

Master Circular

Anti-Money Laundering/Counter- Financing of Terrorism (AML/CFT)
(Updated upto 31st July 2010)



Insurance Regulatory and Development Authority
Parishram Bhavan, 3rd Floor,
Basheerbagh,
Hyderabad - 500 004
Phone No: +91-40-23381300
Fax No: +91-40-66823334

INDEX

Particulars	Page No.
1. Background:	1
2. What is Money Laundering?	1
3. AML/CFT Program	2
I. Internal policies, procedures, and controls:	2
3.1 Know Your Customer (KYC) Norms	2
3.1.1 What are KYC Norms?	2
3.1.2 When should KYC be done?	3
i. Knowing New Customers	3
ii. Knowing Existing Customers	4
iii. KYC on Ongoing Basis	4
3.1.3 KYC and Risk Profile of the Customer	4
3.1.4 Products to be covered:	5
3.1.5 Sources of Funds:	6
3.1.6 Verification at the time of redemption/ surrender	6
3.2 Reporting Obligations:	6
i. Suspicious Transactions Reports:	7
ii. Monitoring and Reporting of Cash Transactions	7
iii. Reporting of receipts by Non-Profit Organisations	7
iv. Reporting of Counterfeit Currency/Forged Bank notes (CCR):	7
3.3 Implementation of Section 51A of UAPA	8
3.4 Record Keeping	10
II. Compliance Arrangements:	11
1. Responsibility on behalf of the agents and corporate agents	11
2. Appointment of Principal Compliance Officer	11
III. Recruitment and Training of employees/agents:	11
IV. Internal Control/Audit:	12
Annexure I	13
Annexure II	15
Annexure III	16
Annexure IV	17
Annexure V	18

**Master Circular on
Anti Money Laundering/Counter- Financing of Terrorism (AML/CFT) –Guidelines for
Insurers**

1. Background:

- 1.1 The Prevention of Money Laundering Act (PMLA), 2002 brought into force with effect from 1st July 2005, is applicable to all the financial institutions which include insurance institutions. The application of anti-money laundering measures to non-depository financial institutions generally, and to the insurance companies in particular, has also been emphasized by international regulatory agencies as a key element in combating money laundering. Establishment of anti money laundering programs by financial institutions is one of the central recommendations of the Financial Action Task Force and also forms part of the Insurance Core Principles of the International Association of Insurance Supervisors (IAIS). Accordingly, the Authority has decided to put in place the following regulatory guidelines/instructions to the Insurers, Agents and Corporate agents as part of a Programme on Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) for the insurance sector.
- 1.2 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 and also through a number of alternate distribution channels like direct marketing, bancassurance etc. The guidelines are therefore of importance to the agents and corporate agents also, to the extent indicated in the guidelines.
- 1.3 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. What is Money Laundering?

- 2.1 Money Laundering is moving illegally acquired cash through financial systems so that it appears to be legally acquired.
- 2.2 There are three common stages of money laundering as detailed below which are resorted to by the launderers and insurance institutions which may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions: -
 - Placement - the physical disposal of cash proceeds derived from illegal activity;
 - Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and
 - Integration - creating the impression of apparent legitimacy to criminally derived wealth.
- 2.3 If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. 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. Such disclosures are protected by law, 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. 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 which should, at a minimum, include:

- I. Internal policies, procedures, and controls;
- II. Appointment of a Principal compliance officer;
- III. Recruitment and training of employees/agents;
- IV. Internal Control/Audit;

The above key elements of the AML/CFT programme are discussed in detail below:

I. Internal policies, procedures, and controls:

Each insurance company has to establish and implement policies, procedures, and internal controls which would also integrate its agents in its AML/CFT program, as detailed below:

3.1 Know Your Customer (KYC) Norms

3.1.1 What are KYC Norms?

- i. 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 especially the person who funds/pays for an insurance contract, either as beneficial owner or otherwise. For the purposes of these norms, the term customers also refer to the proposer/policyholder; beneficiaries and assignee. Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a client.
- ii. Effective procedures should be put in place to obtain requisite details for proper identification of new customers. Special care has to be exercised to ensure that the contracts are not anonymous or under fictitious names.
- iii. Measures have to be taken to identify the beneficial owner and take all reasonable measures to verify his/her identity to their satisfaction so as to establish who the beneficial owner is.
(‘Beneficial owner’ for this purpose means ‘the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.)
- iv. A list of documents to be verified at the time of accepting the risk for compliance with KYC requirement for individuals and others is given in Annexure I (which may be treated as illustrative only). No further documentation is necessary for proof of residence where the document of identity submitted also gives the proof of residence. It is mandatory to obtain any one of the documents to clearly establish the customer identity consistent with risk profile in respect of all new insurance contracts (Please also see 3.1.3 below). Any other document that is accepted by the Insurer should be such that it would satisfy regulatory/enforcement authorities, if need be at a future date that due diligence was in fact observed by the insurer in compliance with the guidelines and the PML Act. Documents collected towards the identity and

- address of the customer should be duly certified by an authorized person as identified by the insurer
- v. Customer information should be collected from all relevant sources, including from agents.
 - vi. Insurance premium paid by persons other than the person insured should be looked into to establish insurable interest.
 - vii. The degree of due diligence to establish KYC could be decided by the insurers where premium is below ₹ 1 lakh per annum. However, premium of ₹ 1 lakh per annum in case of individual business should be considered as a threshold for exercising detailed due diligence, what ever be the payment mode
 - viii. Considering the hardship in complying with the KYC requirement by small value policy holders and possible implications for spread of insurance into rural and low income sectors, especially micro-insurance, the Authority has decided to provide exemption upto a total annual premium of ₹ 10,000/- on life insurance policies held by a single individual from the requirement of recent photograph and proof of residence.
 - ix. At any point in time during the contract period, where an insurance company is no longer satisfied that it knows the true identity of the customer, an STR should be filed with FIU-IND.
 - x. Remittance of premium is an important stage of entering into contract, hence, cash transactions need more diligence and care (Please also see para 3.2 (ii))
 - xi. 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.
 - xii. A list of individuals and entities subject to UN sanction measures under UNSC Resolutions (hereinafter referred to as 'designated individuals/entities') would be circulated to the life and general insurance companies through the respective Councils, on receipt of the same from the Ministry of External Affairs (MEA). This is in addition to the list of banned entities that were circulated to the insurers till date.
 - xiii. Insurers are advised to maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/ entities are holding any insurance policies with the company. An updated list of individual and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed in the United Nations website at <http://www.un.org/sc/committees/1267/consolist.shtml>
 - xiv. Insurers are required to conduct detailed due diligence while taking insurance risk exposure to individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime. Special attention should be paid to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings maintained for assisting competent authorities. Agents/ Corporate agents will have to be appropriately alerted to ensure compliance with this stipulation. While using the FATF Public Statements being circulated through the insurance councils, insurers should go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations.

3.1.2 When should KYC be done?

i. Knowing New Customers:

- a. In case of new contracts, KYC should be done before the issue of every new insurance contract.

This requirement should be complied with in all life insurance contracts as specified. However, taking into account the fact that internationally a number

of countries have exempted general insurance sector from AML/CFT Regulations and in view of the vulnerability of general insurance products more at the claims stage, rather than at entry stage, it is decided that AML/CFT guidelines pertaining to KYC should be applied by general insurance companies at the settlement stage where claim payout/premium refund crosses a threshold of ₹ One lakh per claim/premium refund. However, general insurance companies are strictly advised to comply with para 3.1.1 (xi) and 3.1.5 of the guidelines so as to avoid unwitting involvement in insuring assets bought out of illegal funds and entering into transactions with banned entities/individuals. Besides, In view of the modification made in the guidelines at entry stage for general insurance companies, it is decided to make the guidelines applicable to all general insurance policies coming into force on or after January 1, 2007.

- b. In case of non face to face business which includes Tele calling, Internet Marketing, Logging in of business or payment of premiums/lump sums at branches, collection of documentation be completed for premiums exceeding ₹ One lakh per person per annum within 15 days of issue of policy.

ii. **Knowing Existing Customers:**

It has been decided that the process of AML/CFT should be applied for the policies coming into force on or after 01.04.2004. Since Insurers, invariably collect considerable background of the policyholder as also the beneficiary before entering into contracts no major constraints are expected in this exercise, in respect of the existing contracts. KYC in case of existing customers should therefore be carried out based on the limits fixed for new policies on all contracts/relevant transactions in case of the existing policies. Nevertheless, taking the volume of work and practical hardship to Insurance Companies on account of retrospective application of AML/CFT guidelines to the existing customers from 1.4.2004, the Authority has relaxed the cut-off date by making it effective from 1.1.2006. The AML/CFT requirements will also not be applied to the existing customers paying premiums less than ₹ One lakh per annum.

iii. **KYC on On-going basis:**

Besides verification of identity of the customer at the time of initial issuance of contract which includes obtaining a recent photograph, 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. Any change which is inconsistent with the normal and expected activity of the customer should attract the attention of the insurer for further ongoing KYC processes and action as considered necessary.

3.1.3 KYC and Risk Profile of the Customer

- i. In the context of the 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.
 - a. For the purpose of risk categorization, individuals (other than High Net Worth) 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. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of

the society, government departments and government owned companies, regulators and statutory bodies etc., In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Notwithstanding above, in case of continuing policies, if the situation warrants, as for example if the customer profile is inconsistent with his investment through top-ups, a re-look on customer profile is to be carried out.

- b. 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. In this connection insurers are also advised to carry out the appropriate level of due diligence keeping the observations at 3.1.5 in view.
- ii. Insurers should devise procedure to ensure that proposals for contracts with high risk customers are concluded after approval of senior management officials. It is however, emphasized that proposals of Politically Exposed Persons (PEPs) in particular requires approval of senior management, not below Head (underwriting) /Chief Risk Officer level.
 - iii. Conducting detailed due diligence should not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than normal KYC. These measures should be commensurate to the risk. While it is not intended to be exhaustive, the following are some of the reasonable measures in carrying out detailed due diligence:
 - More frequent reviews of the customers activities/profile/transactions
 - Application of additional measures like gathering information from publicly available sources or otherwise
 - Review of the proposal/contract by a senior official of the insurance company etc.,

Measures so laid down should be in such a way that it would satisfy competent authorities (regulatory/enforcement authorities), if need be at a future date, that due diligence was in fact observed by the insurer in compliance with the guidelines and the PML Act, based on the assessed risk involved in a transaction/contract.

- iv. Notwithstanding any contrary provisions above, detailed due diligence measures should be applied in the event where there are suspicions of money laundering or terrorist financing, or where there are factors to indicate a higher risk.

3.1.4 Products to be covered:

The AML/CFT requirements focus on the vulnerability of the products offered by the insurers to any of the process of money laundering. Some vulnerable products are illustrated in **Annexure II**. Based on the vulnerability criterion and after examining the product and business coverage it has been decided that the following categories of products/business lines may be exempted from the purview of AML/CFT requirements:

- i. Standalone medical/health insurance products.

- ii. Reinsurance and retrocession contracts where the treaties are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with customers.
- iii. Group insurance businesses which are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate its investment.
- iv. Term life insurance contracts, in view of the absence of cash surrender value and stricter underwriting norms for term policies (especially those with large face amounts)

3.1.5 Sources of Funds:

- i. It is imperative to ensure that the insurance being purchased is reasonable. Accordingly, customer's source of funds, his estimated net worth etc., should be documented properly and the advisor and/or employee shall obtain income proofs as in Annexure III, to establish his need for insurance cover. Proposal form may also have questionnaires/declarations on sources of fund, and details of bank accounts. Large single premiums should be backed by documentation, to establish source of funds.
- ii. It is emphasized that mere documentation of income proofs, however, does not constitute establishing 'source of funds'. Insurers should take appropriate measures commensurate with the assessed risk of customer and product profile as part of their due diligence measures which may include:
 - conducting independent enquiries on the details collected on /provided by the customer where required,
 - consulting a credible database public or other, etc.,
- iii. Relevant records and details must be maintained in such a way that it enables verification at a later date and support the fact of having established sources of funds involved in the insurance contract.

3.1.6 Verification at the time of redemption/surrender:

- i. In life insurance business, no payments should be allowed to 3rd 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, electronic payment methods such as ECS, NEFT Systems approved by the Reserve Bank of India.
- ii. Free look cancellations needs particular attention of insurer especially in client/agents indulging in free look surrender on more than one occasion.
- iii. AML/CFT checks become more important in case the policy has been assigned by the policyholder to a third party not related to him (except where the assignment is to Banks/FIs/Capital Market intermediaries regulated by IRDA/RBI/SEBI). Notwithstanding the above, insurers are required to ensure that no vulnerable cases go undetected. Especially where there is suspicion of money laundering or terrorist financing, or where there are factors to indicate a higher risk, AML/CFT checks will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

3.2 Reporting Obligations:

The AML/CFT program envisages submission of Reports on certain transactions to a Financial Intelligence Unit-India (FIU-IND) set up by the Government of India to track possible money laundering attempts and for further investigation and action.

i. Suspicious Transactions Reports:

- a. Suspicious activity monitoring program should be appropriate to the company and the products it sells. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents /office records /memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Compliance Officer (refer para 3 (II) (iii)) for recording his findings. These records are required to be preserved for ten years as indicated in clause 3.4. It is extremely difficult to give an exhaustive list of suspicious transactions. An illustrative list of such transactions is however, provided in **Annexure IV**.
- b. Insurance companies should report the suspicious transactions immediately on identification. Such reports should include attempted transactions, whether or not made in cash, irrespective of the monetary value involved. When such transactions are identified post facto the contract, a statement may be submitted to FIU-IND within 7 working days of identification in the prescribed formats.
- c. Directors, officers and employees (permanent and temporary) shall be prohibited from disclosing the fact that a Suspicious Transactions Report or related information of a policyholder/prospect is being reported or provided to the FIU-IND.

ii. Monitoring and Reporting of Cash Transactions:

- a. 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 ₹ 50,000/-. It would be advisable for the companies to evolve even lower thresholds for cash transactions. It is further advised that:
 1. Premium/proposal deposits beyond ₹ 50,000 should be remitted only through cheques, demand drafts, credit card or any other banking channels.
 2. For integrally related transactions, premium amount greater than ₹ 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.
 3. Insurance companies have to report integrally connected cash transactions above ₹ 10 lakh per month to FIU-IND by 15th of next succeeding month
- b. The above clauses should not be selectively interpreted on individual transaction basis. Splitting of the insurance policies/issue of number of policies to one or more entities facilitating individuals to defeat the spirit of the AML/CFT guidelines should be avoided. Where there is possibility of transactions being integrated through a single remitter, the insurer should refuse to accede to the requests for cash deposits.

iii. Reporting of receipts by Non-Profit Organisations :

All transactions, involving receipts by non-profit organizations (either in the form of assignments and/or in the form of top-up remittances) of value more than ₹ ten lakh, or its equivalent in foreign currency, should be reported to FIU-IND by 15th day of next succeeding month.

iv. Reporting of Counterfeit Currency/Forged Bank notes (CCR):

All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document

has taken place facilitating the transactions should be reported within 7 days of identification to FIU-IND

3.3 Implementation of Section 51A of UAPA:

- i. By virtue of Section 51A of UAPA, the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. To implement the said section an order reference F. No. 17015/10/2002-IS-VI dated 27th August, 2009 has been issued by the Government of India (Copy annexed). The salient aspects of the order with particular reference to insurance sector are detailed in the following paras.
- ii. Shri Kunnel Prem, Consultant & Special Officer-Life, Insurance Regulatory and Development Authority, 3rd Floor, Parishram Bhavan, Bashir Bagh, Hyderabad-500 004. E-mail- premkunnel@irda.gov.in Telefax +91 40 66820961 is the UAPA Nodal Officer for the purposes of implementation of the said order in the insurance sector
- iii. A consolidated list of all the UAPA Nodal Officers of various agencies governed by the order will be circulated every year and on every change in the list, on receipt of the same from Ministry of Home Affairs.
- iv. **Procedure for freezing of insurance policies of 'designated individuals/entities'**

In case any matching records are identified, the procedure required to be adopted is as follows:

- a. Insurance companies shall immediately and in any case within 24 hours from the time of identifying a match, inform full particulars of the insurance policies held by such a customer on their books to the Joint Secretary (IS-I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.
- b. The insurance companies shall also send a copy of the communication mentioned in 3.3(iv) (a) above to the UAPA Nodal Officer of the State/UT where the account is held, IRDA and FIU-IND.
- c. In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, insurance companies would prevent designated individuals/entities from conducting any transactions, under intimation to the Joint Secretary (IS-I), Ministry of Home Affairs at Fax no. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.
- d. The insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND in respect of the insurance policies covered by paragraph 3.3(iv) (a) above, carried through or attempted, in the prescribed format (as per the Master Circular on Anti Money Laundering Guidelines dated 24th November 2008) .
- e. On receipt of the particulars of suspected designated individual/entities IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the insurance companies are the ones listed as designated individuals/entities and the insurance policies, reported by insurance companies are held by the designated individuals/entities.

- f. In case, the results of the verification indicate that the insurance policies are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these insurance policies under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned office of insurance company under intimation to IRDA and FIU-IND.
 - g. The said order shall take place without prior notice to the designated individuals/entities.
- v. **Procedure for unfreezing of insurance policies of individuals/entities inadvertently affected by the freezing mechanism, upon verification that the individual/ entity is not a designated individual/entity**
 - a. Any individual or entity, if they have evidence to prove that the insurance policies, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned insurance companies.
 - b. The insurance companies shall inform and forward a copy of the application together with full details of the insurance policies inadvertently frozen as given by any individual or entity, to the Nodal Officer of IS-I Division of MHA within two working days.
 - c. The Joint Secretary (IS-I), MHA, the Nodal Officer for IS-I Division of MHA shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the insurance policies owned/held by such applicant, under intimation to the concerned insurance company. However, if it is not possible for any reason to pass an Order unfreezing the assets within 15 working days, the Nodal Officer of IS-I Division shall inform the applicant.
- vi. **Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001**
 - a. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets, derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.
 - b. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA Nodal Officer for IS-I Division for freezing of funds or other assets.
 - c. The UAPA Nodal Officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officer in IRDA. The proposed designee, as mentioned above would be treated as designated individuals/entities.

- d. Upon receipt of the requests by these Nodal Officers from the UAPA Nodal Officer of IS-I Division, the list would be forwarded to insurance companies and the procedure as enumerated at paragraphs 3.3 (iv) on freezing of insurance policies shall be followed.
- e. The freezing orders shall take place without prior notice to the designated persons involved.
- vii. IRDA would communicate all Orders under section 51A of UAPA relating to insurance policies, to all the insurance companies after receipt of the same from IS-I Division of MHA.

3.4 Record Keeping

- i. The insurer/agents/corporate agents are required to maintain the records of types of transactions mentioned under Rule 3 of PMLA Rules 2005 as well as those relating to the verification of identity of clients for a period of 10 years. The records referred to in the said Rule 3 shall be maintained for a period of ten years from the date of transaction. Records pertaining to all other transactions, (for which insurance companies are obliged to maintain records under other applicable Legislations/Regulations/Rules) insurance companies are directed to retain records as provided in the said Legislation/Regulations/Rules but not less than a period of ten years from the date of end of the business relationship with the customer.
- ii. Sharing of information on customers may be permitted between different organisations such as banks, insurance companies, Income tax authorities, local government authorities on request. Records can also be in electronic form.
- iii. Insurance institutions should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. In the case of long term insurance, full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity.
- iv. Companies should retain the records of those contracts, which have been settled by claim (maturity or death), surrender or cancellation, for a period of at least 10 years after that settlement.
- v. In situation where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed where practicable, insurance institutions are requested to seek and retain relevant identification documents for all such transactions and to report the offer of suspicious funds.
- vi. In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained for at least 10 years after the business relationship is ended.

II. Compliance Arrangements:

A detailed AML/CFT Policy should be drawn up encompassing aspects of Customer acceptance policy, Customer Identification procedure, Monitoring of transactions, Risk management framework as evolved by the insurer. The policy should have the approval of the board and duly filed with IRDA for information. The policy should be reviewed annually and changes effected based on experience.

i. Responsibility on behalf of the agents and corporate agents:

The guidelines place the responsibility of a robust AML/CFT program on the insurers. Nonetheless, it is necessary that the following steps are taken to strengthen the level of control on the agents and corporate agents engaged by the insurers:

- a. A list of rules and regulations covering performance of agents and corporate 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.
- b. Services of defaulting agents who expose the insurers to AML/CFT related risks on multiple occasions should be terminated and the details reported to IRDA for further action.
- c. Insurance company when faced with a non-compliant agent or corporate agent should take necessary action to secure compliance, including when appropriate, terminating its business relationship with such an agent/corporate agent.

ii. Appointment of Principal Compliance Officer:

a. Appointment:

The companies should designate a Principal Compliance Officer (PCO) under AML/CFT rules, at senior level and preferably not below the Head (Audit/Compliance)/Chief Risk Officer.

The name of the principal compliance officer should be communicated to IRDA and FIU immediately.

b. Rights and Responsibilities:

- i. The Principal Compliance Officer should ensure that the Board approved AML/CFT program is being implemented effectively, including monitoring compliance by the company's insurance agents with their obligations under the program;
- ii. He /She should ensure that employees and agents of the insurance company have appropriate resources and are well trained to address questions regarding the application of the program in light of specific facts.
- iii. He /She should be able to act independently and report to senior management.
- iv. He /She and staff assisting him in execution of AML/CFT guidelines should have timely access to customer identification data, other KYC information and records.

III. Recruitment and Training of employees/agents:


- i. As most part of the insurance business is through agents/corporate agents which brings in non face to face business relationships with the policyholders, the selection process of agents/corporate agents should be monitored carefully. The committee monitoring the agents should monitor sales practices followed by agents and ensure that if any unfair practice is being reported then action is taken after due investigation; Periodic risk

- management reviews should be conducted to ensure company's strict adherence to laid down process and strong ethical and control environment.
- ii. Insurance companies should have adequate screening procedures when hiring employees.
 - iii. Instruction Manuals on the procedures for selling insurance products, customer identification, record-keeping, acceptance and processing of insurance proposals, issue of insurance policies should be set out.
 - iv. The concept of AML/CFT should be part of in-house training curriculum for agents.
 - v. The following training requirements are considered essential based on the class of employees.
 - a. New employees: A general appreciation of the background to money laundering, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.
 - b. Sales/Advisory staff: Members of staff who are dealing directly with the public (whether as members of staff or agents) are the first point of contact with potential money launderers and their efforts are therefore vital to the strategy in the fight against money laundering. It is vital that "front-line" staff is made aware of the insurance institution's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases.
 - c. Processing staff: Those members of staff who receive completed proposals and cheques for payment of the single premium contribution must receive appropriate training in the processing and verification procedures.
 - d. Administration/Operations supervisors and managers: A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff.
 - e. Ongoing training: It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff does not forget their responsibilities. This might be best achieved by a twelve or six-monthly review of training. Timing and content of training packages for various sectors of staff will need to be adapted by individual insurance institutions for their own needs.
 - f. Records of training imparted to staff in the various categories detailed above should be maintained.

IV. Internal Control/Audit:

Insurance companies' internal audit/inspection departments should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. 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. Exception reporting under AML/CFT policy should be done to Audit Committee of the Board.

The above guidelines on establishment of an AML/CFT regime are effective from 1st August 2006.


R.K. Nair
Member (F&I)
P

	managers, officers or employees to transact business on its behalf iv. Copy of PAN allotment letter
Insurance Contracts with partnership firms <ul style="list-style-type: none"> • Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners 	i. Registration certificate, if registered ii. Partnership deed iii. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf iv. Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses
Insurance Contracts with trusts & foundations Names of trustees, settlers beneficiaries and signatories Names and addresses of the founder, the managers/directors and the beneficiaries Telephone/fax numbers	i. Certificate of registration, if registered ii. Power of Attorney granted to transact business on its behalf iii. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses iv. Resolution of the managing body of the foundation/association

Annexure II

Vulnerable Products:

1. Unit linked products which provide for withdrawals and unlimited top up premiums;
2. Single premium products-where the money is invested in lump sum and surrendered at the earliest opportunity;
3. Free look cancellations-especially the big ticket cases;

Note: The list is only illustrative and not exhaustive

Annexure III

Income Proofs

Standard Income proofs:

Income tax assessment orders/Income Tax Returns
Employer's Certificate
Audited Company accounts
Audited firm accounts and Partnership Deed

Non-standard Income Proofs:

Chartered Accountant's Certificate
Agricultural Income Certificate
Agricultural-land details & Income assessments
Bank Cash-flows statements, Pass-book

Note: The list is only illustrative and not exhaustive

Annexure IV

Illustrative list of Suspicious Transactions:

1. Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information
2. Cash based suspicious transactions for payment of premium and top ups over and above ₹ 5 lakhs per person per month. It should also consider multiple DDs each denominated for less than ₹ 50,000/-
3. Frequent free look surrenders by customers;
4. Assignments to unrelated parties without valid consideration;
5. Request for a purchase of policy in amount considered beyond his apparent need;
6. Policy from a place where he does not reside or is employed;
7. Unusual terminating of policies and refunds;
8. Frequent request for change in addresses
9. Borrowing the maximum amount against a policy soon after buying it
10. Inflated or totally fraudulent claims e.g. by arson or other means causing a fraudulent claim to be made to recover part of the invested illegitimate funds
11. Overpayment of premiums with a request for a refund of the amount overpaid.

Note: The list is only illustrative and not exhaustive. For more examples on Suspicious Transactions please visit <http://www.iaisweb.org>

ANNEXURE V**List of Circulars**

S. No.	Circular Ref	Date	Contents
1	022/IRDA/Master AML/Nov-08	24/11/2008	Master Circular on AML guidelines 2008
2	39/IRDA/AML/CIR/FEB-09	26/02/2009	Cash Acceptance Threshold for Premium/Proposal Deposit Remittances
3	018/AML-CIR/IRDA/E- Payments/Jul-09	9/07/2009	E-payments by life insurers
4	30/IRDA/AML/CIR/AUG-09	24/08/2009	Review of AML guidelines vis-à-vis Recommendations of FATF
5	IRDA/F&I/CIR/AML/33/09/ 2009	09/09/2009	Amendment to PMLA, 2009
6	IRDA/F&I/CIR/AML/052/10 /2009	28/10/2009	Guidelines on Implementation of Section 51A of Unlawful Activities (Prevention) Amendment Act (UAPA), 2008
7	IRDA/F&I/CIR/AML/85/12/ 2009	23/12/2009	UAPA Nodal Officer of IRDA
8	IRDA/F&I/CIR/AML/16/02/ 2010	03/02/2010	Amendment to PML Rules 2009
9	IRDA/F&I/CIR/AML/80/05/ 2010	13/05/2010	Amendment to Rule 3 of PMLA Rules 2005
10	IRDA/F&A/CIR/AML/99/06/ 2010	16/06/2010	Review of AML guidelines