



ANTI - MONEY LAUNDERING POLICY MANUAL



شركة الخزنة للتأمين ش.م.ع.
Al Khazna Insurance Company P.S.C.



شركة الخزنة للتأمين
Al Khazna Insurance Company P.S.C.

Anti-Money Laundering Policy Manual

Manual No: AK - 14

Version No: 01

Date: 1/11/2015



شركة الخزنة للتأمين ش.م.ع.
Al Khazna Insurance Company P.S.C.

ANTI-MONEY LAUNDERING POLICY MANUAL

Manual No: AK - #14

Version: 01

Date: 1/11/2015

This document contains confidential information and remains the property of Al Khazna Insurance Company P.S.C. It is not to be used for any other purposes, copied, distributed or transmitted in any form or means or carried outside the company premises without the prior written consent from the management.



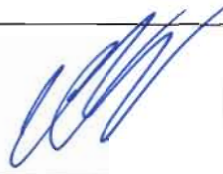


	Name & Title	Signature	Date
Prepared By	Governance and Compliance Department		09/11/15
Review & Approved by	Head of Internal Audit		10/11/15
Approved on behalf of Board of Directors	Chairman of Audit Committee		10/11/15



TABLE OF CONTENTS

S. No	Index	PAGE NO
1	Introduction	5
2	Relevant Laws	6
3	Potential methods on how AKIC can be implicated in money laundering	6
4	Key Preventive Measures to Mitigate such risks	7
5	Know Your Customer (KYC)	8
6	Processes to Prevent Money Laundering Practices	9
7	Reporting and Discloser	9
7-A	Internal Disclosure	9
7-B	External Disclosure	9-10
8	Appendix – STR Form	13



1. Introduction

Put simply, money laundering involves concealing the identity of illegally obtained money so that it appears to have come from a legal source.

The UAE Central Bank has defined money laundering as “any transaction aimed at concealing or changing the identity of illegally obtained money, so that it appears to have originated from legitimate sources, where in fact it has not”.

Typically, there are three acknowledged phases to money laundering: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the “dirty money” appears “clean.

Criminals do not want these funds to be detected by law enforcement or revenue agencies, so they convert their dirty money into an asset, which appears legitimate, such as an insurance policy, bank deposit casino cheque or even real estate. Insurance products, particularly life insurance, provide a very attractive and simple means of laundering money. 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.

Definition of Money Laundering as per UAE Federal Law No (4) for 2002

Money laundering where a person intentionally commits or assists in commission of any of the acts in respect of property derived from any of the offences below shall be considered a perpetrator of the money laundering offence:

- a. The conversion, transfer or deposit of proceeds, with intent to conceal or disguise the illicit origin of such proceeds.
- b. The concealment or disguise of true nature, source, location, disposition, movement, rights with respect to or ownership of proceeds.



c. The acquisition, possession or use of such proceeds.

For the purposes of this law, property shall mean those derived from the following:

- a. Narcotics and psychotropic substances.
- b. Kidnapping, piracy and terrorism.
- c. Offences committed in violation of the environmental laws.
- d. Illicit dealing in fire-arms and ammunition.
- e. Bribery, embezzlement, and damage to public property.
- f. Fraud, breach of trust and related offences.
- g. Any other related offences referred to in international conventions to which the State is a party.

2. Relevant laws

- Federal Law no. 4 of 2002 regarding Criminalization of Money Laundering.
- Central Bank of UAE Circular no. 24 of 2000 and its corresponding addendum.

3. Potential methods on how AKIC can be implicated in money laundering.

- Criminals use dirty money to purchase a general insurance policy to insure some high-value goods.
- These goods had also been purchased with dirty money.
- Subsequently a fraudulent claim is made against the policy.
- The insurance company unknowingly settles the claim.

AKIC does not offer the typical long term life insurance products. AKIC's product range includes motor, property, Marine and Hull, Engineering, Fire, General Accident, Life and Medical through direct and brokers channels.

There are a number of ways that launderers can use insurance products. Some of the red flags that may indicate money laundering include:

- 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.
- Cancellation of policies for return of premium by an insurer's



- Overpayment of premiums with a request for refund of the amount paid.
- 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.
- Terrorism could be facilitated through property and casualty converge include use of worker's compensation payments to support terrorist awaiting assignment and primary coverage and trade credit for transport of terrorist materials, this could also imply breach of regulations requiring the freezing of assets.
- Doing business with brokers through credit then brokers request refund by cancelling policies.
- Brokers settle premiums by clients directly to insurance companies.
- A customer who wishes to fund its policy using payments from a third party.
- Purchasing one or more single-premium policies, and then cashing them in a short time later.
- Premiums being paid into one policy, from different sources, where the relationship between the policyholder and beneficiary seems unusual.

4. Key preventive measures are recommended to mitigate such risks:

1. First, establish and maintain effective internal policies, procedures, and controls to prevent opportunities for money laundering. The money laundering compliance program should be defined by the higher management or the board of directors. Companies must consider local regulations prior to adopting a compliance program.
2. Second, appoint a compliance officer. When a complaints officer is appointed, it is imperative to verify that the qualifications of that person meet the local requirements. The compliance officer should be responsible for the business's day-to-day compliance with the anti-money laundering laws, and for ensuring the compliance program is updated, as needed. The compliance officer should be responsible for overseeing ongoing education and training program. The compliance officer should also be responsible for maintaining records and reporting suspicious cases to the relevant authority.
3. Third, it is important to obtain details of customers in order to verify their identities, including full name and address, passport or identity card (for individuals) and trade license (for companies). Such information must be periodically and regularly updated. The more a company knows about its customers, the better can money laundering abuses be prevented.



4. Fourth, policies and procedures must be adopted for the identification and reporting of suspicious activity. UAE regulations must be reviewed for what it considers to be a suspicious transaction as well as the allowable time delays to report such activity.

5. Fifth, establish an ongoing employee-training program for all employees. Effective training should present real-life money laundering examples, preferably cases that have occurred in AKIC, including how the pattern of activity was first detected and its ultimate impact on the company.

6. Sixth, conduct an independent audit of its anti-money laundering compliance program to assure its adequacy. Such an audit should be conducted periodically based on the risks faced by the company and the requirements of the UAE regulations.

5. Know Your Customer (KYC)

To determine whether your customers fit into the high-risk category, it is advisable to check the following:

- Identifying the customer and/or broker and obtaining identification information from him. This information includes full name, unique identification number, existing residential
- Address, contact telephone number, date of birth and nationality. Different particulars are required from non-personal customers such as companies.
- Know your customer form must be update regularly.
- Verifying the identity of customers using reliable, independent sources, and keeping a copy of all reference documents used to verify their identity.
- Identifying and verifying the identity of payees before making certain types of payment such as surrendering a life insurance policy or refunding a premium.
- Obtaining from the customer, when establishing business relations, information as to the purpose and intended nature of business relations.
- Ongoing monitoring of business relations with customers.
- Conducting scrutiny of transactions undertaken to ensure that transactions are consistent with the life insurer's knowledge of the customer.
- Paying attention to all unusual transactions.
- Periodically reviewing customer identification information to ensure the information is kept up-to-date.



- Having procedures to address risks associated with non-face-to-face relationships or transactions.
- Performing enhanced Customer Due Diligence (CDD) on high-risk customers such as politically exposed persons.

6. Processes to Prevent Money Laundering Practice

- Not deal with any person on an anonymous basis or any person using a fictitious name.
- Report all transactions suspected of being connected with money laundering or terrorist financing.
- Develop and implement policies, procedures and controls to help prevent money laundering and terrorist financing, including the appointment of a management-level compliance officer.
- Provide regular anti-money laundering and combating the financing of terrorism training to staff and agents.
- Perform customer due diligence measures when establishing business relations with any customer, or when undertaking any High amount transactions for any customer who has not otherwise established business relations with the insurer.

7. Reporting and Disclosure

A. Internal disclosure:

Any staff or Board member who suspects a client, broker, colleague or any other party are involved in money laundering has an obligation by law to declare the incident. The relevant document, which is attached to this policy, should be completed and a copy should be submitted to the compliance officer in duplicate. The compliance officer has the obligation of recording the incident in the Incident register of the company. Should the compliance officer be suspected of being involved in money laundering, the plaintiff should inform the CEO/ MD of the incident and then proceed with external disclosure to the Central Bank or DFSA

B. External disclosure:

The Federal Law No. 4 of 2002 regarding Criminalization of Money Laundering creates an obligation on all Financial Institutions to report suspicious transactions to the Anti-Money Laundering and Suspicious Cases Unit "AMLSCU". The Central Bank uses the term



Suspicious Transaction Report “STR” (Refer to addendum to circular number 24/2000 of the UAE’s Central Bank) to refer to such reports lodged by Financial Institutions. For STR template refer to Appendix.

The AMLSCU has made it clear through various public outreach events that suspicious activity report should not be restricted to reporting of suspicious transactions.

STR should include:

- Any suspicious transactions;
- Any attempted suspicious transactions;
- And any suspicious activity or behavior, including the actions of customers or potential customers.

STR should be submitted using the approved form and include all information that supports your STR; any additional information which would help the AMLSCU to further its investigations; and any additional information which could link the STR to other STRs and other investigations if possible.

Information contained in an STR is confidential and Article 20 of the UAE Federal Law No. 4 of 2002 provides Relevant Persons with a protection from any criminal, civil or administrative liability which may result from providing the required information, provided, it is submitted in good faith.

Following the STR submission a Relevant Persons will often have on-going dialogue with the AMLSCU as the investigation continues and more information may be requested. The AMLSCU will provide the Relevant Person with a final outcome when a conclusion is reached.

The AMLSCU may instruct us on how to continue our business relationship with the subject of an STR. If the subject of the STR expresses a wish to move funds before you receive instructions from the AMLSCU, we should immediately contact the AMLSCU for further instructions.

Under Article 15 of the UAE Federal Law No. 4 of 2002 the failure to report an STR to the AMLSCU by those who are aware of a suspicious activity or transaction may be a criminal offence, punishable by a fine or imprisonment or both.

Tipping off if a Relevant Person submits an STR, the Relevant Person or its employees must not inform or tipoff the subject of the STR that a report has been lodged, or that the person is being investigated. Tipping off is an offence created by Article 16 of the UAE Federal Law No (4) of 2002 and is punishable by a fine or imprisonment or both.



When submitting an STR do submit all supporting documentation with your STR; submit an STR for suspicious behavior only i.e. no transaction is required; provide a soft copy of the STR form, rather than submitting a handwritten STR; submit an STR within a reasonable timeframe of identified suspicious; include all relevant details in your STR including source of funds, linked accounts, etc. report confidentially without involving unrelated people as it could alert the customer and be considered as ‘Tipping Off’; maintain your STRS as per the record keeping requirements; send additional STR when further information comes to light in order to supplement the original suspicion; ensure that to make references to previous submissions; provide contact details so that the AMLSCU can contact you with follow up questions; provide a clear trail of the cause for suspicions and as much detail as possible about the person(s) involved; notify AMLSCU at the Central Bank of any STR you have lodged. Do not terminate the relationship intentionally prior or post raising the STR unless there is a logical and/or unavoidable reason behind such action. Wait for an official response from the AMLSCU; do not insert “refer to documents attached” under “Source of Suspicion.” A brief explanation in the space provided is required and identify the suspicion clearly and concisely. Do not forget to notify when you have lodged an STR with the AMLSCU.

Central Bank

The requirement to lodge a suspicious transaction report with the Central Bank of the UAE AMLSCU is contained in UAE Federal Law No. 4 of 2002 regarding criminalization of money laundering. The details of the AMLSCU are:

Central Bank of the UAE,
AMLSCU, P0 Box 854
Abu Dhabi, UAE
Tel; +971 2 666 8496,
Email; cbuaeamlscu@cbuae.gov.ae

DFSA

The AML Module of the DFSA Rulebook also contains a requirement that Relevant Persons report suspicious activities, including transactions, to the AMLSCU. A Relevant Person is also required to notify the DFSA immediately following the submission to the AMLSCU.



Appendix



نموذج تقرير معاملة مشبوهة
Suspicious Transaction Report(STR)

To: The Manager-in-charge AMLSCU Abu Dhabi:02 6669437 Fax: 02 6669427	عناية: المدير المسؤول وحدة مواجهة غسل الأموال والحالات المشبوهة أبوظبي: ٠٢٦٦٦٩٤٣٧ فاكس: ٠٢٦٦٦٩٤٢٧
Subject: Suspicious Transaction Report(STR)	الموضوع: تقرير معاملة مشبوهة
Full Name of Investor:	الإسم الكامل للمستثمر:
Passport No./Details of License:	رقم جواز السفر/تفاصيل الرخصة:
Nationality:	الجنسية:
Address/ Known Addresses:	العنوان/ العناوين المسجلة:
Amount of suspected transactions:	مبالغ المعاملات المشبوهة:
Source of suspicion:	مصدر الشك:
Brokerage Firm Name:	اسم شركة الوساطة:
Signature of employee in charge:	توقيع الموظف المسؤول:
Date:	التاريخ:

AML2