ANTI-MONEY LAUNDERING AND COMBATING TERRORIST FINANCING POLICY

Policy owner: Sadiq Al -Ali, AML & Compliance Manager, on behalf of the Audit Committee

Last revision: February 2015

A. Introduction

AXA Cooperative Insurance Company (ACIC) is providing General and Life Insurance in Saudi Arabia. Operating in the financial services sectors, ACIC is conscious of the risks arising out of money-laundering and terrorist financing. These criminal activities threaten society, as well as the Company, its customers, shareholders and staff.

ACIC is committed to fighting these threats by harnessing the strengths of the entire Group. In this fight ACIC intends to be among the companies of reference. ACIC exercises the utmost vigilance wherever its products and services are involved, whether they are distributed by ACIC owned distribution channels or external distribution channels. This vigilance extends to third party products and services when ACIC is acting as the distributor.

B. What is Anti Money Laundering and Terrorism Financing

What is money laundering and terrorism financing?

Money Laundering: Any actual or attempted act aimed at concealing or camouflaging the nature of illegally or illegitimately earned property to make it look as proceeds from legal sources.

The term "laundering" is used because criminals need to turn their "dirty" criminal money into clean funds that they can use without arousing suspicion. Getting the criminal money into the financial system means that it becomes harder to trace and confiscate. Drug traffickers, armed robbers, terrorists, illegal arms dealers, fraudsters, and tax evaders all need to launder the proceeds of their crimes.

Money laundering process consists of three steps:

a) Placement: Introduce funds gained from illegal sources into financial systems, including insurance sector (insurance contracts).
b) Layering: Hide and separate illegal funds from their sources through a number of complex measures.
c) Integration: Reinvest illegal funds in the legal economy to take the form of legal funds.

Insurance sector is exposed to transactions that might aim at money laundering and terrorist financing.

Terrorism financing: Financing terrorist operations, terrorists, and terrorist organizations. Terrorists can receive incomes from multiple sources, taking the form of formal and informal financing. Financing forms can be categorized as follows:

Financial support
This financing takes the form of charity grants, local society assistance, and other fund-raising initiatives that might come from entities or individuals.
Criminal activity
This financing usually results from criminal activities such as money laundering, fraud, and other financial crimes

Legal source
This type of financing can result from standing legal actions to finance fully or partially those illegal activities.

Legal Environment
Do not hesitate to refer to the link below to learn more about the AML/CTF regulations in Saudi Arabia
http://www.sama.gov.sa/sites/SAMAEN/MoneyLaundry/Pages/RulesandRegulations.aspx

C. ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING

1. Responsibilities

i. **Board of Directors:**
- To supervise the conception and adoption of the anti-money laundering and counter terrorist finance program.
- To ensure necessary internal capabilities and expertise to determine, measure, limit, and control money laundering and terrorist finance risks in the most appropriate way in the insurance sector.
- Promote internal and external anti money laundering and counterterrorist finance measures and standards.
- Reviewing annual review performed by Internal Audit and Compliance Department.

ii. **Senior Management**
- Monitoring day to day compliance with money laundering obligations within all segments of the Company.
- Setting appropriate control measures to guarantee continuous monitoring.
- Ensuring that the Compliance and Internal Audit is provided with prompt advice of unusual/suspicious transactions and other matters of significance.

iii. **Internal Audit**

- To review the effectiveness of the anti-money laundering and counterterrorist finance program
- Evaluate the compliance of applied measures and recommend the update of standards to comply with the development of antimony laundering and counterterrorist finance ways and techniques.

  This review must be annually performed; its results must be submitted to the Board.

iv. Compliance

- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Ensuring that staff is aware of their obligations and the Company's procedures, and that staff representing the Company to all external agencies in Saudi Arabia (SAMA, CMA etc.) and in any other third party enquiries in relation to money laundering prevention or compliance.
- Ensuring that all segments of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Preparing compliance reports to the Board and Senior Management, when required.
- Ensuring that all branch managers complete the "**Annual Acknowledgement Form for the Prevention of Money Laundering"** (See Annexure III.
- Undertaking the internal review of all suspicions transactions and determining whether or not such suspicions have substance and require disclosure to SAMA ~~of FATF~~.
- Obtaining and making use of national and international findings concerning Countries with serious deficiencies.

v. All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Complying fully with all anti money laundering procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Reporting all suspicions of money laundering to the Compliance & AML Manager.
- Promptly completing, every year, **"Annual Acknowledgement Form for the Prevention of Money Laundering"** (see Annexure III for Specimen) confirming that they had no suspicions during the prior year or that any suspicions have been reported and acknowledging that they have re-read this Policy.
- Employees who violate any of the anti-money laundering regulations or the policies and procedures outlined in this Policy will be subject to **disciplinary action**.
- Receiving follow report reports relevant to any suspicious activities relative to money laundering and terrorist finance notified by the company's employees, its agent and brokers.
- Collaborate and follow-up replies relevant to activities which were detected as suspicious money laundering and terrorist finance activities including, cooperation with Saudi FIU.

- Keep record for all reports on suspicious transactions submitted by employees or brokers, including details on investigations' results and rectifying measures which were taken (if available).

vi. There are personal obligations on every member of management and staff that:

- Any complex, huge, or unnatural activity, any suspicious transaction in terms of its objectives, any activity that is or might be related to financing a criminal activity, terrorism, terrorists or terrorist organizations to money laundering and terrorist finance should be reported to Compliance Manager.

2. CUSTOMER DUE DILIGENCE PROCESS

a) Customer Due Diligence(CDD)

CDD exercise must be conducted by completing "Know Your Customer" (KYC) From [See annexure I]. The underwriter must take all necessary measures enabling him of receiving of integral and real data about any customer and his insurance objectives.

Products and services must not be provided to persons having anonymous or illusionary names or persons with whom it is restricted to deal (see Annexure VI for AXA Group Restricted List). CDD should be conducted in the following manner:

Step 1: Categorize client into "High Risk" or "Low Risk"

Step 2: Inquiring about the identity of the customer (or actual beneficiary), and obtain following information:

i) Natural Personalities

Saudi citizens:

- National Identity card of family records
- The address, the residence and the working place of the person

Foreign Individual

- Residency or five year residency card
- Passport for GCC citizen, or diplomatic card for diplomats
- The address, the residence and the working place of the person

ii) Legal Personalities

For all clients, sufficient information about the nature of the business and its ownership and control structure must be obtained so that it is possible to identify the individual (s) that ultimately own(s) or control (s) the client:

Companies

- A copy of Commercial register issued by the competent authority.
- A copy of the Articles of association, or the memorandum of association and their annexes, and any amendments
- A copy of the identification card of the manager in charge.
- A copy of the issued resolution forming the Board of Directors.
- A copy of the Board resolution evidencing the approval of the opening of the account and conferring Authorization on the signatories.
- A List of the persons authorized who are qualified to deal with the accounts, pursuant to what is provided for in the commercial register, and a copy of the identification card of each.

- A List of all company's owners whose names are included in the memorandum of association and a copy of identification card of each.
- If the company has activities that require license from another government authority, a copy of that license is required.

Non-profit Organizations & Entities

- A copy of the license issued by the relevant government authority.
- A copy of the Board resolution evidencing the approval of the opening of the account.
- A copy of the articles of association.
- Authorization from the board of directors for the persons whom would open & deal with & operate the accounts and a copy of the identification card of each.
- A copy of the Authority's approval of accepting the client & open account for.

Government entities

- A copy of all required documents in accordance with its Law and organization regulatory.
- A copy of the authority approval.

If a client is a type of legal person other than one of the types set out above in the policy, Saudi Arabian Monetary Agency approval is required before issuance of the policy. If there are reasons to doubt about the credibility of information provided by the customer, all the possible means should be use to inquire about the relevance of the pieces of information, as calling the phone numbers of the house or work, etc. Special care should be exercised while conducting no face to face business.

3. Customer Risk level assessment

Customers are categorized into the following categories:

a. High risk customers
b. Political Customers
c. Non-profitable organizations

a. High Risk Customers

Following customers are considered high risk:

- Any complex legal arrangements having no clear regulatory or economic purpose or;
- Any person (natural or legal) from or in any country that does not or partially apply FATF's recommendations. Please refer to the link below FATF's non-compliant countries:

  http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

Following measure should be taken before accepting business from a high risk customer:

- Receive a written statement from the real beneficiaries about managers' identities and main contributors, and the relation with them.
- Receive comprehensive data about the customer, such as additional information on the reasons and purpose of the working relation, information about his activities, functional record, and expected activity.
- Recruit employees at their service and apply customer due diligence procedures, and control them permanently in order to guarantee the disclosure of any suspicious or unusual activity at the right time.
- Hold direct interviews with customer's higher management in a regular manner throughout the relation with him.
- Have the approbation of the company at the beginning of the working relation.

In case a customer was categorized as "high risks" customer, but the ACIC sees that it is necessary to keep the relation, the customer due diligence procedures should the lifted and the customer should be under permanent control and level of risks should be reviewed on a quarterly basis. Any business with customer falling in this category must be approved by Chief Executive Officer (CEO).

If the customer was categorized as "high risks" and later categorized as lower risk, such action should only be taken after the approval of CEO.

b. Political Customers / Politically Exposed Person (PEP)

Concerning the dealings with PEPs, maximum possible efforts regarding customer due diligence procedures must be taken, not limited to:

- CEO approval should be taken before launching a working relation with PEP.
- Measure should be taken to determine the source of revenue as well as the source of funds.

- Working relations should be controlled in a continuous manner.
- Additional documents should be requested for identification process.
- Documents relating to PEPs should be rectified through competent authorities.

c. Non-profitable organizations (NPO)

When tackling any operation for such organizations, the following requirements should be taken into consideration:

- NPO should have official license from a specialized governmental body defining its purposes and activities.
- Such bodies and organizations should be categorized as high risks customers, and obligatory care measures shall be taken when dealing with them.

4. What type of transactions to be reported?

- If the transactions is considered by employees as bad or illegal.
- Any transaction which does not comply with customer's data, objective.
- Any transaction through politically exposed person (PEP).
- Transactions which lack economic substance.
- The beneficiary changes
- There is a big increase in sum insured or insurance premium
- Paper and / or huge insurance payments are used
- Third party settles payment
- Anonymous payments are settled through specialized bank instruments
- The address of the insured or the beneficiary is changed
- Unjustified lump sum for life insurance pension plans are settled
- A policy contract is used as guarantee
- A policy contract is annulled at an early stage or when its period is changed
- The type of utility is changed
- There is no sufficient information about insured or beneficiaries.

Potential new relationships that do not appear to be legitimate are declined. Other examples of money laundering and terrorism financing are given in Annexure VI of this policy.

5. Restrictions

i) Protection and saving (P&S) business should be conducted face to face. Online sale of P&S products is prohibited by SAMA.

ii) No cash payments above SR 10,000 should be accepted from the customers (see Annexure IV for cash receipts).

iii) No transaction should be conducted with any natural / legal person included in UN terrorism list (refer UNSCR 1267).

iv) No transaction should be conducted with Sanctions Countries unless it's approved by Group of Compliance.

6. Detection and notification

According to anti-money laundering rules and regulations, ACIC must immediately notify FIU about any complex, huge, or unnatural activity or transaction, any suspicious transaction in terms of its objectives, any activity or operations that is or might be related to financing a criminal activity, terrorism, terrorists or terrorist organizations. A copy of the notification must be submitted to SAMA's insurance control department.

A detailed report including all data and information about suspicious transactions must be submitted to FIU and SAMA, within 10 days as of the date of notification. This report must include at least the following:

- Documents and contracts of the insurance operations;
- Copies of all documents required to build a working relation;
- Any data relevant to the nature of notified operations and,
- Doubt indicators and justifications with all supporting documents

Suspicious transactions must be notified, independently from their relation with other cases. If a report about a suspicious transaction concluded by the customer was previously sent to FIU, this does not prevent the submission of a new report without any delay when a new suspicious case emerges. Senior Compliance and AML Manager is responsible for executing measures of notification submitted to FIU. He must regularly and effectively determine and notify about suspicious transactions, and review reports relevant to huge or unusual.

FIU notification sample, in Annexure VIII should be used to notify about any suspicious transaction by fax, email, or any other mean approved by FIU to guarantee notification rapidity. In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours. The receipt from FIU must be confirmed for any notification about a suspicious transaction. The receipt from FIU must be kept with the report. If no reply is received from FIU, possibility of sending another notification must be considered.

Particular attention must be given in to relations and commercial activities with companies and individuals, including beneficiaries who work inside or through countries who do not apply or partially apply FATF's recommendations. If an operation without a clear economic or regulatory objective is revealed, its background must be inquired, and results must be submitted in writing to FIU. If SAMA informs the company that a certain country does not sufficiently apply FATF's recommendations, the company must classify all working relations made by this country in **high risks** category.

7. Record Keeping

Sufficient records should be maintained to permit reconstruction of individual transactions (including the amounts and types of currencies involved) so as to provide, if necessary, evidence for prosecution of criminal activity.

All information relating to clients shall be properly kept, in particular the following:

- Details of the client and beneficial owner(s) (if any) of the policy, and any other CDD information required;

- For transactions: the origin of the funds, the form in which the funds were provided or withdrawn, such as, cheques, transfer, the identity of the person undertaking the transaction, the destination of the funds, and the form of instruction and authorization.

- In situations where the records relate to on-going investigations or where records relate to transactions which have been the subject of a suspicious transaction report, they shall be retained until it is confirmed that the case has been closed even if this is still ongoing after 10 years.

- The record of all reports submitted to the money laundering and terrorist finance notification official, with every internal remarks and every analysis of the operations. Also, the record including all notifications submitted to FIU, and all reports developed, including notifications and reports which the money laundering and terrorist finance notification official decided not to submit to FIU.

- All other documents as originals or copies, in paper or electronic form, provided that they are admissible as evidence in a court of law.

- All records on transactions, both domestic and international, shall be maintained for at least ten years after the date of the transaction / end of business.

8. Confidentiality

Employees, managers, officials, and all relevant stakeholders must respect confidentiality and should not disclose any piece of information about any suspicious transaction submitted or to be submitted to FIU. Reports are only available to relevant employees, for that any warning to customers is considered as breach of confidentiality and a contravention. In case of notifying FIU, the company has to be fully aware not to inform the customer about the notification, and should keep on dealing with him normally, until instructions are sent from insurance supervision department at SAMA.

The employee who notify about the transaction is free from any blame or charge, whether the transaction is illegal or not, provided that notification was made with good intention.

9. Business through Third parties

If ACIC counts on a third party to perform customer due diligence procedures, it shall do only:

1) If the third party's headquarter is in any GCC country (except KSA).

2) If the third party's headquarter is in another country which applies appropriately FATF's recommendations, and if the customer is a foreign resident in a foreign country and has a clear objective for the insurance relation in the Kingdom.

3) The third party must be whether an agent, broker, or belonging to any of the insurance service providers.

4) The third party complies with all relevant standards (the responsibility of inquiring about the customer's identity remains on the company and not on the third party).
5) The third part must have ability to apply measures required by all the regulations.

6) When relying on a third party, following must be considered:

   i) Receive copies of documents and information relevant to customer due diligence measures of the third party.
   ii) Take the necessary measures to make sure of the provision of the third party of documents and data relative to customer due diligence procedures when asked, and determine through those documents the responsibility of the company in writing and make all documents and data available once asked and without any delay, in a way to enable the company to make sure of customer due diligence procedures performed by the third party.
   iii) Make sure that the third party is licensed and supervised and controlled by a supervision and control body, and is applying customer due diligence procedures requirements as well as records keeping measures according to FATF's rules and recommendations.
   iv) The company must perform a regular and continuous review to guarantee that the third party is abiding by the standards mentioned in this article, and which can include the review of relevant policies and measures, and the review of implemented customer due diligence procedures.

No reliance should be placed on a third party in a high risk country, such as countries which have no anti-money laundering and counterterrorist finance regulations, or have irrelevant anti-money laundering and counterterrorist finance regulations.

10. Overseas business

In case of dealing with third parties outside the Kingdom, must only deal with licensed insurance and reinsurance companies, licensed insurance brokers and agents, who implement anti-money laundering and counter terrorist finance measures.

ACIC must make sure of the commitment of its sister companies and subsidiaries outside the Kingdom to the following:

a) Adopting the rules and regulations of the Kingdom relative to money laundering and terrorist finance, as well as FATF's recommendations, to the level accepted by hosting countries laws and regulations.
b) In case there is any difference between anti-money laundering and counterterrorist finance requirements in the Kingdom with hosting countries of the ACIC's branches or subsidiaries, ACIC must apply the best requirements on its branches and subsidiaries to the level accepted by hosting countries laws and regulations. In case hosting countries laws and regulations contradict those of the Kingdom, such as the incapacity of the branch or subsidiary to commit to the highest requirements, ACIC must notify SAMA about that and abide by any instructions that might be issued in this regard.

c) If the external branch or subsidiary remains incapable of abiding by the best anti-money laundering and counterterrorist finance requirements, because the hosting country laws and regulations do not allow such thing or for any other reason, ACIC should immediately notify SAMA. When evaluating a country's application of FATF's anti-money laundering and counterterrorism standards, the company must do the following:

- Evaluate the requirements applied to combat money laundering and terrorist finance.
- Attach a special attention to reports evaluating the level of commitment of the concerned country to FATF's recommendations, developed by FATF, IMF, or World Bank.
- Preserve an appropriate level of permanent vigilance towards money laundering and terrorist finance risks, and take into consideration the pieces of information available to the company about the level of money laundering and terrorist finance in the countries where any of our customers work.

11. Screening and training Employees

Companies must make sure that the persons to be employed are tested on the level of expertise, integrity, credibility, skills and competences. Moreover, identities, personal data, and CVs must be investigated. ACIC must determine the main positions that might be targeted for money laundering and terrorist finance purposes. Employees who fulfill such positions must be closely controlled in order to guarantee their credibility as well as their continuous application of antimony laundering and counterterrorist finance policies and measures.

The following training types must be provided on annual basis:

a) New employees: Comprehensive background on money laundering and terrorist finance and regular trainings according to their job description.

b) Sales and consultation employees:

- Make the maximum effort to inquire about the customer (know your customer), money laundering indicators, as well as legal requirements and notification measures relative to suspicious transactions.

- Determine suspicious transactions and unusual customers, and huge transactions measures.

c) Processing employees: Determine and notify about suspicious transactions.

d) Administration: High level training on policies and measures relevant to money laundering and terrorist finance, anti-money laundering and counterterrorist finance programs, as well as cooperation means on local, regional, and international levels.

e) Compliance managers: Intensive training and realistic case studies on the aforementioned regulations, policies, and measures relevant to money laundering and terrorist finance.

12. Enhanced Due Diligence for Non Cooperative Countries

The same measures as for PEPs should be applied to any resident of a Non Cooperative Country as defined by the Financial Action Task Force (inter-governmental body of which the GCC is a member).

As of November, 2014 there are no countries on the NCCT list
As of October 2014, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system (for latest list visit http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/).

Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/TF) risks emanating from the jurisdictions.
Iran Democratic People's Republic of Korea (DPRK)
Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with

the FATF to address the deficiencies** The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.

Algeria
Ecuador
Indonesia
Myanmar

13. Tracking individuals or corporates linked to terrorist organizations

AXA Cooperative should screen its clients database for persons subject to sanctions especially those connected to Al Qaeda or the Taliban, as identified by the United Nations and regularly updated under

http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm

AXA Cooperative Insurance MLRO has access to World-check login which can be used to review new clients against the sanctioned lists. The screening is done on monthly basis. MLRO must investigate the alerts generated and notify the senior management in case of any positive matches

ANNEXURES

Annexure I

KNOW YOUR CLIENT FORM FOR COPRORATE CLIENTS

1. Entity Name:	
1. A CR No.	
2. Registered Office Address: **(Physical address to be provided)**	
4. Primary Line of Business:	
5. Number of Years in Business:	
5. A Date & place of Incorporation	

6. Major Shareholders (with shareholding above 10% of total capital) :

Name	Designation	Business Line

7. Details of authorized signatories (Attach authorized Signatory List) :

Name	Designation

8. Contact person at new customer

For Premium follow ups

Designation:

E-mail ID : _____

Entity Phone no : _____

Fax no : _____

P.o.Box:

Documents to be attached

1. CR Copy
2. Authorized Signatory list

KYC ENHANCED FORM

Additional information to be filled if premium above 10,000 SAR

Total Volume of Business :

Expected Annual premium :

Origin of Funds :

Source of Wealth :

Payment Mode :

Additional documents to be collected.

Attachments :Financial Statements

Annexure II

SUSPICIOUS TRANSACTION INTERNAL REPORT FORM

REPORTER: …… **Date:** ……

Name: …….. Tel: ……

Branch/Dept: …… Position: ……

CUSTOMER:

Name: …….. Account No: ……..……..…

Address: ……..……...

……..……..…

Contact Name: …… Contact Tel: ……..……..…

.

Date Relationship started: …… Customer reference: ……..…….

Type of Policy/Business: ……

INFORMATION/SUSPICION:

Information/Transaction: ……..……...

Reason for Suspicion: ……..……...

……

Additional comments by Branch Manager (if any):

……..

……

……

Name and Signature of the reporter: Date: ……..

Note: *it is an offence to advise the customer / client or anyone else of your suspicion or report*

Comments of AML Manager:

Date: _____ Signature: _____

Annexure III

ANNUAL ACKNOWLEGEMENT FORM FOR THE PREVENTION OF MONEY LAUNDERING
Memorandum

To: All Branch Managers / Employees

From: Compliance & AML Manager

Date: …….

SUBJECT: Annual Acknowledgement Form – Prevention of Money Laundering

As an on-going means of control, you are reminded of the need to be alerted to Money Laundering activities. In this respect, we require you to sign to the effect that you have read the ACIC Anti Money Laundering Policy and that you are aware of your responsibilities under the relevant Laws and Regulations on Money Laundering. You also confirm that if there are any suspicious circumstances which come to your knowledge, the matter will be reported to Senior Compliance and AML Manager immediately in accordance with *Section C - 1 of AML and CTF Policy.*

In case if you have any question, please speak to me or call me.

Please sign and return the copy of this memorandum.

Many thanks and Regards,

Compliance and AML Manager

Confirmed: …… (Branch Manager's / Employee Name)

…… (Signature)

…… (Branch Name and Address)

Annexure IV

LARGE CASH TRANSACTIONS FORM

Date: …….

Reporting Branch: …… **Telephone No:** ……

Fax No: …… **E-mail:** …….

In compliance with of KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING (AML) PROCEDURE HANDBOOK., *Section C-5*, we report the following Large Cash Transactions above the Threshold Limit of SR 10,000.

We also confirm that these transactions are in line with Customer's KYC Profiles.

Date	Name of the customer	Policy Number	Transaction Amount

_____

Name & Signature of Reporting Officer

Comments by Branch Manager:

_____

Branch Manager's Name & Signature: _____

Report sent to:
1. Chief Financial Officer
2. Compliance and AML Manager

Annexure V

Typical Insurance Money Laundering and Terrorism Financing Indicators

General indicators	
Information	Insurance party delays the provision or is reluctant to provide information to enable verification to be completed.
Jurisdiction	Insurance party is introduced by an agent/intermediary operating in an unregulated or loosely regulated jurisdiction.
Payment	Insurance party pre-pays insurance premiums unprecedentedly.
	Large amounts of money are transferred through several non-resident accounts.
	Insurance party requests a large purchase of a lump sum contract when the party usually makes small, regular payments.
Beneficiary	Insurance party transfers the benefit of a product to an apparently unrelated third party.
	Insurance party substitutes the ultimate beneficiary with an apparently unrelated third party.
	Insurance party changes the designated beneficiaries without knowledge or consent of the insurer.
	Insurance party changes beneficiaries simply by signing an endorsement on the policy.
	Insurance party terminates a product early at a loss, and the refund check goes to a third party.
Pre-Sale Indicators	
Conduct	Applicant shows no concern for the performance of the policy but much interest in the early cancellation of the contract.
	Applicant is reluctant to provide background information when applying for a policy.
	Applicant provides minimal or fictitious information.
	Applicant provides information that is difficult or expensive for the institution to verify.
	Applicant uses a mailing address outside the insurance supervisor's jurisdiction.
Payment/ Cash Value	Applicant attempts to use cash to complete a proposed transaction when other payment methods are normally used.
	Applicant attempts to use a third party check to purchase a policy.
	Applicant requests to make a lump sum payment (instead of using installments) by wire transfer or with foreign currency.
	Applicant purchases policies in amounts considered beyond his apparent means.
	Applicant borrows the maximum cash value of a single premium policy soon after paying for the policy.

Policies	Applicant appears to have policies with several insurance companies.
	Applicant cancels a large insurance policy within a short time and requests the return of the cash value payable to a third party
Post-Sale Indicators	
Conduct	Customer is reluctant to reveal the reason for his investments.
	Customer accepts unfavorable conditions that are unrelated to his/ her health or age.
	Customer applies for business outside his normal pattern of Business.
Products/ Policies	Customer requests an insurance product that has no apparent purpose.
	Customer applies for a policy far from his geographical location where similar policies exist.
	Insurance policies premiums exceed the customer's apparent means.
	Insurance policies values are inconsistent with the customer's insurance needs.
Transactions	Customer conducts transaction that results in a conspicuous increase of investment contributions.
	Customer conducts transaction involving an undisclosed Party.
	Customer pays his first premium from a bank account outside the country.

Annexure VI

Saudi Arabian Monetary Agency
Insurance Supervision Department

مؤسسة النقد العربي السعودي
إدارة مراقبة التأمين

His Excellency Head of the Financial Investigation Administration

Peace be upon you,

Please find above our report number dating regarding a doubtful financial operation, we hope you investigate it and make the necessary arrangements.

Official Seal: Position:

Suspicious Transaction Report

Number:	
Date:	/ /14 H.
Corresponding:	/ /200 A.D.
Annexes:	

To report a suspicious transaction, this form should be filled out and sent to the Financial Investigation Unit on the following address:
Riyadh – King Fahed Road in the South Side of the Ministry of Interior Building
Fax number: (01) 4127615 – (01) 4127616
To report by phone call the free phone number: 8001222224 around the clock
For inquiries call the phone number: 013128100

(Confidential)

Reporting of a Suspicious Financial Transaction

Section A - Reporting Party Information

Section A.1 - Company Information

Type of Company	Insurance ☐	Reinsurance ☐	Insurance Service Provider ☐
Company Name			
Head Quarter			City
Branch Name			City
Phone Number			

Section A.2 – Informant Contact Information

Name	
Phone Number	
Address	

Section B - Report Content

Section B.1- Policy Information

Type or Class of Policy			
Policy Number			
Premium Amount			
Payment Period			
Payment Method			
Policy Issuing Date	Day	Month	Year
Canceled?	Yes ☐	No ☐	
Cancellation Date	Day	Month	Year
Claims Paid?	Yes ☐	No ☐	
Claims Amount	In numbers SAR	In writing	

Section B.2 - Suspicious Transaction Information

Transaction Execution Date	Day	Month	Year
Type of Transaction			
Total Amount			
In Numbers			
In Letters			
Currency Type			
Policyholder/ beneficiary Information			
Name			
ID Number			

Nationality	

Executor information if different than policyholder

Name	
ID Number	
Nationality	

Causes of Suspicion	

Accompanying Documentation

The Reporting Party should enclose copies of all documents relating to the suspicious transaction including:

- Documents related to payments made (e.g., Receipt, Check, Credit Card Receipt)
- ID of Policyholder
- Copy of the Insurance Policy