

ROYAL MONETARY AUTHORITY OF BHUTAN

༄༅། །། ཀྲིལ་གཞུང་དངུལ་ལས་དབང་འཛིན། །།



**FIU G3: Anti-Money Laundering and Combating the Financing of
Terrorism Guideline for Insurance Companies
2014**

1. INTRODUCTION

- 1.1) This guideline is issued pursuant to Section 141(g) and Section 210 of the Financial Service Act (FSA) 2011. This guideline must be read in conjunction with the additional requirements under the FSA, 2011.
- 1.2). This guideline may be cited as the “**Anti Money Laundering and Combating the Financing of Terrorism guideline for Insurance Companies, 2014**”.
- 1.3). In addition the insurance companies are also to comply with the relevant sections of the FSA 2011 and the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Regulations 2015.

2. MONEY LAUNDERING AND FINANCING OF TERRORISM

- 2.1). Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully ‘laundered’ the criminal is able to enjoy these monies without revealing their original source.
- 2.2). Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can be funded from legitimate income.
- 2.3). Insurers offer a variety of products aimed at transferring the financial risk of a certain event from the insured to the insurer. These products include life insurance contracts, annuity contracts, non-life insurance contracts, and health insurance contracts. These products are offered to the public through trained agents of the insurance companies. This guideline is therefore of importance to the agents and corporate agents also, to the extent indicated in the guideline.
- 2.4). The obligation to establish an anti-money laundering program applies to an insurance company, and not to its agents, and other intermediaries. Hence the responsibility for guarding against insurance products being used to launder unlawfully derived funds or to finance terrorist acts, lies on the insurance company, which develops and bears the risks of its products.
- 2.5). Financial institutions such as insurers are therefore placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through the institution. Law protects such disclosures, enabling the person with information to be able to disclose the same without any fear. Insurance institutions likewise need not fear breaching their duty of confidentiality owed to customers.

3. VULNERABILITIES IN INSURANCE

- 3.1). Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (cash or bank transfer) and contract law. Insurers should take these factors into account when assessing this vulnerability. This means they should prepare a risk profile of the type of business in general and of each business relationship.
- 3.2). When a life insurance policy matures or is surrendered, funds become available to the policyholder or other beneficiaries. The beneficiary to the contract may be changed possibly against payment, before maturity or surrender, in order that payments are made by the insurer 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.
- 3.3). Examples of the type of life insurance contracts that are vulnerable as a vehicle for laundering money or terrorist financing are products, such as:
- single premium life insurance policies that store cash value
 - fixed and variable annuities
- 3.4). Non-life insurance money laundering or terrorist financing can be seen through inflated or totally bogus claims, e.g. by arson or other means causing a bogus claim to be made to recover part of the invested illegitimate funds. Other examples include cancellation of policies for the return of premium by an insurer's cheque, and the overpayment of premiums with a request for a refund of the amount overpaid. Money laundering can also occur through under-insurance, where a criminal can say that he received compensation for the full amount of the damage, when in fact he did not. Examples of how terrorism could be facilitated through property and casualty coverage include use of worker's compensation payments to support terrorists awaiting assignment and primary coverage and trade credit for the transport of terrorist materials.
- 3.5). Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious reinsurance companies or reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions. Examples include:
- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds,
 - the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding,
 - the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.
- 3.6). Insurance intermediaries independent or otherwise are important for distribution, underwriting and claims settlement. They are often the direct link to the policyholder and therefore intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The same principles that apply to insurers should generally apply to insurance intermediaries. In addition to the responsibility

of intermediaries, customer due diligence ultimately remains the responsibility of the insurer involved.

4. AML/CFT PROGRAM

In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism, every insurer needs to have an AML/CFT program as cited in section 7.1 of AML/CFT Regulation 2015 which at a minimum should cover:

- Customer Due Diligence (CDD), the detection of unusual or suspicious transactions and the reporting obligation, and the communication of these policies, procedures and controls to the employees,
- appropriate compliance management arrangements,
- record keeping arrangements,
- an ongoing employee training programme, and
- an adequately resourced and independent audit function to test compliance (e.g. through sample testing) with these policies, procedures, and controls

4.1. Provision of Copies to RMA

A reporting entity must provide to the RMA a copy of its AML/CFT Program within 3 months of the commencement of this guideline and within one month of any review of the program conducted in accordance with sub-section 4.2.

4.2 Review of Programs

A reporting entity must conduct a review of its AML/CFT Program within two years of the lodgment of its AML/CFT Program and every two years thereafter.

4.3 Compliance Reports

A reporting entity shall provide to the RMA every six months a report on the actions taken by it to give effect to its AML/CFT Program.

5. KNOW YOUR CUSTOMER (KYC):

- 5.1). Considering the potential threat of usage of the financial services by a money launderer, insurance company should make reasonable efforts to determine the true identity of all customers requesting for its services as cited in section **4 of AML/CFT Regulation 2015**. Hence effective procedures should be put in place to obtain requisite details for proper identification of the customers.
- 5.2). Prior to providing a financial service to a customer a reporting entity shall sight the identification documentation as per section **4.3 of the AML/CFT Regulations 2015**, and record the specified information in relation to that customer and retain a copy of the documents as required under section **16.1 of AML/CFT Regulations 2015**.
- 5.3). The insurer must conduct on-going due diligence on the business relation with the customer to ensure that the transaction are consistence with the firm's knowledge of customer's business risk and source of income as per section **4.11 of the AML/CFT Regulations 2015**.

- 5.4) Insurance premium paid by persons other than the person insured should be looked into to establish insurable interest.
- 5.5) The insurer should not enter into a contract with a customer whose identity matches with any person with known criminal background or with banned entities and those reported to have links with terrorists or terrorist organizations (Annex I).
- 5.6) Besides verification of identity of the customer at the time of initial issuance of contract, KYC should also be carried out at the claim payout stage and at times when additional top up remittances are inconsistent with the customers known profile.

6. IDENTIFICATION OF BENEFICIAL OWNERS AND LEGAL PERSONS

For the purposes of this guidance paper the expression '**beneficial owner**' applies to the owner/controller of the policyholder as well as to the beneficiary to the contract

- i). Where the customer is a company, the insurer shall, apart from identifying the customer, also identify the directors of the company.
- ii). Where the customer is a partnership or a limited liability partnership, the insurer shall, apart from identifying the customer, also identify the partners.
- iii). Where the customer is any other body corporate or unincorporated, the insurer shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporated.

7). RISK PROFILE OF THE CUSTOMER

- 7.1). In the context of very large base of insurance customers and the significant differences in the extent of risk posed by them, the companies are advised to classify the customer into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence required.
 - i). For the purpose of risk categorization, individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Where there are low risks, it may be appropriate for an insurer to apply simplified verification procedures. These procedures, of course, must still be sufficient for the institution to achieve the goal of verification- establishing a reasonable belief that it knows the true identity of its customer. In addition refer section **3 and 14 of AML/CFT Regulation 2015**.
 - ii). For the high risk profiles, like for customers who are non-residents, high net worth individuals, trusts, charities, NGO's and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC and underwriting procedures should ensure higher verification and counter checks.

7.2). **Enhanced due diligence** is called for with respect to higher risk categories. Decisions taken on establishing relationships with higher risk customers should be taken by senior management. For detail refer section **4.10 of AML/CFT Regulation 2015**.

8. VERIFICATION AT THE TIME OF REDEMPTION/SURRENDER

8.1). In life insurance business, no payments should be allowed to third parties except in cases like superannuation/gratuity accumulations and payments to legal heirs in case of death benefits. All payments, should be made after due verification of the bona fide beneficiary, through account payee cheques.

8.2). AML/CFT checks become more important in case the policy has been assigned by the policyholder to a third party not related to him.

9. NEW OR DEVELOPING TECHNOLOGIES

9.1). An insurer shall put in place policies and procedures to address any specific risks associated with the use of new technologies.

9.2). An insurer shall implement the policies and procedures referred to in section 9.1 when establishing customer relationships and when conducting ongoing due diligence. In addition refer section **10 of AML/CFT Regulation 2015**.

10. RELIANCE ON INTERMEDIARIES AND THIRD PARTIES

10.1). An insurer may rely on an intermediary or third party to perform CDD measures in accordance with the **section 12 of AML/CFT Regulation 2015**.

10.2). This guideline sets the responsibility of a robust AML/CFT program on the insurers. Nonetheless, it is necessary that the following steps be taken to strengthen the level of control on the agents engaged by the insurers:

- i) A list of rules and regulations covering performance of agents must be put in place. A clause should be added making KYC norms mandatory and specific process document can be included as part of the contracts.
- ii) Insurance Company when faced with a non-compliant agent should take necessary action to secure compliance, including when appropriate, terminating its business relationship with such an agent.
- iii). Services of defaulting agents who expose the insurers to money laundering and terrorist financing related risks on multiple occasions should be terminated and the details reported to FIU for further action.

11. ONGOING MONITORING AND PAYING ATTENTION TO UNUSUAL/SUSPICIOUS TRANSACTIONS

11.1). An insurer shall monitor on an ongoing basis, its business relations with customers.

- 11.2). An insurer shall, during the course of business relations, observe the conduct of the customer's policy and scrutinize transactions undertaken to ensure that the transactions are consistent with the insurer's knowledge of the customer, its business and risk profile and where appropriate, the source of funds. In this respect "**transactions**" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.
- 11.3). As per section **4.3.1 (e)(i) of AML/CFT Regulation 2015**, an insurer shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.
- 11.4). As per section **4.3.1 (e)(ii) of AML/CFT Regulation 2015**, an insurer shall take reasonable steps to inquire into the background and purpose of the transactions in section 11.3 and document such information and its findings.

12. REPORTING OBLIGATION OF THE FIRM

The FSA 2011, Section 141 (a), provides for reporting entities to report both STRs and CTRs to the FIU. This guideline establishes the specific reporting obligations.

12.1) Reporting cash transaction report to the FIU

With a view to ensuring that premiums are paid out of clearly identifiable sources of funds, it has been decided that remittances of premium by cash should not exceed Nu. 50,000/-. It would be advisable for the companies to evolve even lower thresholds for cash transactions. It is further advised that:

- i). Premium/proposal deposits beyond Nu. 50,000 should be remitted only through cheques, demand drafts, credit card or any other banking channels.
- ii). For totally related transactions, premium amount greater than Nu. 50,000 in a calendar month should be examined more closely for possible angles of money laundering. This limit will apply at an aggregate level considering all the roles of a single person-as a proposer or life assured or assignee.
- iii). Insurance companies have to report the total connected cash transactions above Nu. 50,000 per month to FIU within 10th day of next succeeding month in the required format (see Annex II)

12.2) Reporting of Suspicious Transactions to the FIU

- i). Every insurer shall report to the Financial Intelligence Unit any transaction or attempted transaction which the insurer has reasonable grounds to suspect, that funds are the proceeds of an unlawful activity or are related to terrorist financing should be reported to FIU in terms of section **6.1 of the AML/CFT Regulations 2015**.

- ii) Insurance companies shall lodge with the FIU a Suspicious Transaction Report (STR) in the required format as specified in Annex III. Where an obligation to lodge a STR arises the report shall be delivered to the FIU no later than 2 working days on being satisfied that the transaction is suspicious.
- iii). Suspicious transactions might fall into one or more of the following examples of categories (for details refer **FIU G-2: Suspicious Transaction Guidelines for Reporting Entities, 2014**)
- any unusual financial activity of the customer in the context of his own usual activities,
 - any unusual transaction in the course of some usual financial activity
 - any unusual or disadvantageous early redemption of an insurance policy,
 - any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g. payment of claims or high commission to an unusual intermediary,
 - any unusual method of payment,
- iv). Insurers should ensure that:
- there is a clear procedure for staff to report suspicions of money laundering and the financing of terrorism without delay to the compliance officer,
 - there is a clear procedure for reporting suspicions of money laundering and the financing of terrorism without delay to the FIU, and
 - all staff to know whom their suspicions should be reported.

13. DELIVERY OF REPORTS TO FIU

Reports required to be delivered to the FIU under these guidelines may be delivered by post, by hand or electronically. The time limits apply irrespective of the delivery method used by the reporting entity. The reporting entity is responsible for ensuring that the reports are delivered to the FIU within the time required by this guideline. In urgent cases the reporting entity should notify the FIU of the details of the transaction by telephone and send the report by post, hand or electronically in accordance with this guideline. In addition refer **section 6.1.5-6.1.13 of AML/CFT Regulation 2015** for details.

14. PROVISION OF ADDITIONAL INFORMATION

If a reporting entity has communicated information to the FIU, the FIU may, by written notice given to the reporting entity, require the reporting entity to give such further information as is specified in the notice, within the period and in the manner specified, to the extent to which the reporting entity has that information; or to produce, such documents as specified in the notice; and relevant to the matter to which the communication relates.

15. INTERNAL CONTROL/AUDIT

Internal audit departments of Insurance companies should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. It is of importance that the audit function is independent and, if applicable, that the auditor has direct access and reports directly to management and the board of directors. The reports should specifically comment on the robustness of the internal policies and processes

in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects.

16. RECORD KEEPING

For Record keeping requirement insurer should refer section 16 of AML/CFT Regulation 2015.

17. APPOINTMENT OF AML/CFT COMPLIANCE OFFICER

The Insurers should designate an AML/CFT Compliance Officer under **FIU G1: Guidelines for appointment of AML/CFT Compliance Officer (AMLCO)**. The name of the AML/CFT compliance officer should be communicated to FIU immediately. The compliance officer should be well versed in the different types of products and transactions which the institution handles and which may give rise to opportunities for money laundering and the financing of terrorism.

18. CONFIDENTIALITY AND PROTECTION OF INFORMATION

For Confidentiality and Tipping off provisions insurer should refer section 22 of AML/CFT Regulation 2015.

19. TRAINING OF STAFF

19.1). Insurers staff and agents should receive initial and ongoing training on relevant AML/CFT legislation, regulations, guidance and the insurers own AML/CFT policies and procedures. Although each insurer should decide for itself how to meet the need to train members of its staff in accordance with its particular legal, regulatory and commercial requirements, the programme will at a minimum include:

- a description of the nature and processes of laundering and terrorist financing, including new developments and current money laundering and terrorist financing techniques, methods and trends,
- a general explanation of the underlying legal obligations contained in the relevant laws, and
- a general explanation of the insurers' AML/CFT policy and systems, including particular emphasis on client acceptance policies, record keeping, verification and the recognition of suspicious customers/transactions and the need to report suspicions to the compliance officer.

19.2). The concept of AML/CFT should be part of in-house training curriculum for agents and employees. Records of training imparted to staffs and agents should also be maintained.

20. PENALTY

Non compliance to any provision of this guideline shall be liable to a fine as per **section 23 of AML/CFT Regulation 2015**.