combatting the Financing of Terrorism |
| BOG | Bank of Guyana |
| CDD | Customer Due Diligence |
| CO | Compliance Officer |
| CFATF | Caribbean Financial Action Task Force |
| EDD | Enhanced Due Diligence |
| FATF | Financial Action Task Force |
| FIU | Financial Intelligence Unit |
| IA | Insurance Act 2016 (Act No. 17 of 2016) |
| IAIS | International Association of Insurance Supervisors |
| KYC | Knowing Your Customer |
| KYE | Knowing Your Employee |
| ME | Mutual Evaluation |
| ML | Money Laundering |
| ML/TF | Money Laundering and Terrorism Financing |
| NRA | National Risk Assessment |
| PEP | Politically Exposed Person |
| PF | Proliferation Financing |
| SA | Supervisory Authority |
| SDD | Simplified Due Diligence |
| STR | Suspicious Transaction/Activity Report |
| WMD | Proliferation of Weapons of Mass Destruction |

## 1.0 INTRODUCTION

### 1.1 The Anti-Money Laundering Guidelines for the Conduct of Insurance Business

The insurance industry is potentially at risk of being misused for money laundering and financing terrorist activities. The products and services offered in the insurance industry can provide an opportunity for these criminal activities. As a result, an insurer or an insurance intermediary may be involved knowingly or unknowingly in money laundering and/or financing of terrorist activities thus exposing it to legal, operational, and reputational risks.

The Bank of Guyana (the Bank), pursuant to its mandate to regulate, supervise and develop the insurance industry has developed guidelines to combat money laundering and financing of terrorism in the insurance industry.

Internationally, initiatives to prevent the misuse of financial systems by persons laundering money and financing terrorism led to the formation of the Financial Action Task Force (FATF). FATF is an intergovernmental policy-making body that sets standards, develops and promotes policies to combat money laundering and terrorist financing. In 2012, FATF revised and issued 40 Recommendations to combating money laundering and terrorist financing. These are recognized as the global standards for combating money laundering and terrorist financing. The International Association of Insurance Supervisors (IAIS), recognizes the FATF recommendations as the guiding principles for anti-money laundering and combating the financing of terrorism.

The Bank (BOG) is required to circulate the United Nations Sanctions List to the reporting companies under its purview for information and necessary action.

These Anti-Money Laundering Guidelines for Insurance Companies are to be followed by all persons conducting insurance business in Guyana. The Guidelines highlight methods of prudent customer identification, record keeping, identification of suspicious activities and reporting such activities to the FIU for further investigation.

Failure to comply with these Guidelines may bring into question the fitness and propriety of the company. Where any procedures are required to be established under these Guidelines, such procedures must be followed and the insurance company may, upon the request of BOG, be asked to demonstrate compliance.

These Guidelines should always be considered together with, inter alia, the obligations of the Anti-Money Laundering and Countering the Financing of Terrorism Act, No. 13 of 2009 (AMLA) and all of its amendments.[1] Notwithstanding *anything* contained in these Guidelines, the provisions contained in the AMLA *shall prevail* over the provisions not in conformity with or *contradicting* any provisions contained in the AMLA.

The BOG will from time to time update these Guidelines to reflect new legislation, developments in the finance sector, changes to international standards and good practice and the Regulations.

The requirements set out herein in these Guidelines must be considered as a mandatory minimum.

### 1.2 Branches and Subsidiaries

Where an Insurance Company has branches or subsidiaries in other jurisdictions, the practices and procedures, consistent with these Guidelines, must be uniform throughout all parts of the business.

[1] See Appendix A.

However, if different practices emanate from the host jurisdiction the more specific requirements of host regulators and authorities should be monitored and met. Where the requirements of the host jurisdiction differ from those required by these Guidelines, the higher of the requirements (either host or these Guidelines) must be applied.

**1.3 Legislative Framework**

The following laws and guidelines comprise the AML/CFT legislative framework:

1. Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (Act No. 13 of 2009) and Amendments
2. AML/CFT Regulations No. 4 of 2010
3. AML/CFT Regulations No. 4 of 2015
4. AML/CFT Regulations No. 7 of 2015
5. Insurance Act 2016 (Act No. 17 of 2016
6. Insurance Act 1998 (repealed)
7. Power of Attorney (Amendment) Act 2022
8. Companies Act Cap 89:01
9. AMLCFT Handbook for Reporting Entities
10. Guidance Notes for Insurance Companies & Brokers

**2.0 GENERAL**

**2.1 Definitions**

“Act” means The Anti-Money Laundering and Countering the Financing of Terrorism Act No. 13 of 2009 and its subsequent amendments.

“The Bank” means the Bank of Guyana.

“Beneficiary” refers to the beneficiary to the insurance contract or pension plan.

“Customer” refers to the policyholder or prospective policyholder.

“Insurance company” refers to insurance companies licensed under the Insurance Act, No. 17 of 2016.

“Insurance intermediaries” mean agents and brokers licensed under the Insurance Act No. 17 of 2016.

**2.2 Key Concepts**

“Money Laundering” means the act of a person who:

a) knows or ought to have reasonably known that the property is or forms part of the proceeds of crimes and;

b) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether that agreement, arrangement or transaction is legally enforceable or not; or

c) performs any other act in connection with such property, whether it is performed independently or with any other person,

d) Whose effect is to:
   - conceal or disguise the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof; or
   - enable or assist any person who has committed or commits an offence, whether in Guyana or elsewhere to avoid prosecution; or
   - remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence;

e) acquires, uses or has possession of property and who, at the time of acquisition, use or possession of such property, knows or ought reasonably to have known that it is or forms part of the proceeds of a crime committed by another person;

f) knowingly transports, transmits, transfers or receives or attempts to transport, transmit, transfer or receive a monetary instrument or anything of value to another person, with intent to commit an offence.

"**PEP**" means Politically Exposed Person. This refers to a person holding a prominent position in a public office and includes spouse, close relative or associate of such person. Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a local or foreign country, e.g., Heads of States or Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc., including their spouses, close relatives and associates or legal persons and arrangements controlled by such persons.

"**Person**" means any natural or legal entity.

"**Proceeds of Crime**" means any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence irrespective of the identity of the offender and includes, on a proportional basis, property into which any property derived or realised directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property from the time the offence was committed.

"**Regulations**" refer to the Anti-Money Laundering and Countering the Financing of Terrorism Regulations and the Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations 2013.

"**Reporting Company**" means an insurance company and a designated non-financial business and profession as defined in the Anti-Money Laundering and Countering the Financing of Terrorism Act No. 13 of 2009 and its subsequent Amendments.

"**Terrorism Acts**" are as defined in the Anti-Money Laundering and Countering the Financing of Terrorism Act No. 13 of 2009.

### 2.3 Vulnerabilities in the Insurance Industry

The insurance industry is vulnerable to money laundering and financing of terrorism in a number of ways. The Bank brings to the attention of the industry some of the transactions or products that may be vulnerable to money laundering and financing of terrorism. The industry shall be required to take more precautions in these transactions:

a. Life policies may become vulnerable in that when it matures or is surrendered, funds become available to the policyholder or beneficiary. In such cases, the beneficiary may sometimes be changed, possibly against payment before maturity or surrender, in order that the insurer can make payments to a 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 with their origins elsewhere in the financial system.

b. Examples of the type of insurance contracts that are vulnerable as a vehicle for laundering money are products such as:

   i. unit-linked or non-unit-linked single premium contracts;
   ii. purchased annuities;
   iii. lump sum top-ups to an existing life contract; and
   iv. lump sum contributions to personal pensions contracts.

c. General insurance companies may be vulnerable to money laundering and financing of terrorism through inflated and bogus claims e.g., by arson, or other means causing false claims to be made to recover part of the invested illegitimate claim.

d. Re-insurance may be used for money laundering and financing of terrorism by establishing fictitious reinsurance companies and reinsurance intermediaries fronting arrangements and captives, or by misuse of normal reinsurance transactions which may include the deliberate placement via the insurer of the proceeds of crime with a reinsurance company in order to disguise the source of funds.

e. Insurance intermediaries are an important channel of distribution and the link between the insurer and the policy holder may be used for money laundering and financing of terrorism by either failing to carry out due diligence or being established to facilitate illegal transactions.

f. Premium financing by non-regulated financial companies can be used as an avenue for money laundering and financing of terrorism where the insured uses illegal funds to repay the premium loan with an intention of receiving clean funds upon the occurrence of the risk and compensation by the insurer. The finances used for premium financing may also be from an illegal source and are being laundered by advancing loans to policyholders or prospective policyholders.

**2.4 Stages of Money Laundering**

Despite the variety of methods employed, the laundering process is accomplished in three stages. The stages of anti-money laundering may occur in any order and may not necessarily be in the order provided.

The stages, described below, may comprise numerous transactions by the launderers that could alert an insurance company or an intermediary of the criminal activity:

a) **Placement** – the physical disposal of the initial proceeds derived from illegal activities. It entails the physical movement of cash or property away from the location where it was illegally obtained and its placement in the legitimate financial system.

b) **Layering** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. This may include a scenario where a single premium investment is accompanied by a request for a letter of guarantee, and/or followed by surrender, or loan and unit trust investments shortly followed by repurchase.

c) **Integration** – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, an integration scheme places the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. This may be obtaining assets e.g. through investment in a policy, obtaining payment by way of cheque or electronic payment from the insurer and reinvestments in other instruments.

The insurance industry is a potential major target for money laundering operations because of the variety of services and investment vehicles offered that can be used to conceal the source of money.

## 3.0 POLICIES AND PROCEDURES TO COUNTER MONEY LAUNDERING AND FINANCING OF TERRORISM

The AML/CFT Act 2009 designates the Bank as the AML/CFT SA for the insurance companies/brokers. The primary responsibilities of the Bank as an SA include *inter alia*:

- reviewing the compliance programme of all insurance companies/brokers to determine its adequacy and compliance with applicable laws and guidelines;
- approving the Compliance Officer;
- issuing guidelines, instructions or recommendations to aid compliance with AML/CFT requirements;
- taking proportionate and dissuasive regulatory action against those insurance companies and intermediaries regulated by it which fail to comply adequately with AML/CFT statutory obligations and guidelines issued by the Bank; and
- cooperating and sharing information promptly with the FIU, and other domestic competent authorities as required for the purposes of AML/CFT. This includes disclosing information to the FIU as soon as is reasonably practicable where it has knowledge or has reasonable grounds for believing that insurance companies and intermediaries may have been engaged in money laundering or terrorist financing.

## 4.0 RESPONSIBILITIES OF THE BOARD AND MANAGEMENT

### 4.1 The Board

a. It is the responsibility of the board of directors of insurance companies to:

i. Establish policies and procedures to ensure the effective prevention, detection, reporting and control of possible money laundering and terrorist financing activities.

ii. Review the policies and procedures once every two (2) years and from time to time as may be necessary, to ensure compliance with the Law. Any changes on the policies and procedures must be filed with the Bank within thirty (30) days of effecting the changes.

iii. Communicate the policies to all staff whether in local or foreign branches, departments or subsidiaries and develop instruction manuals setting out procedures for:

- Customer acceptance and identification
- Customer due diligence
- Record-keeping
- Recognition and reporting of suspicious transactions
- Staff screening and training
- Establishing the legitimacy of the source of funds

b. Comply with the relevant legislation and seek actively to promote close cooperation with law enforcement authorities.

c. Instruct their internal audit or compliance departments to verify, on a regular basis, compliance with policies, procedures and controls against money laundering and terrorist financing.

d. Regularly review the policies and procedures on countering money laundering and terrorist financing to ensure their effectiveness. Assess and ensure that the risk mitigation procedures and controls are working effectively.

e. Register with the FIU and comply with their reporting obligations under the AML/CFT Act 2019:

- **Threshold Transaction Report (TTRs)** – any transaction facilitated for a customer (single or accumulated) within a month that is equal to or above two million dollars ($2,000,000) must be reported on or before the 7th day of the following month.

- **Suspicious Transactions Reports (STRs)** – must be submitted by the reporting entity no later than three (3) days after forming a suspicion.

- **Terrorist Property Reports (TPRs)** any transaction (without delay) after a person or entity has been identified on the United Nations Security Council (UNSC) Consolidated List or is listed or specified by order of the Minister of Finance in accordance with section 2(2) of the AML/CFT Act 2009. This report is also required to be filed on a quarterly basis on the 7th day after the end of each quarter.

f. Appoint a Compliance Officer according to the requirements stipulated in section 19 (1) (a) of the Act.
g. Develop a group policy on anti-money laundering and combating the financing of terrorism and extend this to all its branches and subsidiaries where applicable outside Guyana.

**4.2 Senior Management**

a. Senior Management is responsible for the day-to-day implementation, monitoring and management of the insurance company's AML/CFT compliance programme, including ensuring adherence to established AML/CFT policies and procedures. Among other things, Senior Management should ensure that policies and procedures:

i. are risk based, proportional and adequate to mitigate ML and TF risks of the insurance company;

ii. comply with all relevant AML/CFT laws, regulations and guidelines; and

iii. are implemented effectively across relevant business areas or throughout the financial group as applicable.

b. Senior Management must review policies and procedures periodically for consistency with the insurance company's business plan, product and service offerings, and risk appetite. Attention should be paid to **new and developing technologies** and companies should identify and assess the ML/FT risks arising from **new products/services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks**. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

c. Senior Management should also ensure that:

i. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT programme are acted upon in a timely manner;

ii. Relevant, adequate and timely information regarding AML/CFT matters is provided to the Board;

iii. The CO receives the appropriate training on an ongoing basis to effectively perform his duties;

iv. There is an ongoing employee training programme which enables employees to have sufficient knowledge to understand and discharge their AML/CFT responsibilities; and

v. The Compliance and Internal Audit functions are resource adequately in terms of people, IT systems and budget to implement, administer and monitor the AML/CFT program requirements effectively.

**4.3 Role of the Compliance Officer**

a. Every insurance company and broker shall for the purpose of securing compliance with Section 19 (3) of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (Act No. 13 of 2009) designate a manager or official employed at a managerial level as the CO of that institution[2]. The CO must be approved by the Bank and must satisfy the definition of an "officer" as contained in the respective legislation[17] that governs financial institutions. Accordingly, the CO must satisfy the "fit and proper" requirements outlined in section 11 of the Insurance Act No. 17 of 2016.

b. Where a company has five (5) or fewer employees, as may be the case with an insurance broker, the most senior employee shall be the CO. Where the company is part of a financial group, consideration may be given to the suitability of an applicant from within the group, provided that appropriate service level arrangements are in place.

c. As far, as is practical, the CO must have sufficient authority, independence and seniority to be able to effectively carry out his duties in accordance with the FOR. The identity of the CO must be treated with strictest confidence by the employees of the institution.

d. The CO must have the necessary knowledge and expertise to effectively discharge his role and responsibilities, including keeping abreast of the latest developments in ML/TF techniques and the AML/CFT best practices within the industry. Consequently, the CO should possess professional qualifications/ certification in AML/CFT. Notwithstanding, on an ongoing basis, insurance companies/brokers must ensure that the CO and other staff receive specialized training that is appropriate to their particular job function, so that they are able to effectively discharge their duties. Specialized training on the prevention and detection of ML/FT include, but is not limited to:

[2] Section 19 (3), The person identified in subsection (1) (a) shall be a compliance officer at management level responsible for establishing and maintaining compliance with the requirements of section 18.

i. AML/CFT legislative and regulatory requirements;

ii. The FATF 40 Recommendations, including ML/TF typologies;

iii. The identification, assessment and management of ML/FT risk;

iv. The design and implementation of risk based internal systems of AML/CFT control;

v. The design and implementation of AML/CFT compliance testing and monitoring programs;

vi. Review and handling of internal unusual or suspicious activity reports;

vii. The identification and handling of completed and attempted suspicious activity and transactions;

viii. The process for submitting a suspicious activity or transaction report to the FIU;

ix. The handling of monitoring, production and restraint orders received from law enforcement agencies;

x. The ML/TF vulnerabilities of relevant services and products;

xi. ML/TF trends and typologies; and

xii. Managing 'tipping off' risk.

e. Good governance practices require that the CO should be independent of the receipt, transfer or payment of funds, or management of customer relationships and assets. In considering the independence of the CO, consideration should be given to any potential conflicts of interest that may arise between the compliance function and any other responsibilities discharged by the CO. In determining independence the following should be taken into account:

i. The nature of the reporting lines between the CO and management of the insurance company. Ideally, the CO should have a direct reporting line to senior management and where necessary to the Board of Directors (or relevant Committee of the Board) of the institution. The CO should not have a reporting line to a senior manager with business line responsibilities. For smaller companies where independence may not be practical, consider administrative reporting to a business line manager and functional reporting to a more senior officer or to the Board. Ultimately, the insurance companies and brokers must be able to demonstrate the independence of the CO in form in instances where practically, independence cannot be achieved functionally.

ii. Potential conflicts of interest between their compliance responsibilities and any other responsibilities that the CO may have. In general, the CO should not have any other responsibilities than that of compliance. However, where this is not feasible, insurance companies and brokers should make appointments that as far as possible, avoid conflicts of interest.

- The remuneration structure. Insurance companies should ensure that remuneration of the CO is not related to the performance of any one-business line within the organization.

iv. For consistency and to ensure ongoing attention to the compliance regime, the appointed CO may delegate certain duties to other employees. However, where such a delegation occurs, the CO retains responsibility and accountability for the compliance programme.

v. The CO must have:

- Unfettered access to, and direct communications with Senior Management and the Board;
- Timely and uninhibited access to customer identification, transaction records; and
- Other relevant information throughout the organization.

**4.4 Responsibilities of the CO**

The CO has overall responsibility for the implementation of the AML/CFT programme. At a minimum, the CO must perform the functions and duties as prescribed in AML/CFT Act and Regulations among other things should:

i. Have oversight of the AML/CFT control activity in all relevant business areas for the purposes of establishing a reasonable threshold level of control consistency throughout the company;

ii. Keep the AML/CFT programme current relative to the insurance companies and brokers identified inherent risks and giving consideration to local and international developments in ML and TF;

iii. Conduct regular risk assessments of the inherent ML and TF risks including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF risks and develop appropriate control mechanisms;

iv. Conduct periodic assessments of AML/CFT control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF risks are addressed;

v. Ensure systems resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the insurance companies and brokers;

vi. Develop written AML/CFT policies and procedures that are kept up to date and approved by the Board;

vii. Ensure that ongoing training programmes on ML and TF are current and relevant and are carried out for all employees, senior management and the Board;

viii. Ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information; and

ix. Report pertinent information to the Board and Senior Management regarding the adequacy of the AML/CFT framework or any associated issues.

**5.0 INDEPENDENT TESTING**

Insurance Companies/Brokers must conduct independent testing of their compliance programme. It is important that these reviews are performed by auditors who have had appropriate AML/CFT training and experience in respect of ML and TF risk and an appropriate level of knowledge of the regulatory requirements and guidelines.

**5.1 External Audits**

a. Reviews of the insurance companies and brokers AML/CFT policies, procedures and processes for compliance with legislation must be conducted annually.

b. External audits of insurance companies and brokers with agency arrangements must include a sample of business introduced by incorporated agents of the insurance company. The external auditor should also assess the controls put in place by the insurance companies and brokers to ensure that the agents comply with the company's compliance programme and those agents are included in the insurance company's AML/CFT training.

**5.2 Internal Audits**

a. The Internal Auditor should perform regular reviews to evaluate the adequacy of implementation of the Insurance Company/Broker AML/CFT policies, procedures and systems. The Bank may also request that an Insurance Company/Broker conduct an internal AML/CFT audit if, in the Bank's opinion, such an audit is warranted. The frequency of internal audit review may be determined by the company commensurate with its complexity, size and risk profile, but at a minimum should be conducted every three (3) years. The basis for the audit frequency must be clearly articulated in the Insurance Company/Broker audit policy and scope.

b. The review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor and the Bank have been satisfactorily addressed.

c. The internal audit should also review the risk assessment carried out by the company to ensure that it is sufficiently comprehensive. The adequacy of the compliance programme should also be reviewed to ensure that it is effectively mitigates any identified risks.

d. Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation should be made available for Bank's review upon request. Any breaches, policy or procedure exceptions or other deficiencies noted during the audit should be documented in an audit report and reported to senior management and the Board or a designated committee in a timely manner. Senior management should advise on corrective actions to address deficiencies and a timeline for implementing such actions. The Board or designated committee and audit should track audit deficiencies and ensure that corrective actions are implemented in a timely manner.

e. The internal audit would include, *inter alia:*

   i. A review of the insurance company/broker risk assessment and risk rating process for reasonableness given its risk profile (services, policy holder and geographic locations (both insurance company and its policy holders locations));

   ii. Determining the adequacy of the Insurance Company/Broker ML/TF risk assessment framework and application of a risk-based approach in the design of its AML/CFT policies, procedures and controls;

iii. Appropriate risk-based transaction testing to verify adherence to the AML/CFT record keeping and reporting requirements;

iv. An evaluation of management's efforts to resolve breaches and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable;

v. A review of employee training for effectiveness, completeness and frequency and the extent of employees' and officers' (including senior management's) compliance with established AML/CFT policies and procedures;

vi. A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for AML/CFT compliance including a review of the criteria and processes for identifying and reporting suspicious transactions;

vii. An assessment of the overall process for identifying and reporting suspicious activity, including a review of 'not filed' (closed not suspicious) internal suspicious transactions/activity reports to determine the adequacy, completeness and effectiveness of the adjudication process. It should be noted that the internal audit review does not include a review of actual SAR/STRs filed with the FIU.

f. The internal audit review should include interviews with key employees, such as staff of the compliance unit, customer facing employees handling transactions and their supervisors to determine their knowledge of the AML/CFT legislative requirements and the insurance companies and brokers policies and procedures.

**6.0 RISK-BASED APPROACH[3]**

a. The BOG issued Corporate Governance Guidelines to the insurance industry in July 2019. This Guideline sets out *inter alia*, the minimum standards that are expected of a risk management framework of an insurance company. Although the aforementioned Guidelines do not refer to AML/CFT, the Bank will adopt a risk-based approach to this specific area and expects licensees to incorporate AML/CFT in their risk management frameworks.

b. Where policyholders are assessed to be of higher money laundering and terrorist financing risks, insurance companies shall take enhanced measures to manage and mitigate those risks. Correspondingly, where the risks are lower, simplified measures may be applied. Simplified measures include reducing the frequency of customer identification updates or reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

c. An insurance company shall identify, assess and take effective action to mitigate money laundering and terrorist financing risks and adopt a holistic approach to the Risk Based Approach and should avoid a silo approach when assessing the relationship between risks.

[3] See Annex A, Examples of Risk Factors for ML/TF Risk Assessments of Insurance Entities

d. An insurance company may assess the money laundering and terrorist financing risks of individual customers by assigning appropriate risk rating to their customers.

e. While there is no agreed upon set of risk factors and no one single methodology to apply these risk factors in determining the appropriate risk rating of policy holder, an insurance company shall consider the following factors:

In relation to country risk, customers with residence in or connection with high-risk jurisdictions for example:

- those that have been identified by FATF, as jurisdictions with strategic AML deficiencies;
- countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- countries which are vulnerable to corruption; and
- those countries that are believed to have strong links to terrorist activities.

f. In assessing the country's risk associated with a policy holder, consideration may be given to data available from the United Nations, the International Monetary Fund, the World Bank, the Financial Action Taskforce, among others and the insurance company's own experience or the experience of other group entities, where the insurance company is part of a group, which may have indicated weaknesses in other jurisdictions.

g. The following are examples of customers who might be considered to carry lower money laundering risks:

- customers who are employed with a regular source of income from a known legitimate source which supports the activity being undertaken;
- the positive reputation of the customer, e.g. a well-known, reputable public or private company, with a long history that is well documented by independent sources, including information regarding its ownership and control; and,
- a public entity.

h. Some customers, by their nature or behaviour might present a higher risk of money laundering and terrorist financing. Factors might include:

- a politically exposed person, or the public profile of the customer indicating involvement with, or connection to, politically exposed persons;
- complexity of the relationship, including use of corporate structures, trusts and the use of nominee accounts where there is no legitimate commercial rationale;
- a request to use numbered accounts or undue levels of secrecy with a transaction;
- involvement in cash-intensive businesses;
- nature, scope and location of business activities generating the funds or assets, having regard to sensitive or high-risk activities;
- where the origin of wealth cannot be easily verified; or
- retail participants tend to have a greater level of money laundering and terrorist financing risk associated to them in contrast to wholesale customers who usually will have a regulatory status and an established business. Persons engaged in money laundering and financing of terrorism will tend to avoid licensing obligations and regulatory scrutiny preferring the opacity of private corporations and trusts.

**7.0 KNOW YOUR CUSTOMER PRINCIPLES**

a. To counter attempts of money launderers from using insurance companies in Guyana, every company must use the "Know Your Customer" principle in their day-to-day business activities. This is the driving force behind these Guidelines and international legislation to counter money laundering and forms the core of these Guidelines.

b. The overriding requirement behind the principle of "Know Your Customer" is to establish the identity of the party(ies) wishing to create a business relationship. This applies equally wherever the applicant may be based and whether the applicant is an individual, corporation, trust, nominee or other.

c. "Know Your Customer" principles do not infringe on the confidentiality and privacy of client affairs. Insurance companies/brokers are prohibited from entering or continuing a business relationship with any person who resides in jurisdictions where there are secrecy laws that prohibit the release of any KYC information or which laws prevent an obstacle to the KYC due diligence process.

d. Insurance companies must develop KYC policies and procedures that aim to identify the types of customers or beneficiaries that are likely to pose a higher than average risk of money laundering and financing of terrorism activities.

e. Prior to the establishment of a business relationship, insurance companies must assess the characteristics of the required product, the purpose and nature of the proposed business relationship and any other relevant factors in order to create and maintain a risk profile of the customer. Based on this assessment, insurance companies will decide whether or not to accept the business relationship.

f. In assessing the risk profile of a policy holder or beneficiary, insurance companies must consider the following factors:

   i. nature of the insurance policy, which is susceptible to money laundering and terrorism financing risks, such as single premium policies;

   ii. origin of the policy holder or beneficiary such as place of birth, residency, the place where the policy holder or beneficiary's business is established, the location of any other party the customer conducts business, such as, high risk and non-cooperative jurisdictions designated by FATF or those known to the insurance company to lack proper standards in the prevention of money laundering and terrorist financing;

   iii. nature of the policy holder's or beneficiary's business, which may be particularly susceptible to money laundering and terrorist financing risks, such as money changers or casinos that handle large amounts of cash;

   iv. for a corporate policy holder's or beneficiary, unduly complex structure of ownership for no good reason;

   v. means of payment as well as type of payment such as cash, wire transfer, third party cheque without any apparent connection with the prospective customer or beneficiary; and

   vi. any other information that may suggest that the customer or beneficiary is of high risk.

**8.0 CUSTOMER DUE DILIGENCE**

**8.1 General Provisions**

a. Insurance companies shall conduct due diligence of their policyholders before and after entering into a business relationship. The Board of directors is required to formulate policies on the information required from customers that will take into consideration the risk profile of customers.

b. Insurance companies shall not keep anonymous accounts or accounts in obviously fictitious names. Insurance companies are required to undertake the following measures in regard to the principle of due diligence:

i. Identify the customer and verify the customer's identity using reliable, independent source documents, data or information;

ii. Identify the beneficiary and verify the identity of the beneficiary such that the insurance company is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, insurance companies should understand their ownership and control structure;

iii. Obtain information on the purpose and intended nature of the business relationship between the customer and the insurance company; and

iv. Conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and accounts throughout the course of the business relationship, to ensure that the transactions being conducted are consistent with the insurance company's knowledge of the customers or beneficiary, their businesses and risk profile, including, where necessary, identifying the source of funds;

v. Insurance companies may apply simplified due diligence in respect of a customer where there is no suspicion of money laundering and;

vi. Where the risk profile of the customer is low;

vii. There is adequate public disclosure in relation to the customers; or

viii. There are adequate checks and controls from the customer's country of origin or the source of the funds.

c. Insurance companies shall take reasonable steps to satisfy themselves as to the identity of their customers or beneficiaries, which should be objective and reasonable.

d. If claims, commissions, and other monies are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these monies should also be the subject of identification and verification.

e. Insurance companies shall pay special attention to all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

f. Where the insurance company is unable to satisfy itself on the identity of the customer or beneficiary, it must not commence a business relationship or perform the transaction and should consider making a suspicious transaction report as required under the Act.

g. Where the insurance company has already commenced the business relationship and is unable to satisfy itself on the identity of the customer or beneficiary, it should consider terminating the business relationship, if possible, and making a suspicious transaction report as required under the Act.

h. Insurance companies must hold either original documents or suitably certified copies of original documents of identification on its files. Where suitably certified copies are obtained, the insurance companies should ensure that the pages containing the relevant information are copied e.g. the pages containing the relevant names, reference number, date, and country of issue etc.

It should be remembered that it is not possible for an Insurance Company to delegate the responsibility for Customer Due Diligence to another party; however, in certain circumstances it is acceptable for the collection of the identity documents to be delegated.

i. Where applicants put forward documents with which an insurance company is unfamiliar, either because of origin, format or language, the Insurance Company must take reasonable steps to verify that the document is

indeed genuine, which may include contacting the relevant authorities. Where the insurance company is unable to verify a document they should consider whether they have sufficient documentary evidence on the applicant to be satisfied as to their identity. In the absence of being so satisfied the application should not proceed.

j. The details of requirements given in section 9 should be considered the minimum standard and the insurance company should adopt a risk-based approach when assessing the documents required. This is also applicable to situations where a list of persons is able to act on behalf of a company. When taking a risk-based approach, the insurance company should also consider whether it would be appropriate to identify some or all of the signatories.

k. Prior to placing reliance on third parties in other jurisdictions insurance companies/brokers must be satisfied that there are no laws in the jurisdictions in which the third party operates that would prohibit the fulfilment of the CDD operations (e.g. bank secrecy laws).

**8.2 Due Diligence of Individual/Natural Customer**

a. Insurance companies shall institute effective procedures for obtaining satisfactory evidence of the identity of individual customers or beneficiaries including obtaining information about:

i. true name or name(s) used,
ii. identification card, passport or driver's license or any other official means of identification,
iii. current address,
iv. date of birth,
v. nationality; and
vi. occupation/business.

b. And this information shall be evidenced by the relevant copies of the documents taken after the verification of the original copies.

c. If there is any doubt that an identification document is genuine, contact should be made with relevant authority to verify the information.

d. Insurance companies shall maintain the current residential address of their policyholders at all times of the tenure of the policy.

e. Insurance companies shall also identify the source of funds of policyholders or beneficiaries if the policyholders or beneficiaries are assessed to be of high risk based on the factors set out in section 14.

**8.3 Due Diligence of Corporate Customers**

The following documents or information will be obtained in respect of corporate customers or beneficiaries:

i. A suitably certified copy of the Certificate of Incorporation or equivalent document establishing the registered number of the company or document of listing, and, if not on this document, evidence of the registered office of the contracting party. If the registered office is not the address shown on the application then the Insurance Company must be satisfied as to the reason for this address to be used;

ii. Memorandum and Articles of Association (if insurance company considers necessary having regard to the risk of the particular customer);

iii. A list of all directors;

iv. A list of the officers from whom the insurance company is to take instructions and specimen signatures. The insurance company should ensure that the officer(s) listed are qualified and experience in their respective roles and that their identification information are properly vetted;

v. Where possible a copy of the latest annual returns should be submitted in respect of the body corporate in accordance with the law under which it is established.

vi. Confirmation that the company has not been, or is not in the process of being dissolved, struck off, wound up or terminated.

b. A company may be considered to be of low risk if:

i. The company is listed on the stock exchange in Guyana.

ii. The company is owned by the Government of Guyana.

iii. The company acquires an insurance policy for pension schemes which does not have a surrender clause and the policy cannot be used as collateral; or

iv. The company acquires a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages.

v. The company is regulated by a supervisory body as defined in the Act.

c. Where a company is effectively controlled by an individual or a small group of individuals, insurance companies must consider whether it is necessary to verify the identity of such individual(s).
d. Insurance companies shall exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficiaries of such companies must be obtained.

**8.4 Un-incorporated Business**

In the case of partnerships and other unincorporated businesses whose partners are not known to the insurance company, satisfactory evidence must be obtained to verify the identity of at least two partners and all authorized signatories designated to sign insurance contracts.

**8.5 Trust Accounts**

a. Where the applicant for a business relationship is a trustee, the insurance company must satisfy itself that:

i. The Trustees have been identified in accordance with the appropriate verification requirements for corporate applicants or individuals. Where there is more than one Trustee, appropriate identification must be obtained for each individual;

ii. Satisfactory evidence of proper appointment of the Trustees has been received e.g. Extracts of the Deed of Trust;

iii. The nature and purpose of the trust is known;

iv. The source or origin of the assets under the trust is known and the insurance company considers it satisfactory;

v. The persons from whom the insurance company is to take instructions have been identified and specimen signatures have been obtained; and

vi. The trustees have provided details of the parties to the trust at the time the application was being made. These are as follows:

- The settlor(s), whose details should include the full name(s), date(s) of birth and, if they are still living, the current addresses of any individuals. If the settlor is not alive the date of death should be included. If the settlor has been other than an individual, or individuals, the trustee should provide sufficient information for the Insurance Company to identify the settlor(s) should they wish to do so;

- Any protector(s), whose details should include the full name(s), date(s) of birth and the current addresses of any individuals;

- All beneficiaries (as and when defined).

b. The list of beneficiaries provided by the trustees might include certain beneficiaries whose identity the trustees have not verified such as infants, and beneficiaries defined only by class.

c. Where a class of beneficiaries is disclosed, the insurance company should verify that the class exist and undertake necessary checks it considers necessary to achieve this. It is not necessary at this point to identify the individual members of this class.

d. The list must also include those contingent beneficiaries named at the time of the application for business, which may include charities.

e. The details of beneficiaries should include the full name(s), dates of birth and current addresses of any individuals, and sufficient information to identify any other class, corporate entity, charity or other beneficiary.

f. In any event the insurance company must verify the identity of the beneficiary, as appropriate, should payment by the insurance company directly to a beneficiary, or for the benefit of a beneficiary, be requested by the trustees (whether named on the original list provided by the trustee, subsequently added, or included originally only by class).

g. In the absence of satisfactory evidence, or where it may be impossible to identify the parties involved in the application at a date in the future due to insufficient information, the application for a business relationship shall not proceed any further.

h. Where a trustee who has been verified is replaced, the identity of the new trustee must be verified before they are allowed to exercise any control over the assets.

i. The insurance company may wish to undertake regular reviews of the parties to a trust through the duration of the policy, the timing of such reviews to be at the discretion of the insurance company.

**8.6 Pension Fund Plans**

a. Where the policy holder for a business relationship is the trustee of an occupational retirement arrangement the insurance company must satisfy itself that:

i. The trustees have been identified in accordance with the appropriate verification requirements for corporate applicants or individuals. Where there is more than one trustee, appropriate identification must be obtained for each individual;

ii. Any scheme administrator has been identified in accordance with the appropriate verification requirements for corporate applicants or individuals;

iii. Satisfactory evidence of proper appointment of the Trustees (and Scheme Administrator) has been received e.g. Extracts of the Trust Deed;

iv. The source or origin of the assets under the trust is known and the insurance company considers it satisfactory;

v. A list of the persons from whom the insurance company is to take instructions and specimen signatures have been obtained (although their identity need not be verified); and

vi. The trustees (and/or Plan Managers) have provided details of the parties to the trust at the time the application was being made. These will be:

- The sponsoring employer and members of the scheme. The details of members should include the full name(s), dates of birth and current addresses;

- Where the beneficiaries are named the trustee should list each. The details of beneficiaries should include the full name(s), dates of birth and current addresses of any individuals;

- Where the beneficiaries are not individuals, the details of beneficiaries should include sufficient information to identify any class, corporate entity, charity or other beneficiary;

- Where the beneficiaries are disclosed as being a group of employees of the sponsoring employer this may be considered sufficient.

- Where a class of beneficiary other than employees of the sponsoring employer is disclosed the insurance company should satisfy itself that the class does exist and undertake whatever steps it considers necessary to achieve this.

**8.7 Other Annuity Schemes**

a. Where an applicant for a business relationship opts to purchase an annuity all the parties to the scheme should have their identities verified as appropriate.

b. In the absence of satisfactory evidence, the application for a business relationship shall not proceed any further.

**8.8 Other Applicants**

a. Other Applicants for a business relationship may arise and the insurance company should obtain relevant suitable evidence of their/its identity.

b. As a guide, where the application for a business relationship is in the name of another category of applicant the insurance company should confirm the following:

i. The applicant exists. This may be achieved by obtaining copies of the constitution or similar;

ii. This investment is legitimately being made on behalf of the organisation;

iii. Evidence of the current address for delivery of documents should have been received. This may be a copy of a recent utility bill not exceeding six (6) months.

iv. A list of all directors, executives or committee members is received, and, verification of the identity of at least two of them, is obtained;

v. A copy of the latest annual report and accounts is obtained where possible;

vi. A list of the officers from whom the insurance company is to take instructions and specimen signatures is held. The insurance company should verify the identity of at least two of the principal signatories. When signatories change, the insurance company should ensure that it continues to hold verified identity of at least two signatories. Under certain circumstances, the insurance company may wish to verify the identity of additional or all of the signatories.

c. In the absence of satisfactory evidence, the application for a business relationship shall not proceed any further.

**8.9 Powers of Attorney and Third Party Mandates**

a. When an application for a business relationship is received from an applicant acting under a power of attorney or similar, evidence of identification should be obtained for the holder(s) of the power(s) of attorney and/or third party mandates in addition to the evidence of identification for the person granting the power. The insurance company should be satisfied that the power or mandate exists. The reason for granting the power of attorney should also be recorded.

b. In assessing whether a power of attorney is adequate for the purpose(s) intended, insurance companies should be guided by the requirements of the Powers of Attorney (Amendment) Act No. 2 of 2022.

**8.10 Accounts for Children**

When an applicant for a business relationship is a child who is not in possession of suitable identification documents the insurance company may rely on a written confirmation of details of identity of the applicant from a parent or guardian providing that:

i. The identity of the parent or guardian providing the confirmation has been verified in accordance with these Guidelines;

ii. The relationship between the child and the person providing the confirmation is established to the satisfaction of the insurance company; and

iii. The insurance company should endeavour to verify the identity of the child as set out in these Guidelines when payment to the child is requested. If at that time the child is still not able to provide suitable documentary evidence of identity the insurance company should decide whether it is satisfied with the confirmation received and take such additional action as it considers necessary.

**8.11 Politically Exposed Persons (PEPS)**

a. The decision to undertake a transaction with a PEP, a family member or close relative of a PEP, and transactions in which a PEP is the beneficial owner shall be taken at a senior level and the guidelines for making such decisions shall be clearly spelt out in writing in the customer acceptance policy. All transactions involving a PEP shall be subject to enhance monitoring on an ongoing basis.

b. Insurance companies shall gather sufficient information on any prospective policy holder falling under this category including checking all the information available on the person in the public domain, verify the identity of the person and seek information about the source of wealth /funds before accepting the PEP as a customer.

c. EDD requirements may also be applied to customers who become PEPs subsequent to the establishment of the business relationship.

**8.12 Simplified Due Diligence (SDD)**

In some lower risk scenarios, and subject to applicable local laws, the standard level of due diligence may be simplified. Examples of lower risk scenarios are:

a. Products that only pay out at death and/or in the event of disability;

b. Customers that are publicly listed companies on exchanges with adequate disclosure requirements for transparency of beneficial ownership;

c. Transactions involving de minimis amounts, such as life insurance policies where the annual premium is no more than USD/EUR 1 000 or a single premium of no more than USD/EUR 2500;

d. Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

e. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme (e.g., small insurance premiums);

f. Insurance products or services that provide appropriately defined and limited services to certain types of policyholders, so as to increase access for financial inclusion purposes.

In those situations, SDD may include verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g., if account transactions rise above a defined monetary threshold); reducing the frequency of customer identification updates; reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold; not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

**8.13 Acceptable Applicants**

a. Where the insurance company believes that the applicant for the business relationship is an acceptable applicant, the acceptable applicant may be accepted without detailed identification and verification checks being made, provided that the insurance company has reasonable grounds for believing that the applicant for business is an acceptable applicant.

b. The insurance company should record in detail on the client file the basis on which the acceptable applicant has been accepted.

c. Where the acceptable applicant is acting as a trustee, nominee or on behalf of someone other than itself as principal, the insurance company may accept the identification of the acceptable applicant, but must still satisfy themselves as to the evidence of their appointment and must provide details of the identity of any other persons involved as set out in these Guidelines.

d. Where it is necessary for the identity of one of the parties to be verified, for example where payment is to be made directly to a beneficiary of a trust, it is acceptable to rely on an acceptable applicant to provide verification of identity documents. Where this happens an acceptable applicant may provide either:

- A copy of documentary evidence held on the acceptable applicant's file, which the acceptable applicant had used (historically) to verify the identity of the party. This may have been obtained some time ago and might now have expired (but was current at the time that identity was verified). Such a copy document may be accepted as long as the information on that verification document is the same as the application form and provided that the information supplied meets the requirements of these Guidelines; or

- Originals or copies of documents obtained specifically in relation to the particular transaction.

e. All copy documentary evidence passed to the insurance company must be certified by the acceptable applicant as being a true copy of either an original or copy document held on its file.

f. If this evidence is not provided by the acceptable applicant, the insurance company must either obtain the evidence themselves, or obtain satisfactory evidence from an alternative source.

The insurance company must monitor the status of all acceptable applicants on an ongoing basis.

**8.14 Enhanced Due Diligence (EDD)**

a. In higher risk scenarios, EDD should be performed. Higher risk scenarios could include, for example, situations involving risk indicators such as the request for a payment to a third party who is not the beneficiary and has no apparent relationship with him or where multiple surrenders seem to have no apparent economic justification or where the origin of funds is not clear.

b. EDD should include obtaining additional information including the intended nature of the business relationship, and on the source of wealth or source of funds of the customer. Insurers and intermediaries should also extend the range of information collected to the policyholder ownership structure, or review his/her tax residency, connected parties or other risk factors; and seeks to independently corroborate customer information through public or other available sources.

c. EDD is also required for business relationships with all foreign PEPs and with higher risk domestic PEPs or international PEPs. This involves obtaining senior management approval before establishing or continuing the relationship, take reasonable steps to establish the source of wealth and the source of funds and conduct enhanced monitoring on the relationship. In instances where higher risks are identified in relation to beneficiaries of life insurance policies or their beneficial owners, senior management must be informed and enhanced scrutiny must be conducted on the whole business relationship with the policyholder, prior to a pay-out being made. This includes determining whether filing a STR is necessary.

d. Additional controls for higher risk situations may include close monitoring such as increased monitoring of transactions (frequency, thresholds, volumes, etc.). In some cases, insurers and intermediaries shall also conduct a compliance review or get senior management approval on the establishment of or the offering of any additional account/policy/contract or relationship, or conduct more frequent customer reviews.

**8.15 High Risk Customers[4]**

a. Insurance companies shall apply enhanced due diligence in respect of high-risk customers or beneficiaries. Some examples of high risk customers or beneficiaries are:

   i. Customers that are legal entities whose structure makes it difficult to identify the ultimate beneficial owner or controlling interests. (Note: This can happen at inception or, subsequently, an individually owned insurance policy can be assigned to a legal entity. KYC/CDD processes should apply at both stages.)

   ii. Policy holder and/or the beneficiary of the contract are companies whose structure makes it difficult to identify the beneficial owner, e.g., multiple layers or because the entity's ownership structure crosses jurisdictions; Policy holder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form:

   - Occupation with a low average income and the policy has high ongoing deposits.
   - A history within an occupation with a higher risk for ML/TF due to local crime typologies, high access to cash based businesses or international exposure.
   - Customers who are reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information.
   - Customer transfers the contract to another insurer; (low risk after a long relationship, higher risk if after a short period of time, especially with high fees).
   - Insurer is made aware of a change in beneficiary only when the claim is made.
   - Customer incurs a high cost by seeking early termination of a product.
   - Customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive.

[4] Table 5

For high-risk customers, the following additional measures must be applied to enhance due diligence:

- Obtaining senior management approval for establishing business relationship;
- Obtaining comprehensive customer profile information e.g. purpose and reasons for entering the insurance contract, business or employment background and source of funds;
- Assigning a designated staff to serve the customer who bears the responsibility for customer due diligence and ongoing monitoring to identify any unusual or suspicious transactions on a timely basis;
- Requisition of additional documents to complement those which are otherwise required; and
- Certification by appropriate authorities and professionals of documents presented.

**8.16 On-Going Due Diligence on Existing Customers or Beneficiaries**

a. Insurance companies shall conduct on-going due diligence on existing customers and particularly shall pay attention to all requested changes to the policy or exercise of rights under the terms of the contract. Enhanced due diligence must be conducted on high-risk customers.

b. Some of the transactions after the establishment of business relation that will require the enhanced due diligence include:

- There is change in beneficiaries for instance, to include non-family members, request for payments to persons other than beneficiaries:
- There is significant increase in the amount of sum insured or premium payment that appears unusual in the light of the income of the policy holder;
- There is use of cash or payment of large single premiums;
- There is payment or surrender by a wire transfer from or to foreign parties;
- High frequency of changes in a policy;
- There is payment by banking instruments which allow anonymity of the transaction,
- There is change of address or place of residence of the policy holder or beneficiary,
- There are lump sum top-ups to an existing life insurance contract,
- There are lump sum contributions to personal pension contracts,
- There are requests for prepayment of benefits,
- There is use of the policy as collateral or 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,
- There is change of the type of benefit for instance, change of type of payment from an annuity into a lump sum payment,
- There is early surrender of the policy or change of the duration where this causes penalties or loss of tax relief,
- The insurance company is aware that it lacks sufficient information about the policy holder or beneficiary; or
- There is suspicion of money laundering.

**8.17 Non-Face-To-Face Transactions**

a. Where possible insurance companies shall carry out face-to-face interviews to conduct due diligence particularly for high-risk customers.

b. Where a face-to-face interview is not conducted, for example where the transactions are conducted via the internet, insurance companies shall apply equally effective policyholder identification procedures and on-going monitoring standards as for face-to-face policyholders.

c. Insurance companies shall carry out the following specific measures to mitigate the risk posed by such customers of non-face-to face transactions.

d. Certification of identity documents presented by suitable certifiers.

e. Requisition of additional documents to complement those required for face-to-face customers.

f. Completion of on-line questionnaires for new applications that require a wide range of information capable of independent verification such as confirmation with a government department:

   i. Independent contact with the prospective policy holder by the insurance company,

   ii. Require the payment of insurance premiums through an account in the policy holder's name with a bank,

   iii. More frequent updates of the information on customers of non-face-to-face transactions; or

   iv. In the extreme, refusal of business relationship without face-to-face contact for high-risk customers.

**8.18 Intermediaries**

a. Insurance Companies may rely on insurance intermediaries to perform customer due diligence procedures. However, the ultimate responsibility for knowing the policyholder or beneficiary always remains with the insurer. Insurance companies shall therefore satisfy themselves as to the adequacy of policyholder's due diligence procedures conducted by the insurance intermediaries.

b. Where insurance companies rely on the intermediary for due diligence, they shall immediately obtain the necessary information concerning the relevant identification data and other documentation pertaining to the identity of the policyholder or beneficiary from the insurance intermediary.

c. The insurance intermediary shall obtain satisfactory evidence of the identity and legal existence of the persons applying to do business with it. The evidence shall be verified by reliable documents or other verifiable and independent means.

d. The insurance intermediary shall ensure that all requirements imposed by law relating to records and documentation are met. All customer records shall remain up to date, relevant and easily accessible.

e. The insurance intermediary shall submit such information to the insurer upon request and without delay.

f. The insurance intermediary shall monitor on a continuous basis its business relationship with its customers.

g. The insurance intermediary shall not engage in a business relationship with a client who fails to provide evidence of their existence. The insurance intermediary shall not keep anonymous accounts or accounts in fictitious names of their clients.

h. Insurance intermediaries shall adopt a risk based approach where they employ enhanced customer due diligence for high-risk category of customers.

i. Insurance companies shall undertake and complete their own verification of the customer and beneficial owner if they have any doubts about the ability of the insurance intermediary to undertake appropriate due diligence.

**8.19 Beneficiaries**

a. For life or other investment-related insurance business, insurance companies shall, in addition to the customer due diligence measures required for the customer and the beneficial owner, conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment related insurance policies:

- that the beneficiary is identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;

- that is a legal arrangement or designated by characteristics or by category such as spouse or children, at the time that the insured event occurs or by other means such as under a will, obtaining sufficient information concerning the beneficiary to satisfy the insurance companies that it will be able to establish the identity of the beneficiary at the time of the pay-out. The information collected shall be recorded and maintained in accordance with these Guidelines.

b. Verification of the identity of beneficiaries and persons known to be likely to benefit must, where possible be undertaken as soon as the beneficiary or beneficiaries are identified or designated. Where it is not possible to do so, verification must be undertaken prior to any (or on behalf of) that beneficiary.

**8.20 Acquisition of a Business or Block of Customers**

a. There are circumstances where an insurance company may acquire a business with established business relationships or a block of customers, for example, by way of portfolio purchase.

b. Before taking on this type of business, in order to avoid breaching the Guidelines, an Insurance Company should undertake enquiries on the vendor sufficient to establish the level and the appropriateness of identification data held in relation to the customers and the business relationships of the business to be acquired.

c. An insurance company may consider it appropriate to rely on the information and documentation previously obtained by the vendor where the following criteria are met:

- The insurance company has assessed that the customer due diligence policies, procedures and controls operated by the vendor were satisfactory; and

- The insurance company has obtained from the vendor, identification data for each policyholder acquired.

d. Where deficiencies in the identification data held are identified (either at the time of transfer or subsequently), the accepting insurance company must determine and implement a programme to remedy such deficiencies.

**8.21 New Technologies**

a. Insurance companies shall take reasonable measures to prevent the use of new technologies for money laundering purposes.

b. Insurance companies shall conduct a money laundering risk assessment—

i. prior to the introduction of a new product, new business practice or new technology for both new and pre-existing products;

ii. so as to assess money laundering risks in relation to—

- a new product and a new business practice, including a new delivery mechanism; and
- new or developing technologies for both new and pre-existing products.

c. The outcome of such assessment shall be documented and be submitted to the Bank as part of its submission for approval of new polices or upon request.

**9.0 IDENTIFICATION REQUIREMENTS**

This section details the standard minimum requirements for identifying different principals within an application for a business relationship. These are the minimum requirements and the insurance company should assess each case to decide whether additional information should be sought.

**9.1 Individual Identification Requirements (Identity)**

a. The identity of an individual is deemed to comprise of the true full name or names of the individual. Where the name of the individual has changed for a reason other than marriage the company may wish to obtain additional documents. Any previous name or names, and any aliases used should also be disclosed.

b. Once the usual residential address has been established to the satisfaction of the insurance company any change to that address may be notified to the insurance company in any way that the insurance company decides is satisfactory.

c. Where two or more individuals apply as joint applicants for a business relationship the identity of each individual must be verified.

d. In order to do this an insurance company shall either:
- Verify the identity of the individual by means of reviewing suitable identification documents; or
- Take such measures that will produce satisfactory evidence of identity.

e. In the absence of satisfactory evidence the application for a business relationship shall not proceed any further.

**9.2 Documentary Evidence of Identity**

a. The preferred documents to verify identity are either a Passport or a National Identification Card. This should be accompanied by a document or documents in section 9.1 to confirm the address.

b. Where it is not possible to obtain either a Passport or a National Identification Card then the insurance company should consider the risk profile of the application as to the documentary evidence it considers acceptable. This should be not less than two (2) other formal documents carrying appropriate personal details which show verifiable reference numbers.

**9.3 Verification of the Address of an Individual**

a. The Insurance Company shall hold on file documentary evidence of the current residential address of an individual at the time the application is made.

b. To verify the address for an individual the insurance company may obtain either an original or certified copy of one of the following issued in the name of the individual and showing the address appearing on the application:

- A utility, or rates and taxes bill;
- Proof of ownership or rental of the current address;
- A bank statement.

c. In all cases the documents seen should be the most recent available.

d. Alternatively, the insurance company may obtain a letter from the employer of the individual confirming the current address of the individual.

e. It is the responsibility of the Insurance Company to ensure that they hold a current address for an individual at all times, however, once the verification of the address of the individual has been accepted, the insurance company may accept further notification of address in any form acceptable to them.

**9.4 Inability to Certify the Address of an Individual**

a. Where the insurance company has been unable to obtain certified documentary evidence of the address of an individual, and where the Insurance Company has exhausted the options available in 9.3, the insurance company must:

i. Hold on file an address to which correspondence is to be sent.

ii. Obtain a written physical description of the location of the current address;

iii. Detail the steps attempted to produce documentary evidence and the reasons why they have failed;

iv. Carry out a risk assessment on the policy holder taking into account factors such as:
- the information provided as documentary proof of identity;
- the location of the policy holder;
- the size of the investment;
- any additional information provided by the policy holder;
- to assess whether the information already obtained cumulatively gives the insurance company sufficient information for the insurance company to be satisfied that they have identified the individual. In the absence of being so satisfied, the application for a business relationship shall not proceed any further.

b. Obtain written confirmation of acceptance “sign-off” for this application from a senior member of staff authorised to accept this business on behalf of the insurance company;

c. Ensure that the policy is identifiable for monitoring and review purposes.

d. When the insurance company is notified of any change of address for an individual for whom verification of address has not been obtained, the insurance company must endeavour to obtain verification of the new address in accordance with section 9.3.

f. Where the insurance company is still not able to verify the new address, steps “a” to “e” above must be completed. This must occur for each subsequent change of address until documentary evidence is received.

**9.5 Verification of Identification by the Insurance Company**

a. It is acceptable for an Insurance Company to carry out the verification of identity for itself, regardless of the involvement of a third party. This may either be done using their own staff or by using an outside agency specialising in this activity.

b. When either databases (or similar) or an outside agency is used the insurance company must be able to demonstrate that the information or company used is reliable and that some assessment of their correctness has been made. The overriding requirement to ensure that the identification evidence is satisfactory rests with the insurance company.

c. Where the insurance company undertakes the verification of identity (other than face to face) printouts from any data search or copies of other documents must contain:

- The name of the person who has reviewed the information;
- The date;
- Details of their source; and
- Where the information is provided by an outside agency, the name of the agency.

**9.6 Verification of Identity by a Related Party**

a. Where an employee, partner or principal of a broker or acceptable applicant is the applicant for a business relationship, either personally or in the role of an individual Trustee or Nominee, they may not act as Suitable Certifier[5] to verify the identity of either themselves or of other parties or documentation relevant to the application. Any certification of copy documents must be completed by a third party.

b. This does not apply when the application is made by an individual acting as an authorised officer of an acceptable applicant.

**9.7 Timing of Verification**

a. Where evidence of identity is required, it must be obtained “as soon as is reasonably practicable” after the applicant for a business relationship applies to enter a business relationship with the insurance company.

b. Normally, the application will not be concluded until such time as the verification is complete.

c. However, it is appreciated that it is not feasible for an insurance company to leave any monies un-invested, therefore, it is acceptable for the insurance company to invest the monies in such a way that neither the applicant for a business relationship nor insurance company are disadvantaged. Thus, the insurance company can start processing the business immediately, provided that it is at the same time taking steps to verify the

[5] See paragraph 9.8

policy holder's identity. In any event, the verification must be completed satisfactorily before the policy is issued.

d. An insurance company may wish to consider indicating in brochures or on application forms that evidence of identification must be provided and that additional verification may be needed which could result in delays in processing the investment.

**9.8 Suitable Certifier**

a. All copy documents must be certified as true copies by a Suitable Certifier. A Suitable Certifier is an individual who, by personal qualification, the position they hold within their organisation or approval by the Insurance Company, is deemed suitable to certify any copy documents provided to the Insurance Company as part of the Know Your Customer due diligence.

b. A Suitable Certifier may be:

i. An employee of the insurance company, or any group company of the insurance company;
ii. An Agent bound by contract to the insurance company, or any group company of the insurance company;
iii. An authorised representative of an embassy or consulate of the country who issued the identification document;
iv. A notary public, commissioner of oaths or attorney at law;
v. An acceptable applicant, or authorised employee of an acceptable applicant, acting in relation to the application;
vi. An authorised representative of the sponsoring employer for an approved occupational pension only.

c. The insurance company must have in place procedures, which demonstrate that where the authority under which the certification is given is not known to the insurance company, that appropriate verification of the certifier is undertaken.

d. The appointment of a Suitable Certifier is not transferable.

e. An insurance company must have verified the identity of any Suitable Certifier to the level of an individual as detailed in sections 9 (a) i and 9 (a) ii. The insurance company must hold a specimen signature of the Suitable Certifier on file and must have procedures in place to review the signatures certifying the policyholder's identification documentation produced, on a regular basis to ensure their veracity.

**9.9 Certification of Identification Documents**

a. Where the information has been obtained for this application for a Business Relationship, all copy documents must either:

i. Be signed and dated by the Suitable Certifier. The Suitable Certifier should also write their name in block letters underneath their signature and should include a statement to the effect that it is a true copy of the original; or

ii. Be accompanied by a covering letter or other document signed by the Suitable Certifier attaching the copy documents and confirming that they are true copies of the originals. The covering letter should also make reference to all documents attached.

b. Any document certified by a Suitable Certifier must also contain the following:

   i. The name of the certifier;
   ii. His occupation;
   iii. Any specific form of words to be used when certifying the documents as true copies of the original as instructed by the insurance company;
   iv. Any other provisions which the insurance company wish to impose.

c. The insurance company must take whatever steps it deems necessary to ensure that the Suitable Certifier is aware of the requirements of these Guidelines.

**10.0 LIFE INSURANCE PRODUCTS AND OTHER INVESTMENT-RELATED INSURANCE PRODUCTS[6]**

a. For the purpose of these Guidelines, "life insurance products and other investment-related insurance products", as referred to in the FATF Glossary, are understood as contracts primarily designed to financially protect the customer/policyholder and its related third parties (who include the insured, the beneficiary/ies of the contract, and the beneficial owners) against the risk of an uncertain future event – such as death or critical illness. Related third party beneficiaries may be the policyholder, or another nominated or a designated beneficiary, and can be a natural person as well as a legal entity or a legal arrangement. Life insurance products can also be bought as investment or saving vehicles and to support estate planning or pension plans.

b. Most life insurance products are designed for the long-term and some will only pay out on the occurrence of a verifiable event, such as death or retirement. However, some have saving or investment features, which may include the options for full and/or partial withdrawals or surrenders at any time. Life insurance policies can be individual policies or group policies – for example, companies may provide life insurance for their employees as part of a benefits package.

c. Generally, the ML/TF risks associated to the life insurance sector is lower than that associated with other financial products (e.g., loans, payment services) or other sectors (e.g., banking, gambling, precious stones and metal dealers). Indeed, many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime.

d. There is also a risk, even limited, that funds withdrawn from life insurance contracts could be used to fund terrorism.

Table 1 – Examples of life insurance products and indicative risk ratings (without prejudice to the other ML/TF risk factors such as transaction, distribution, geographical or customer risks).

[6] Annex B, Life Insurance Distribution Channels and Brokers

*Table 1*

| EXAMPLES OF PRODUCT DESCRIPTION | TYPICAL FEATURES | INDICATIVE RISK RATING |
|---|---|---|
| **Complex products with potential multiple investment accounts; and/or products with returns linked with the performance of an underlying financial asset**<br><br>***Example of product names:***<br>Universal Life<br>Variable Universal Life<br>Wrapper Insurance<br>Investment Linked Policies<br>Unit Linked Policies<br>Investment Linked Assurance Schemes | • Offers the ability to hold funds and/or assets<br>• May offer the option of asset transfers into the policy<br>• Full or partial underlying investments under control of the customer<br>• May have a high upper limit for the amounts of funds held | • **Higher/moderately high risk** compared with other life insurance products |
| **Products designated for High Net Worth (HNW) persons or products for individual generally with guaranteed returns**<br>***Example of product names:***<br>HNW individual Life Insurance<br>Traditional Whole Life | • Offers the ability to hold funds<br>• Only with high limit for funds held<br>• Underlying investments managed by the insurer | • **Higher/moderately high** risk compared with other life insurance products |
| Product that pays for periodic Income benefit for the life of a person<br><br>***Examples of product name***:<br>Fixed and Variable Annuities | • Offer the ability to hold funds<br>• May have a high limit for fund held<br>• Accumulation period followed by a liquidation period<br>• Underlying investments managed by the insurer | • **Moderate risk** compared with other life insurance products |
| **Product designed to provide endowments for an individual or an institution**<br>***Examples of product name:***<br>Endowments | • May offer the ability to hold funds<br>• Underlying investments managed by the insurer | • **Moderate risk** compared with other life insurance products |
| **Products subscribed by a company to pay a periodic income benefit for the life of employees**<br>**Examples of product name:**<br>Group Annuities | • Typically used for retirement savings and pension schemes<br>• Generally subscribed by a company in order to provide a future benefit to its employees<br>• Underlying investments managed by the insurer | • **lower risk** compared with other life insurance products |

| EXAMPLES OF PRODUCT DESCRIPTION | TYPICAL FEATURES | INDICATIVE RISK RATING |
|---|---|---|
| **Product that pays a lump sum, or a regular payout (annuity) to the beneficiary, in the event of the death of the insured, in the event of a long-term care or critical illness**<br>**Example of product name:**<br>Term Life Individual<br>Group Long-term Care<br>Critical Illness | • No ability to hold funds<br>• Generally payments only in case of a specific external event | • **lower risk** compared with other life insurance products |

**11.0 CANCELLATION PERIODS**

a. Where an applicant for a business relationship takes up the right to decline to proceed with a contract during a cancellation period, the circumstances surrounding the applicant's request to cancel must be considered and if they are viewed as suspicious then this suspicion must be reported. That being the case, reporting procedures must be followed.

b. Any payment out to a policyholder as a result of such a right being exercised should normally be to the ceding account from which the monies were originally sent. If the payment out is to be by cheque it should be payable to the policyholder and marked "Account Payee Only".

c. Under certain circumstances payment may be to a third party account, for example a "client money account", or payment to the original account may be impossible, for example if the account has subsequently been closed. In these circumstances the insurance company must be satisfied of the connection between the payee and the Client, and must also consider whether the payment request is suspicious, in which case, reporting procedures must be followed.

**12.0 ASSIGNMENTS AND TRANSFERS OF OWNERSHIP**

a. Where a policy is assigned to a third party, verification of identity should be obtained either before assignment takes place, or as soon as reasonably practicable thereafter.
b. Whether an assignment has been notified or not, when a payment is to be made from the policy (as a withdrawal, surrender or claim) to an account not in the name of a verified person or entity, the insurance company must ensure that verification of identity of the account holder has been completed in accordance with these Guidelines before payment is made.

**13.0 EXISTING CLIENTS AND RETROSPECTIVE REVIEW**

**13.1 Retrospective Review**

a. The insurance company must have in place a programme to review the identification documents on each file.

b. The programme should be based on risk prioritisation, and all high risk relationships for which a deficiency in verification documentation exists should be addressed and completed as a matter of priority.

c. Other relationships which are not yet being reviewed on a risk basis should be reviewed for any deficiency in verification documentation following the occurrence of a “trigger” event.

d. For the purpose of this document the trigger events should be deemed to be those events detailed in 13.3. This should run concurrently with a review of higher risk relationships.

**13.2 Exceptions to the Review**

The following relationships may normally be excluded from the scope of the progressive programme:

a. Small exempted one-off transactions.
b. Acceptable applicants where the acceptable applicant is the customer itself and acting on its own behalf with no underlying principal;
c. All insurance policies where there is no surrender value.

**13.3 Trigger Events**

For the purposes of low risk cases there are two trigger events which will automatically cause a file to require review:

a. A subsequent business transaction on the policy; or
b. A surrender or redemption request.

However, a file can cause suspicion at any time and other events may prompt a review.

**13.4 Subsequent Business Transactions**

a. For the purposes of this section, a subsequent business transaction is a transaction, which was not expected by the insurance company. It should be noted that a “regular” premium payment (whether the same as the previous premium payment or not) is not a subsequent business transaction.

b. If the applicant for a business relationship is an existing policyholder of the insurance company and has had its identity verified within the preceding two years, it is not necessary to re-verify identity for that subsequent business transaction.

c. However, where a subsequent business transaction occurs and the applicant for a business relationship is an existing policy holder but it is more than two years since verification of identity was undertaken and the verification on file is not of the level required by the current Guidelines, or no verification of identity is held on file, or where previously the policy holder was subject to a waiver, but where the existing, plus proposed, investment are now above the waiver level, or where there is reason to believe that the information previously supplied by the policy holder has been superseded, then the identity of the policy holder must be verified.

d. Additionally, whether identification of the policy holder is held or not, where any subsequent business transaction is undertaken which is significantly different from the normal pattern of previous business then the insurance company must consider whether this requires additional information or not and whether this is a suspicious transaction or not.

**13.5 Surrender or Redemption**

In the case of a redemption or surrender of a policy, wholly or partially, an insurance company will not normally be required to verify the identity of the policyholder (even when no, or insufficient, information is held on file) where payment is made:

a. To the name of the policy holder(s) by means of a cheque crossed “account payee”; or

b. To a bank account held (solely or jointly) in the name of the policyholder by any electronic means effective to transfer funds.

**14.0 SOURCE OF FUNDS**

**14.1 The Source of the Applicant for a Business Relationship’s Monies**

a. The insurance company should make enquiries as to how the applicant for a business relationship has acquired the monies to be invested. A risk-based approach will be needed in respect of the extent of the information that may be required and/or validated for this purpose.

b. The insurance company should not normally accept generic descriptions of the source of wealth from the applicant for a business relationship, such as “savings,” “investments,” “inheritance,” or “business dealings”.

**14.2 Remitting the Monies**

a. The insurance company shall establish how the payment is to be made, from where and by whom.

b. Where the monies are being remitted from accounts other than in the name of the applicant for business the insurance company must be satisfied that the reasons for the account remitting the monies not being in the name of the applicant for a business relationship are understood, and where considered necessary, the identity of the holder of the account from which remittance has been made should be verified. In the absence of being so satisfied the application for a business relationship must not proceed any further.

**14.3 Monies Received**

a. The insurance company should be satisfied that the monies received have come from expected account(s).

b. While, ideally, the insurance company should demonstrate its satisfaction by linking the information provided with the monies remitted to the information supplied under 14.2, it is accepted that this may not always be possible. Where the insurance company does not receive complete originator information from the remitting bank the insurance company must review the information provided and consider whether additional information should be sought. A risk-based approach must be used in deciding whether to seek additional information.

**14.4 Multiple Accounts Remitting Monies**

Where the monies are being remitted from several accounts, the insurance company should understand the reasons for this and be satisfied in each case.

**14.5 Additional Remittances**

Where the insurance company receives additional remittances, other than expected premiums for a regular premium contract, it must ensure that the source of monies and account(s) remitting the monies is known in accordance with sections 14.1 and 14.2.

**14.6 Regular Payments**

a. Where a policyholder remits monies on a regular premium contract the Insurance Company must have in place procedures requiring the review of these policies on a regular basis to ensure that the requirements of sections 14.2, 14.3, and 14.4 are being complied with. The frequency of such review should be set to take account of risk factors such as the type of policyholder, (e.g. PEP, the size of premium, frequency of remittance and location of the remitting bank.

b. Should, at any time, the insurance company become aware of a change of remitting account the file should be reviewed to ensure that sufficient information is held to satisfy the requirements of sections 14.2, 14.3, and 14.4. Additionally should the level of premiums contributed on a regular basis change, the insurance company should review the information held to ensure that the requirements of section 14.1 are met.

**14.7 Payment Out of Monies**

Monies remitted by the insurance company should be paid to an account in the name of the policyholder. Where payment is made to an account other than in the name of the policyholder the reasons for this should be understood and recorded and where considered necessary evidence of identity of the account holder should be obtained.

**14.8 Use of Multiple Accounts When Paying Monies Out**

When payment of monies to be remitted by the insurance company is requested to be made to more than one account, whether in the name of the policyholder or otherwise, the reasons for this should be understood and recorded and, where considered necessary, evidence of identity of the account holder(s) should be obtained.

**14.9 Multiple Small Payments When Paying Monies Out**

When the policyholder requests the monies to be remitted by multiple “small” payments, whether to the same account or not, and whether in the name of the Client or otherwise, the insurance company should consider whether additional enquiries are required to ascertain the reasons for this. Where additional enquiries are made the reasons for the multiple payments should be understood and recorded and, where considered necessary, evidence of identity of the policyholder(s) should be obtained.

**15.0 SUSPICIOUS REPORTING**

**15.1 Suspicious Reporting**

a. Where an employee/director of an insurance company reports a knowledge or suspicion of money laundering, there remains a duty to protect “policy holder’s confidentiality”; however, no breach of that duty is committed by a person reporting the information associated with the knowledge or suspicion to the Financial Intelligence Unit (FIU).

b. Money laundering suspicions could be aroused at any time when dealing with a Client’s affairs, from pre-sale negotiations to contract cessation. The time at which suspicion is aroused is irrelevant; indeed, it could occur sometime after the association with a transaction or specific case. The fact that suspicion has been formed means that there is a legal obligation to report to the FIU.

c. Furthermore, this responsibility still applies where an investment for whatever reason is rejected by the insurance company and there are grounds for reporting suspicions of money laundering.

**15.2 What is "Knowledge"**

Knowledge has been defined by **Baden Delvaux** v. **SBOGety General** [1992] to include the following:

a. Actual knowledge;
b. Wilfully shutting one's mind to the obvious;
c. Wilfully and recklessly failing to make such enquiries as a reasonable and honest person would make;
d. Knowledge of circumstances which would indicate facts to an honest and reasonable person; and
e. Knowledge of circumstances, which would put an honest and reasonable person on enquiry.

**15.3 What is "Suspicion?"**

a. Suspicion is personal and subjective and falls far short of proof based on firm evidence.

b. Suspicion has been defined as being beyond mere speculation and must be based on some foundation. A person who considered a transaction to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime.

**15.4 Compliance Officer**

a. A senior officer of the insurance company, must be appointed by the board of the insurance company as compliance officer to oversee relevant policies and procedures; receive reports of suspicions from employees; determine whether the information gives rise to a suspicion; investigate that suspicion; decide whether to report or not; record his action (which may involve further disclosure to the FIU and act as the central co-ordination point.

b. The reporting entity must notify the Bank of the proposed appointment for fit and proper verification and further approval.[7]

**15.5 Suspicious Circumstances**

a. Suspicions may be aroused as a result of one, or a combination, of any number of circumstances which may be associated with a policy holder case or transaction. Money launderers constantly invent new schemes, but the list below gives examples of the traits shown in some of those so far identified:

i. **Evasiveness**
- Concealment of identity of policy holder;
- Concealment of identity of beneficial owner;
- Concealment of ownership of funds;
- Incomplete application details and lack of willingness to provide evidence to answers required.

ii. **Inappropriateness**
- Application beyond lifestyle or means;
- Unexplained changes in investment pattern;
- Investment taken against advice or not appropriate to customer's true needs;
- Sudden changes in intermediary transaction pattern;
- Unexplained receipt of bulk premiums from intermediary accounts

[7] Section 141 of the Insurance Act 2016

iii. **Unexplained or**

- Third party transaction (payments or improper withdrawals) circumstances;
- Cash or “near-cash” payments or withdrawal requests;
- Multiple sources of payment;
- Cross jurisdiction funding for payment;
- Payment of premium from early surrender of another investment in unusual circumstances;
- Payment from obscure or unregulated organisations;
- Unnecessarily complex and/or unusual transactions or intentions, or patterns of transactions;
- Requests for part investment and return of surplus funds;
- Immediate interest in surrender penalties or requests for large withdrawals or policy loans;
- Early surrender of a contract;
- Receipt of unexplained telegraphic transfers, requests to return telegraphic transfers;
- Requests for no correspondence to go to policy holder;
- Complex ownership structures involving layers of companies and/or trusts;
- Suspicious of behaviour by either the policyholder or intermediary.

b. The presence of any one or more of the above circumstances does not in itself mean money laundering is occurring. Each employee or director of an insurance company must judge a case on its own merits.

c. Here any of the above circumstances or other circumstances giving cause for concern, have been identified on an application or file this fact should be recorded.

d. Comprehensive details of any subsequent actions, explanations and decisions taken on the application or file must also be documented and maintained on the file.

e. If, for any reason, at any stage of the life of a policy, the insurance company becomes aware of any doubts as to the identity of a policyholder (or any other party to a policy) this must be reported to the compliance officer using the normal reporting procedure for suspicious transactions. The compliance officer may take whatever steps they consider appropriate to satisfy the insurance company as to the identity of the policy holder (or other party) and if they consider there is a suspicion they should report as detailed in Section 7.2.

f. Departments should be encouraged to share information which may highlight suspicious transactions e.g. underwriters and claims investigators.

**15.6 Complex and Unusual Transactions**

All complex or unusual transactions and complex or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose, must be scrutinised by the insurance company and the background and purpose of such transactions ascertained so that the insurance company is satisfied as to why the transaction is being structured in this way. In the absence of being so satisfied, the insurance company must not proceed with the transaction and report the suspicion in the normal way. Full details of any information obtained, and decisions made, should be recorded on the file.

**15.7 Suspicion Reporting Procedure**

a. Procedures for reporting suspicions by employees or directors to the FIU are as laid out in the FIU's AML Handbook for Reporting Entities 2021.[8]

b. Notwithstanding these procedures, insurance companies and Brokers are also to be guided as follows:

   i. An insurance company shall establish written internal procedures, which enable all directors, managers and employees to know to whom they should report any knowledge or suspicions of money laundering activities.

   ii. Any knowledge or suspicions of money laundering activities should be reported to the compliance officer who shall determine whether the information gives rise to a suspicion, investigate that suspicion; decide whether to report or not; record his action (which may involve further disclosure to the FIU) and act as the central co-ordination point.

   iii. All suspicions must be reported to the FIU promptly.

   iv. Once a suspicion has been reported, it may not be suppressed by the insurance company and broker. Although an employee's line manager may add comments and recommendations to the suspicion report to assist in evaluating the circumstances surrounding the suspicion, the report must be sent to the compliance officer and an appropriate record maintained. A suspicion is not transferable and, as such, cannot be passed on as the report is progressed within the organisation.

   v. Where, in the judgement of the Compliance Officer, it is believed that the suspicion is well founded, the suspicion must be reported to the FIU.

c. Where a transaction has not been proceeded with for any reason, and any member of staff of the insurance company considers that there may be a suspicion of money laundering or other suspicious activity, normal reporting procedures should be followed.

**16.0 TIPPING OFF**

Insurance companies that obtain information, which is suspicious or indicates possible money laundering or terrorism financing (ML/TF) activity shall not disclose such information to unauthorised persons and shall report to the FIU as required.

**17.0 COMBATING THE FINANCING OF TERRORISM**

a. Terrorism is the unlawful threat of action designed to compel the government or an international organization or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause. Financing of terrorism (FT/TF) is the process by which funds are provided to an individual or group to finance terrorist acts.

[8] FIU's AML Handbook for Reporting Entities 2021, pages 31-34

b. The key difference between ML and TF is that with ML, the person seeks to disguise the origins of illicit funds with a profit motive in mind; while in contrast, a person funding terrorism may use legitimately held funds to pursue illegal and ideological motives. An insurance company or broker should bear this in mind when assessing the risks posed by those funding terrorism. An insurance company/broker that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organisations or that the transaction is linked to or is likely to be used in terrorist activity, is committing a criminal offence.

c. TF often involves small sums of money and may be difficult to detect. Notwithstanding, many of the AML controls an insurance company/broker have in place will overlap with measures to counter the financing of terrorism (CFT). These may include for example, risk assessments, customer due diligence procedures, transaction monitoring and reporting of suspicious activity and transactions. The guidance provided in these Guidelines therefore applies equally to CFT as it does to AML, even where this is not explicitly stated.

d. Insurance companies shall, upon receipt from the Bank keep updated, the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism and such other relevant resolutions, which require sanctions against individuals and entities belonging or related to the Taliban and the Al-Qaida organization among others.

e. Insurance companies shall maintain a database of names and particulars of listed persons on the UN Sanctions List and such lists as may be issued by the United Nations Security Council.

f. Insurance companies shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branches or subsidiary.

**18.0 FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION**

*a.* The FATF provides a broad working definition for proliferation financing (PF):

> *"the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."*

b. Proliferation of weapons of mass destruction (WMDs) can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles).

c. PF poses a significant threat to global security and unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen. The FATF Recommendation 7 places obligations on countries to comply with all United Nations Security Council Resolutions to apply targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction. The role of financial institutions is to implement controls to prevent access to financing by individuals and entities who may be involved in or supporting such proliferation. Even though Guyana does not yet have a regulatory framework for proliferation financing, it is recommended that financial institutions' AML/CFT compliance programmes include PF controls, such as screening against the applicable UN lists of designated persons and countries.

## 19.0 RECORD KEEPING

### 19.1 Record Keeping

a. The records prepared and maintained by an insurance company on its policy holder's relationships and transactions should be such that:

   i. Requirements of legislation, including these Guidelines, are fully met;
   ii. Competent third parties will be able to assess the insurance business' observance of money laundering policies and procedures;
   iii. Any transactions effected via the insurance company can be reconstructed;
   iv. The insurance company can satisfy, within a reasonable time, any enquiries or court, and
   v. Orders from the appropriate authorities as to disclosure of information.

b. Any records retained in computer or microfilm format must be capable of being reproduced in a manner acceptable to the BOG and to the Courts and in accordance with the Evidence Act Chapter 5:01.

### 19.2 Administration Records

a. All documentary items relevant to policyholder identity and transaction history must be maintained and be capable of being retrieved efficiently.

b. These requirements extend to all those functional areas of an insurance company, which may be involved at any stage in the life of an insurance contract. Where records are maintained by third parties (including brokers and acceptable applicants), the onus shall be on the insurance company to ensure that any records are stored securely and are capable of being retrieved. Further, the insurance company must ensure that any transactions, which are originated or requested by the policyholders (such as electronic transfers), are accompanied by all details sufficient to identify the immediate source/recipient of the funds.

c. Where file notes and supporting information are created these items must be legible, dated and carry either a name or user identification for the person completing them, so ensuring an audit trail and proper use as evidence in any potential legal proceeding. File notes evidencing decisions must demonstrate that they are produced by an appropriate person with appropriate knowledge of the circumstances and matters surrounding a case.

d. Where relevant, records maintained electronically will only be admissible if it can be demonstrated that the systems maintaining them are accurate and fully efficient. The author of any such record must be identifiable.

### 19.3 Records Verifying Evidence of Identity

Records which evidence the identity of an individual, corporation, trustee, nominee or other entity, as described in these Guidelines, must be maintained for the required period (at least a seven[7] year period).

### 19.4 Transaction Records

a. All items which constitute a transaction in the life of a contract must be recorded and be retrievable for the required period. These records must be able to show exactly what was requested by the policyholder and the subsequent results of processing.

b. For example, records showing the following may be maintained:

i. The origin of the funds;
ii. The form in which they were offered or withdrawn i.e. cheque, cash, telegraphic transfers;
iii. The identity of the person originating the transaction;
iv. The destination of the funds;
v. The form of instruction and authority.

**19.5 Compliance Records**

a. Insurance Companies must maintain written records in two broad categories:-

- Reports of suspicions;
- Maintenance of adequate procedures;
- To demonstrate to BOG that ongoing compliance are being adhered.

**19.6 Money Laundering Report Register and Suspicion Report Records**

a. The suspicion reporting procedure will generate information and/or documents the form of which may vary for each organisation. They must however include a register containing the following for each report made to the FIU:

i. An outline of the circumstances of the suspicion;

ii. Details of the action taken following the processing of the report within the organisation;

iii. Details of the date on which the report is made;

iv. The identity of the person who makes the report;

v. Identification of the law enforcement officer to whom the report is made (if applicable); and

vi. Information sufficient to identify any relevant papers.

c. Relevant reports, disclosures to, acknowledgements and consents by the FIU must also be retained.

d. Records must also be kept of all reports made to the compliance officer, which are not passed on to the FIU. These records should also demonstrate the decision making process and the reasons why a disclosure was not made.

**19.7 Register of Money Laundering Enquiries**

a. An insurance company shall maintain a register of all enquiries made of it by law enforcement or other authorities acting under powers provided by any anti-money laundering requirements.

b. The register maintained above shall be kept separate from other records and shall contain as a minimum the date and nature of the enquiry, the name and agency of the inquiring officer, the powers being exercised, and details of the account(s) and/or transaction(s) involved.

**19.8 Retention Periods**

a. The Required Period for the purposes of these Guidelines is at least seven (7) years from the date when:

i. All activities relating to a one-off transaction or a series of linked transactions were completed; or

ii. The business relationship was formally ended; or

iii. If the business relationship was not formally ended, when the last transaction was carried out.

b. Where a report has been made to the FIU, or the insurance company knows or believes that a matter is under investigation, the insurance company shall retain all relevant records for as long as required by such FIU.

**20.0 STAFF AWARENESS AND TRAINING**

**Training Requirements**

a. The insurance company shall provide, or shall arrange to be provided, education and training for all staff to ensure that they are, as a minimum, aware of:

i. The provisions of the anti-money laundering requirements;

ii. Their personal obligations under the anti-money laundering requirements;

iii. Their personal liability for failure to report information or suspicions in accordance with the anti-money laundering requirements;

iv. The internal procedures for reporting suspicious transactions within the insurance company; and

v. The identity of the money laundering reporting or compliance officer.

b. Additionally, the insurance company shall provide training to assist all staff:

i. In the recognition and handling of transactions carried out by or on behalf of, any person who is, or appears to be, engaged in money laundering;

ii. In dealing with customers where such transactions occur; and

iii. In procedures to be adopted where transactions have been reported to the FIU in accordance with these guidelines, or where the FIU or any law enforcement entity are carrying out or intending to carry out a money laundering investigation.

iv. The insurance company shall provide, or shall arrange to be provided, specific training appropriate to the particular categories of staff, dependent on the jobs performed which in addition to the training set out above includes:

- The legal obligations and the offences associated with money laundering activities;
- The types of suspicious transactions in respect of which diligence should be exercised;
- The policies and procedures in place to prevent money laundering;
- Customer identification, record keeping and other procedures; and
- The recognition and handling of suspicious transactions.

c. Senior staff includes directors, both executive and non-executive.

**20.1 Training Records**

Training records which demonstrate that appropriate training has been provided to all participants, including temporary staff, must be maintained by the insurance company.

**20.2. Screening**

a. Insurance companies/brokers shall develop internal procedures for assessing whether employees taking up key positions meet fit and proper requirements[9] in respect of:

   i. verification of the identity of the person involved; and

   ii. verification whether the information and references provided by the employee are correct and complete.

b. Key positions include senior management with the responsibility for supervising or managing staff, and for auditing the system and employees who deal with:

   i. new business and the acceptance – either directly or via intermediaries – of new policyholders, such as agents
   ii. the collection of premiums; and
   iii. the settlement and payments of claims.

c. Insurance companies and brokers shall maintain records on the identification data of the employees in key positions. The records will demonstrate due diligence performed in relation to the fit and proper requirements.

**20.3 Refresher Training**

a. The Insurance Company shall provide, or shall arrange to be provided, refresher courses at regular intervals, not less than annually for key, “front line”, and other appropriate staff, in order to maintain awareness and to continue diligence of prevention procedures and regulatory requirements.

b. Where there have been significant changes to legislative, regulatory or internal requirements and/or procedures, the insurance company shall provide, or arrange to be provided, suitable training to make all staff aware of their responsibilities.

**21.0 SUBMISSION OF RETURNS**

Insurance companies and brokers shall file with the Bank on a quarterly basis a return on compliance with these guidelines within fifteen (15) days after the end of the quarter in the prescribed format.

[9] Section 11 of IA 2016

**APPENDICES**

**ANNEX A**

**Examples of Risk Factors Relevant for the ML/TF Risk Assessments of Insurance Entities**

**Risk Based Approach**

This Annex provides examples of different categories of risk factors relevant in an insurance context, highlights red flags and outlines mitigating factors which an insurer or broker may wish to take into account when performing risk assessments. This Annex should be read in conjunction Section 6 RBA of this Guidance, as well as the applicable national and sectoral risk assessments.

Where a risk factor is coupled with one or more red flag indicators, insurers and intermediaries may wish to apply a more stringent approach to CDD and monitoring. The following are risk factors which an insurer or broker can consider when performing their risk assessment. The overall risk level of a business relationship is usually the result of a combination of several risk factors. By exception, it could be based on one single risk factor, if deemed significant.

**Product Risk Factors**

Product risk is assessed by identifying how vulnerable a product is to money laundering and terrorist financing based on the product's design. Product risk should be assessed periodically and when significant changes are made to product offerings (including the development of new products/services). Product risk is a significant factor in identifying unusual activity.

The following *table 2* describes attributes used to assess the vulnerability of product offerings and provides lower and higher risk examples.

*Table 2*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| Ability to hold funds or transact large sums | Product design that does not hold a balance or can't be withdrawn against, such as group benefits | Product design that allows funds to be held on behalf of the customer; high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments |
| Customer anonymity or third-party transactions | Product design that only allows transactions from customers with identification, or where all funds flow back to customer | Product design that allows deposits and payments by third parties or that provide for non-face-to-face transactions (for example, mobile apps if payment source unknown) |
| Liquidity | Product design that includes significant fees or other penalties for early withdrawals | Product design that has no (or no significant) fees or other penalties for early withdrawal |

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| Time horizon | Products that are typically held for a long period of time, such as years, until retirement or death | Products that are typically held for a shorter time period |
| Purpose and intended use of products | Product design makes it easy to identify if products are not being used as intended | Product design makes it difficult to identify if products are not being used as intended |

The following product features tend to increase the risk profile of a product:

- Flexibility of payments, for example the product allows payments from unidentified third parties or high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments or cash payments;
- Ease of access to accumulated funds, for example the product allows partial withdrawals or early surrender at any time, with limited charges or fees;
- Negotiability, for example the product can be traded on a secondary market or used as collateral for a loan; and
- Anonymity, for example the product facilitates or allows the anonymity of the customer.

The following product features tend to decrease the risk profile of a product:

- Product only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
- No surrender value;
- No investment element;
- No third party payment facility;
- Total investment is curtailed at a low value;
- Life insurance policy where the premium is low;
- Accessibility only through employers, for example a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
- Product cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option; and
- No cash payments.

**Service and Transaction Risk Factors**

Service and transaction risk can be assessed by identifying how vulnerable a product is to use by a third party or unintended use based on the methods of transaction available. Service and transaction risk is influenced by product design. Understanding potential service and transaction risks in the business is a significant factor in recognizing unusual activity at a customer level.

Service and transaction risk is considered higher when the features or services of a product make it possible for customers to use the product in a way that is not consistent with the purpose of the product. For example, an insurance policy with investment funds may be intended as a long-term investment, but could be vulnerable to frequent transactions because it allows for low fee transactions and there may be no disincentive to withdrawing money at any time.

The following tables describe attributes used to assess service and transaction risk and provide lower and higher risk examples.

*Table 3*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Difficulty to trace ownership of funds** | Pre-printed cheques bill payments, EFT payments with verified banking records | Cash, bank drafts in bearer form, travellers cheques, and counter cheques (where the ownership information is handwritten or typed in a different font than the rest of the cheque).<br>**Potentially**: Some Digital Currencies |
| **Customer is not the payer or recipient of the funds** | The funds are moved from or to another financial institution | The third party paying or receiving funds has not previously been disclosed. |
| **Payment source or recipient is based outside of country** | The recipient or payer is the owner and is in a low risk country | The recipient or payer is the owner and is in a higher risk country.<br><br>The recipient or payer is a third party outside of country (More difficult to trace or confirm source of funds). |
| **Number of transactions** | Low number of transactions or transaction frequency that is typical for the product | Large number of transactions back and forth with the customer or third parties is normal for the product design. |
| **Transactional patterns** | Regular and expected customer account activity | Significant, unexpected and unexplained change in the customer's typical activity, such as early surrenders or withdrawals is a service offered. |

**Distribution/Broker Channel Risk Factors**

The distribution channel is the method a customer uses to open a new policy or account. The distribution channel risk is identified by assessing how vulnerable the channel is to money laundering or terrorist financing activities based on attributes that may make it easier to obscure customer identity.

The risk of failing to correctly identify a customer may be higher for distribution channels that use a broker, or do not require face-to-face contact. Depending on product, distribution channel risk is mitigated using distributors who are also subject to AML/CFT legislation, which requires a compliance programme to be in place, or a pension scheme subscribed through the customer's employer.

The following table describes attributes used to assess the vulnerability of a distribution channel and provides lower and higher risk examples.

*Table 4*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Distributor has AML/CFT obligations** | Distributor is overseen by a regulatory authority and subject to AML/CFT laws equivalent to life insurer or stronger | Distributors not subject to AML/CFT requirements. |
| **Payment to life insurer** | Customer pays Life Insurer directly from Insurer. Their account at a bank or securities dealer | Customer pays a distributor, who then pays the Life Insurer<br><br>Risk: The broker obscures the source of payment. |
| **Direct relationship of customer to Life Insurer** | Contracted agents and banking consultants<br><br>Products distributed by Life Insurer employees | No face-to-face relationship with Life Insurer employee or an agent.<br><br>For example, trusts or insurance sold by telephone or online without adequate safeguards for confirmation of identification. |

- The following distribution/broker risk factors may contribute to higher risk:
  - Non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards to mitigate the risks of identity fraud;
  - The broker is involved in the management of claims;
  - Long chains of intermediaries; and
  - The broker is used in unusual circumstances (e.g., motivated by an unexplained geographical distance).

- The following factors may contribute to lower risk:
  - Distribution is done through certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

**Geographic Risk Factors**

Life insurers should periodically assess geographic risk by identifying how vulnerable the business is to money laundering or terrorist financing activities based on business connections to regions and countries, which are perceived to present a higher risk.

**Risk, Threats and Vulnerabilities associated to the Geographical Implantations of Life Insurers and Intermediaries' part of Insurance /Financial Groups**

There is no universally agreed upon definition or methodology for determining whether a particular country or geographic area (including the country/geographical area within which the insurer or intermediary operates) represents a higher risk for ML/TF. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of risk include:

- Countries/areas identified by credible sources[33] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

- Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation.

- Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

**Customer Risk Factors**

Customer-based risk factors are assessed to evaluate the level of vulnerability to money laundering and terrorist financing threats posed by customers based on their characteristics. Understanding the inherent risks helps us effectively identify appropriate mitigating controls and manage residual risks. Customer risk factors combined with business risk factors, can be used as criteria for risk scoring to identify high-risk policyholders. Policyholder based risk factors include:

- Customer identity
- Third party involvement
- Customer's source of wealth/funds
- Politically exposed customers
- Known criminal or terrorist

The following *table 5* describes customer-based risk attributes used to assess vulnerability to money laundering and terrorist financing.

*Table 5*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Identification** | Customer provides photo identification or can be identified using third party sources | Customer has difficulty producing identification or the authenticity of the identification provided is questionable. |
| **Third party relationships** | No third party involvement | Controlled by a third party, or multiple indicators of third party deposits or payments. Controlled by a Gatekeeper without any interaction with the beneficial owner. |
| **Customer's legal form** | Customer is a living person Customer is a large, publicly traded legal entity with clear ownership and control | Customer is a legal entity with a complex structure difficult to ascertain those who own or control the entity. Policyholder and/or the beneficiary of the contract are companies with nominee shareholders and / or shares in bearer form. |
| **Source of funds and wealth; including occupation or business type** | Customer's business type or occupation is in a lower risk industry | Customer's business or occupation is in a higher risk industry (such as involved in one or more of cash intensive business, international exposure or associated with crime typologies) Customer's business or occupation is associated with a lower income for a high value deposit without a confirmed source of funds/wealth (inheritance/ real estate/ beneficiary of insurance) |
| **Depth and duration of relationship with customer** | Customer has a long history with the life insurer or its agents and additional information is on file (such as credit underwriting, life insurance underwriting, KYC). | Customer is new to life insurer with little or no experience with the customer. |
| **Customer only holds accounts with lower risk products and services** | Customer holds policies or accounts that are registered with the government, e.g., Registered Retirement Savings Plan | Customer only holds non-Registered policies or accounts, e.g., investment or bank account with an affiliate. |

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Attribute** | Lower risk example | Higher risk example |
| **Other factors** | Customer does not have negative news media or media confirms what is known about the customer (such as career confirmation or community engagement) | Customer has ties to or is on a designated sanctions list. Customer has a history of predicate offences or is associated with negative news. |
| **Political exposure** | Customer does not have any ties to politically exposed persons | Customer is considered a politically exposed foreign person. |

**Customer Identity**

Customer identity risk refers to the risk that the life insurer is doing business with a customer who is not who they say they are, or is involved with money laundering or terrorist financing.

To mitigate customer identity risk, the identity of customers may be ascertained by reviewing customer identification and the customer profile is supplemented with underwriting information or any existing relationships with the customer.

The customer profile may include:

- The length of customer relationship with the insurer;
- History of suspicious or unusual transactions;
- Negative news which may affiliate the customer with allegations of criminal behaviour; and
- Notices or requests from law enforcement.

**Third Party Involvement**

Third party involvement in an insurance product may increase the money laundering and terrorist financing risk, as unknown parties may have an interest in, or control of the policy or account.

When an unusual transaction or series of transactions involving a third-party source or recipient of funds is identified, additional information similar to customer due diligence may help mitigate risk. Enhanced due diligence steps can include requesting the relationship to the customer, the involvement with the policy or account, and the source of wealth. Some products do not allow or restrict deposits or payments by third parties.

**Third Party Red Flags**

- Gatekeepers such as accountants, lawyers, or other professionals holding accounts/policies/contracts at an insurer, acting on behalf of their customers, and where the insurer places unreasonable reliance on the gatekeeper;

- Customers who assign or otherwise transfer the benefit of a product to an apparently unrelated third party; and

- Customer changes the beneficiary clause and nominates an apparently unrelated third party.

- Payments are regularly received from third parties that are no apparent relationship with the policyholder.

**Customer's Source of Wealth**

To mitigate the risk of not understanding the customer's source of wealth, life insurers risk based approach programmes may monitor higher value transactions, and responds to red flags by reviewing for consistency with the policyholder's source of wealth in combination with the policyholder:

- Policies and accounts with the insurer; and
- Business type, occupation and industry, geographic residency and political exposure.

**Geographic Risk**

A customer's geographic location or connections may indicate higher risk for money laundering or terrorist financing activities. To mitigate risk, controls are recommended based on domestic and international geographic risk factors.

**Domestic Geographic Risk Factors**

Where data is available, the assessment of higher domestic geographic risk based on data from internal insurer historical case experiences or government data based on crimes applicable to money laundering and other predicate offenses by region can be used as a risk factor or within monitoring programme.

*Table 6*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Higher crime regions** | Customer does not reside in a region with higher frequency and severity of crimes with money laundering risk. | Customer resides in a region with high frequency and severity of crimes with money laundering risk. |
| **History of high risk activity or fraud** | Customer does not reside in a region that experiences a higher incidence of high-risk activity or fraud. | Customer resides in a region that experiences a higher incidence of high-risk activity or fraud. |

**International Geographic Risk Factors**

Customer risk is higher among customers with connections outside country, especially connections to higher risk countries.[10]

*Table 7*

| ATTRIBUTE | LOWER RISK EXAMPLE | HIGHER RISK EXAMPLE |
|---|---|---|
| **Foreign tax or physical residency of customer** | Countries risk ranked as low by the Life Insurer. | Countries risk ranked as high by the Life Insurer. |
| **Foreign ties or transactions** | Customer does not have any indicators of foreign residency or transactions outside of country. | Customer has requested or performed transactions with ties to high-risk countries. |

[10] See Annex A, Examples of Risk Factors Relevant for the ML/FT Risk Assessments of Insurance Entities, page 68

**Geographic Risk Red Flags**

- Geographic risk: 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).
- Has the policyholder provided certification of their domestic tax residency that is supported by other information that the insurer or broker knows about the customer?
- What is the tax residency of the customer.
- Are all communications sent internationally without foreign residency ties.
- Does the source of wealth, source of funds or other known relationship include ties to higher risk countries?
- Death claim payments to a beneficiary residing in a high-risk country due to terrorism.
- Premiums and/or settlements are paid through accounts held with financial institutions established in jurisdictions associated with higher ML/TF risk; and
- Broker is based in, or associated with, jurisdictions associated with higher ML/TF.

**ANNEX B**

**Life Insurance Distribution Channels and Brokers**

Insurance is sold through a variety of distribution channels. In instances, life insurance policies are sold through brokers. The life insurer will have limited or no direct contact with the policyholder. Life insurance policies may also be sold online, where there may not be any face-to-face interaction with the customer by the insurer or broker. When identifying and evaluating the ML/TF risk associated with the method through which the product is sold, the life insurer should consider the risks related to the broker used and the nature of their relationship with the life insurer and the customer.

**Risk Assessment**

The ML/TF risk assessment forms the basis of a life insurer's and broker's RBA. The key purpose of such an assessment is to understand and mitigate inherent ML/FT risks, and enable the life insurer/broker to effectively manage residual risks.

**Examples of Inherent Risk factors in a Life Insurance Context**

This table should be read together with *table 1* concerning the risk factors linked to life insurance products.

*Table 8 – Examples of Inherent Risk factors in a life insurance context*

| RISK FACTOR | EXAMPLES RISK FACTOR | EXAMPLE DESCRIPTION |
|---|---|---|
| **Customers and related third parties (policyholder and if any, its beneficial owner, the beneficiary and if any, its beneficial owner)** | Customer base growth | Rapid growth and/or turn-over of customer base in terms of amount and customer diversity pose higher ML/TF risks. Therefore, an insurer should pay extra attention to a new campaign aimed at increasing the customer base significantly, to a subscription of a high net worth life policy by a new customer compared to a well-known customer with already other business relationships with the insurer for long time. |

| | | |
|---|---|---|
| | Individuals who are more difficult to identify | Difficulty in identifying the person on whose behalf the business relationship or transaction is being conducted, generally with involvement of third-parties (e.g., policy holder different from the insured person and beneficiary and with no apparent relationships with them, or third-party payer on the contract with no apparent relationship with the policy holder). |
| | Structures that make it difficult to identify the beneficial owner of the policyholder or of the beneficiary | Complex ownership and control structures involving multiple layers of shares registered in the name of legal entities and/ or non-transparent structures (e.g., trusts and other legal arrangements designated as beneficiaries of life policies, enabling a separation of legal ownership and beneficial ownership of assets). |
| | Unusual circumstances associated with the customer's business relationships or transactions | Customer activity not consistent with the customer's known profile and lacks business rationale or economic justification causing economic losses (e.g., an early surrender for a large amount without understandable rationale or transactional activity causing economic losses). |
| | PEPs exposure[11] | Business relationships involving a person(s) (i.e., policyholder, beneficiary, beneficial owner of the policyholder or of the beneficiary) defined as a Politically Exposed Person including his/her family members or close associates, as covered under R. 12. (e.g., a PEP designated as a beneficiary by an unrelated policyholder could hide a corrupt activity – additional caution should be exercised to identify these situations, as the PEP may not be identified until the end of the policy, at payout). |
| | Payment methods | Payment methods which may contribute to increased ML/TF risks (e.g., cash or other forms of payment vehicles fostering anonymity; payments from different bank accounts without explanation; payments received from unrelated third parties, (see table 4, page 66 and page 69 third party involvement.) |
| | Origin or source of funds and wealth | Unclear or suspicious source of wealth and/or source of funds that are involved in the business relationship. (e.g., large investment in a unit-linked product by a low-income person without a clear source of wealth). |

[11] See FATF Guidelines on Politically Exposed Persons (Recommendations 12 and 23)

| | | |
|---|---|---|
| | Higher risk individuals | Customers which are classified as higher risk including persons previously reported by the insurer/broker to the FIUs or who operate in a higher risk industry or profession from an AML/CFT perspective This includes persons active in charities and non-profit organization, precious metals and stone dealers, money services businesses, cash intensive businesses such as "cash for gold" or casinos, arms dealers. |
| **Products and Services** | Products associated with high risk payment | Product that may inherently favour international customers, cash, third parties and complex payments or have features that allow for pay-outs not limited to pre-defined events (e.g., international life insurance products designed for expatriates). |
| | Product which accumulate large funds, transact large sums, or allow high amount withdrawals | Product that are designed for the accumulation of large funds and/or allow a large transaction (e.g., insurance wrapper products). |
| | Products which favour anonymity or are easily transferable | Products or services that may inherently favour anonymity, or products that can readily cross international borders, or are easily transferred, (e.g., life insurance policy issued to the bearer or negotiated on secondary market). |
| | Products which allow early surrender | Products which allow for early surrender and have a surrender value. |
| | Products with low value policy benefits and simple product features | Products have simple features and are low in value may carry lower ML/TF risks |
| **Distribution channels** | Non face to face sales channels | Channels which do not provide for a physical meeting between the customer and an employee or broker, and is not supported by other mitigation measures like identification performed by an obliged or authorized person such as a public notary (e.g., life insurance policy sold on-line) or without adequate safeguards for confirmation of identification or to mitigate the risks of identity fraud (see Annex A, table 2 page 62 and table 4 page 66.) |

| | | |
|---|---|---|
| | Reliance and outsourcing | Reliance on intermediaries and /or outsourcing to third parties which are not subjected to the same AML/CFT obligations as the life insurer or is not well known to the life insurer (e.g., life insurance policy sold by small independent intermediaries or by third parties which may have less sophisticated controls in place). |
| | Management of the customers payments | Intermediaries, which manage the investments and the flow of funds on behalf of the customer on their accounts (e.g., life insurance policy sold by intermediaries accepting cash payments and/or payments on their own accounts). |
| **Geography** | Products and services | Products and services that are marketed or sold in higher ML/TF risk countries. |
| | Customers | Customers, beneficiaries, policy holder and/or related third parties are based in or linked to higher ML/TF risk countries; or reside in countries considered to be uncooperative in providing beneficial ownership information. |
| | Intermediaries | Intermediaries that are based in or sell to higher ML/TF risk jurisdictions (e.g., intermediaries owned and/or controlled by persons established in higher ML/TF risks jurisdictions.) (See page 67) |

In performing a risk assessment, life insurers that distribute their products and services through intermediaries should consider the following:

- Size and status of the broker – Broker operations range from local sole proprietors to large international organisations. Smaller brokers may have less sophisticated AML/CFT framework and may benefit from more direction from the insurer.

- Role of the broker in handling customer's funds - When identifying the risk associated with a broker, the insurer should also take into account whether the broker handles funds directly from the customer – including in relation to handling payouts of the contract, whether the broker plays a purely facilitating/introducing role. It should be noted that insurance intermediation may also facilitated by digital (e.g. online internet portals and mobile phone applications, etc.) or other means (e.g., telemarketing, calls centres, etc.)

The risk assessment should be commensurate with the nature, size and complexity of the business. For smaller or less complex life insurers or intermediaries (for example, where customers fall into similar categories and/or where the range of life insurance products offered are very limited), similar risk assessment might suffice. It should take into account all risk factors, which the life insurer and intermediaries consider to be relevant, including product, geography, distribution and customer risk factors.

Life insurance may be employed for legitimate tax planning purposes. Life insurers and intermediaries should nevertheless consider tax-related aspects as part of their risk assessment, since certain characteristics of life insurance products may make them attractive to individuals seeking to hide income, commit tax fraud and evade tax or tax reporting requirements.

Life insurers and brokers should define a clear methodology for development and their risk assessment, especially in the case of complex organisations such as large, cross-sectoral multinational groups or national multi-business groups.

In the case of life insurers or brokers that are part of a group, risk assessments should take into account group wide risk appetite and framework, where relevant. Depending on the circumstances and local jurisdictional requirements, the parent company should perform a consolidated risk assessment for the entire group, taking into account the geographic situations of each relevant life insurance entity and if any, the legal obstacles preventing foreign entities from applying AML/CFT group-wide procedures, including exchange of information with the group. This will ensure that there is adequate oversight and consistent mitigating measures across all relevant entities of the group. Where applicable, they can consider synergies integration and consistency with other risk assessments performed by other internal functions, such as compliance and operational risk management.

Where appropriate, life insurers and brokers may cooperate for example, at an industry or country level to produce guidance and inform the production of their risk assessments.

ML/TF risk assessments should be periodically reviewed and refreshed in line with the requirements of the Bank, or guidelines or typologies from national competent authorities, including the FIUs, or international bodies. Risk assessments should be reviewed promptly in response to internal factors, such as launch of new product, acquisition or significant change of characteristics of customers due to a merger; and external factors such as regulatory changes, change in the national or supranational risk assessment, or new/emerging AML/CFT typologies.

**ANNEX C**

**Examples of money laundering and suspicious transactions involving insurance**

This document contains examples of money laundering and suspicious transactions involving insurance. It was originally created as an appendix to the IAIS *Guidance paper on anti-money laundering and combating the financing of terrorism* (October 2004) and is updated periodically to include additional examples identified.

**Indicators**

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

- application for a policy from a potential client in a distant place where a comparable policy could be provided “closer to home”

- application for business outside the policyholder’s normal pattern of business

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

- any want of information or delay in the provision of information to enable verification to be completed
- an atypical incidence of pre-payment of insurance premiums
- the client accepts very unfavourable conditions unrelated to his or her health or age
- the transaction involves use and payment of a performance bond resulting in a cross-border payment ( wire transfers) = the first ( or single) premium is paid from a bank account outside the country
- large fund flows through non-resident accounts with brokerage firms
- insurance policies with premiums that exceed the client's apparent means
- the client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment
- insurance policies with values that appear to be inconsistent with the client's insurance needs
- the client conducts a transaction that results in a conspicuous increase of investment contributions
- any transaction involving an undisclosed party
- early termination of a product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party
- a transfer of the benefit of a product to an apparently unrelated third party
- a change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy)
- substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder
- requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments
- attempts to use a third party cheque to make a proposed purchase of a policy
- the applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract
- the applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments
- the applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency

- the 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

- the applicant for insurance business appears to have policies with several institutions
- the applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means

- the applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party

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

- the applicant for insurance business use a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

The above indicators are not exhaustive.

**Life insurance**

- A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of USD 1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some USD 1.2 million and represented the last step in the laundering operation.[12]

- An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

- On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank *accounts* and then transferred to an *account* in another jurisdiction. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas *accounts*. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

[12] FATF Report on Money Laundering Typologies, 2002 - 2003

- In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over

  USD 1.5 million was initially placed with a bank in England. The “layering process” involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent’s supervisor was also charged with violating the money laundering statute.

  This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

- Customs officials in Country X initiated an investigation which identified a narcotics trafficking organisation utilised the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

  Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean. To date, this investigation has identified that over USD 29 million was laundered through this scheme, of which over USD 9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.[13]

- A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual‘s fraudulent management activity.

- A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of USD 1 million in case of death. The other was a mixed insurance with value of over half this amount.

- A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around USD 7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.

[13] FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 - 2004

**Non-life insurance**

- A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.[14]

- Four broking agencies were forced to freeze funds after US court action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, codenamed Golden Jet, was coordinated by the Drug Enforcement Agency (DEA) based in the USA but also involved the FBI and the UK authorities. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft.

- It is understood that the brokers affected by the court order included some of the largest UK insurance brokers. The case highlighted the potential vulnerability of the insurance market to sophisticated and large scale drug trafficking and money laundering operators. The court order froze aircraft insurance premiums taken out by 17 Colombian and Panamanian air cargo companies and by 9 individuals. The action named 50 aircraft, including 13 Boeing 727s, 1 Boeing 707, 1 French Caravelle and 2 Hercules C130 transport aircraft. The British end of the action was just one small part of a massive antidrug trafficking action co-ordinated by the DEA. Officials of the DEA believe Golden Jet is one of the biggest blows they have been able to strike against the narcotics trade. The American authorities led by the DEA swooped on an alleged Colombian drugs baron and tons of cocaine valued at many billions of dollars were seized and a massive cocaine processing factory located in Colombia together with aircraft valued at more than USD22 million were destroyed in the DEA coordinated action. According to the indictment, the cargo companies were responsible for shipping tons of cocaine from South to North America all through the 1980s and early 1990s, providing a link between the producers and the consumers of the drugs. Much of the cocaine flowing into the USA was transported into the country by air. During this period the Colombian cartels rose to wealth and prominence, aided by those transport links.

**Intermediaries**

- A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding the raising suspicions with the insurance company.[15]

[14] FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004
[15] FATF Report on Money Laundering Typologies, 202 - 2003

- Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.[16]

- An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

- A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around USD 400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

**Reinsurance**

- An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer, which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate, the insurer probably intended to assure continuation of the reinsurance arrangement.

- A state insurer in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the company was linked to potential war lords and drug traffickers. A report was made to the law enforcement authorities.

[16] FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 - 2004

**Return premiums**

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time
- return premium being credited to an account different from the original account
- requests for return premiums in currencies different to the original premium, and
- regular purchase and cancellation of policies.

**Over payment of premiums**

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums, has, been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say USD10,000 or equivalent)
- the request to refund the excess premium was to a third party
- the assured is in a jurisdiction associated with money laundering and
- where the size or regularity of overpayments is suspicious.

**High brokerage/third party payments/strange premium routes**

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

**Claims**

A claim is one of the principal methods of laundering money through insurance. Outlined below are examples of where claims have resulted in reports of suspected money laundering and terrorist financing.

- A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the client's creditors discovering funds that had allegedly been smuggled overseas. Documents indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering.

- A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest "dirt money" for a profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organised by the purchasers to ensure a claim occurred and that they received "clean" money as a claims settlement.

- Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

- During an on-site visit, an insurance supervisor was referred to a professional indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurer's papers, which identified one of the bank's clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.

- After a successful High Court action for fraud, adjusters and lawyers working for an insurer involved in the litigation became aware that the guilty fraudster was linked to other potential crimes, including money laundering.

**Assignment of claims**

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

**Non-life insurance – fraudulent claims**

- Police in Country A uncovered a case of stolen car trafficking where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A. Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over USD 2.5 million.

  The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of damages.

  On receipt of the damages, the false claimants gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over USD 12,500 per month from the leader's accounts to the country in question. The money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its gains into real estate.[17]

[17] FATF Report on Money Laundering and Terrorist Financing Typologies, 2003 – 2004

- An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of $2 million from similar fraud schemes carried out by terrorist groups.

**(No. 1438)**