ANTI MONEY LAUNDERING & COMBATING TERRORISM FINANCING RULES

قواعد مكافحة غسل الأموال وتمويل الإرهاب لشركات التأمين

Insurance Supervision Department
إدارة مراقبة التأمين
SAMA would like to introduce the draft statute of Anti Money Laundering & Combating Terrorism Financing Rules, which will be applied to combat money laundering and terrorist financing related to insurance activities. SAMA is requesting insurance companies, insurance service providers and the public a written response/comments to make visual observations. The written response/comments on this Code should be sent within 20 days of the date of its publication and be addressed to:

Mr. Mohammad A. Al Shayea,
Director of Insurance Supervision.

الأستاذ/ محمد بن عبد العزيز الشابع
مدير مراقبة التامين.
CONTENTS

Introduction

General provisions relevant to the requirements of anti-money laundering and counterterrorist finance measures

Business relation acceptance conditions, customer identification process and customer due diligence procedures

Anti-money laundering and terrorist financing internal policies

Compliance procedures

Detection and notification about suspicious transactions

Records keeping

Customers’ categories and risk levels assessment

Policies and procedures relative to the company’s activities outside the Kingdom

Regulatory sanctions

Annexes

Annex (1) Money laundering indicators
Annex (2) Financial Intelligence Unit (FIU) Notification Sample
Saudi Arabian Monetary Agency ("SAMA")
Anti Money Laundering & Combating Terrorist Financing Rules

Introduction

Objective of these regulations

1. The objective of these rules is to confirm the compliance of insurance and reinsurance companies, including subsidiaries of foreign insurance and reinsurance companies, and insurance service providers, with restrictions, procedures, rules, and principles in the field of anti-money laundering and terrorist financing, in a way to apply the following:

   a) Implement the Law on Supervision of Cooperative Insurance Companies and its Implementing Regulations, especially articles 2, 10, 12, 15, 16, 19, 55, 56, 71, 76, 77, and 78.

   b) Implement anti-money laundering Law under the Royal Decree number M/39, dated on 25/6/1424H and its Implementing Regulation.


   www.fatf-gafi.org/document
   والتصديقات السبع الخاصة بمكافحة تمويل الإرهاب الصادرة عن مجموعة العمل
   www.fatf-gafi.org/document
   والاتفاقيات الدولية لمنع تمويل الإرهاب (نيويورك 1999)، واتفاقيات الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات

d) Protect licensed companies and their customers as per the Insurance Implementing Regulations, from illegal transactions or exploitation as canals for money laundering or terrorist finance activities or any other criminal activity.

e) Safeguard, protect, and promote the confidence, the integrity, and the credibility of the Insurance sector, and protect insured people.

Definitions

2. 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.

Terrorist finance: Financing terrorist operations, terrorists, and terrorist organizations.

Actual beneficiary: Any natural personality who is the final owner or the dominator of the customer's funds, or who implements any operation or task on his behalf, or any person who has an effective or final control on a legal personality or a legal procedure.

Know your customer: Procedures of customer identification as well as about provided information, by collecting detailed pieces of information about any

Definitions

2. 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.

Terrorist finance: Financing terrorist operations, terrorists, and terrorist organizations.

Actual beneficiary: Any natural personality who is the final owner or the dominator of the customer's funds, or who implements any operation or task on his behalf, or any person who has an effective or final control on a legal personality or a legal procedure.

Know your customer: Procedures of customer identification as well as about provided information, by collecting detailed pieces of information about any
Customer or transaction, such as identities, effective documents of individuals, companies, owners, partners, real beneficiaries, legal signatories, agents, and others; postal address, financial address, email address, phone numbers, the nature of works, information, and the capital for legal facilities; funds sources, subsidiaries, countries, and dealt with or by products, and all what is required to be known about the customer or the transaction.

Customer due diligence: Policies, restrictions, and measures that must be implemented by companies in order to know more about the customer and inquire about his identity and insurance objectives, as for the majority of transactions/relations, especially the cases of customers considered by companies as high risk customers and requiring due diligence, such as politically uncovered, non-profitable organizations, and others.

Suspicious transaction: It is the transaction considered by the company's employee as bad or illegal. It is necessary to notify the competent authorities about such transactions through the report of suspected transactions. The employee who notifies about such a transaction is free from any blame or charge, whether the transaction is legal or not, provided that notification was made with good intention.

Unusual transaction: A transaction that does not comply with the customer's data, objectives, and transactions register. 
Hint: Notifying, hinting, implicitly considering or noting that the company or
any other authority might be inquiring or is considering inquiring about the customer or any of his transactions.

Company – companies: Insurance and reinsurance companies, as well as insurance service providers including insurance brokers, insurance agents, reinsurance brokers, and reinsurance agents.

Subsidiaries: A company whose majority of actions are owned by the mother company, whether inside or outside the country.

Attachment: shall mean the provisional ban on transferring, exchanging, disposing with or moving funds and proceeds or attaching same pursuant to an order by a court or a competent authority.

Supervisory Authorities: shall mean government authorities that have the power to license, supervise and/or oversee companies.

Competent Authorities: shall mean all government authorities that are authorized to combat money laundering and terrorist financing each within its own jurisdiction.

Working relation: It is the working relation or professional or commercial relation between the company and any customer. This relation does not require the participation of the company in any effective transaction or transactions. Advice and consultation is considered as working relation.

Customer: Any individual customer or an execution individual customer, whether natural or legal, or any customer who is provided with insurance by the company.

Financial Intelligence Unit: Financial Intelligence Unit of the Ministry of Insurance Supervision Department.
Non-profit organizations: Any legal personality (institution or entity) which main activity consists of fund-raising and disbursing funds for religious, educational, cultural, or social purposes, or any other charity activity.

Political personality: Any person who occupies or had recently occupied, or aiming at or is candidate to occupy a high civil position at the government, or military position, or any position at a State company, etc. This definition covers the direct members of the person’s family (such as wife, parents, children, brothers and sisters), and all cooperating persons. The cooperating personality is anyone who works as consultant or agent for the aforementioned person.

Notification: The act by which the company notifies the Financial Intelligence Unit about any suspected transaction, including the submission of a report.


Third party: Any natural or legal personality who, on behalf of the customer/beneficiary, deals with the company, or provides it with customers, such as brokers, insurance agents, or any local or international liberal professions employers.

KSA Initiatives
3. The recent few years witnessed fast, long-term, and wide developments on the level of the international financial sector. It included comprehensive and harmonized struggle against money laundering and terrorist financing. Therefore, KSA adopted many initiatives including judicial measures and other measures which respond to international developments. Following are some of these initiatives adopted in KSA:

**International level**
- KSA signed and ratified the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna 1988)
- KSA signed and ratified the International Convention for the Suppression of the Financing of Terrorism (New York 1999)
- KSA is a member State of GCC and is a full member of the Financial Action Task Force (FATF)
- In September 2003, KSA completed the mutual evaluation by a team of FATF, based on 40 + 8 FATF recommendations. It was one of the first countries to be evaluated as per this new approach. The results of this evaluation were discussed during a
plenary session held in February 2004 in Paris, and were very positive.

**Regional and collective level**

- On the sidelines of a conference held in April 1998, KSA signed and ratified the Arab Anti-Terrorism Convention, under the auspices of the Arab League.
- In May 2004, KSA signed and ratified GCC Convention on Combating Terrorism.
- KSA is a founder State of MENA FATF, created in November 2004, the objective of which is to promote and implement anti-money laundering and counterterrorist finance international standards, and which adopted 40 + 9 anti-money laundering and counterterrorist finance recommendations of FATF.

**المستوى الإقليمي والجماعي**

- على هامش مؤتمر عقد في شهر أبريل 1998، وقعت المملكة العربية السعودية وأقرت الاتفاقية العربية لمكافحة الإرهاب برعاية جامعة الدول العربية.
- في شهر يوليو 1999، وقعت المملكة العربية السعودية وأقرت اتفاقية منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي.
- في شهر مايو 2004، وقعت المملكة العربية السعودية وأقرت اتفاقية دول مجلس التعاون الخليجي لمكافحة الإرهاب.
- إن المملكة العربية السعودية هي عضو مؤسس لمجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (مينا - فاف) التي أنشئت في شهر نوفمبر 2004 ويقوم هدفها على ترويج وتنفيذ المعايير الدولية.
National level

- On 25/6/1424H, KSA issued the Anti-Money Laundering Law and its Implementing Regulation, under the Royal Decree number M/39, dated on 25/6/1424H, and as per the Decision of Council of Ministers number 167 dated on 20/6/1424H. It presented therefore a legal basis to criminalize money laundering and terrorist finance activities.

- Under article 11 of Anti-Money Laundering regulation, the Financial Intelligence Unit was created at the ministry of interior, to be the central authority which receives and analyses reports on suspicious transactions and relevant to money laundering and terrorist finance activities.

- KSA formed two permanent national committees of different ministries and governmental bodies, including SAMA, to tackle money laundering and terrorist finance issues in the Kingdom.
SAMA initiatives
Since its foundation in 1952, SAMA issued a multiple series of guidelines to the parties which are under its supervision, relevant to defining the identity of customers as well as other information, customer due diligence instructions when dealing with customers, keeping relevant documents and files, in addition to notifying concerned authorities about suspected transactions. Those guidelines were mentioned in a number of regulatory and pilot guides.

In November 1995, SAMA issued its first set of guidelines relevant to anti-money laundering activities to all banks operating in the Kingdom. Therefore, recognizing the international and legal supervision efforts to combat the phenomenon of money laundering, SAMA updated its guidelines of 1995 and issued in 2003 a more comprehensive set of "rules governing anti-money laundering and counterterrorist finance".

General provisions relevant to the requirements of anti-money laundering and counterterrorist finance measures

General implementation of anti-money laundering and counterterrorist finance measures

4. Every company should implement the rules relevant to the recommendations published by FATF, including detailed commitments and measures which will be mentioned at a later stage, and which must be taken by the company to prevent money laundering and terrorist financing. The company must take into consideration the nature of its activities, its organization...
structure, the type of its customers and transactions at the time of setting anti-money laundering and counterterrorist finance policies and measures. It has as well to make sure of the sufficiency and relevance of measures taken compared with general requirements and objectives mentioned in these rules.

5. Companies must commit to the following:

a) Develop written policies and procedures aiming at combating money laundering and terrorist financing, as per article 15 of Insurance Implementing Regulations; confirm the full compliance with all regulatory and procedural requirements, including registers keeping and cooperation with the Financial Intelligence Unit of the ministry of interior and the competent authorities responsible for the implementation of Anti-Money Laundering and Counterterrorist Finance Rules and its Implementing Regulations, including the disclosure of information at the appropriate moment.

b) Make sure of the full understanding of all company's officials and employees of the content of those rules, and take all necessary measures to combat money laundering and terrorist financing.

c) Review anti-money laundering and counterterrorist finance policies and procedures in a regular way to insure their effectiveness, including the review of policies and measures relevant to anti-money laundering and counterterrorist finance policies and procedures issued by the internal audit department or the compliance official to insure compliance, including: (1) evaluating the rules of detecting any money laundering or terrorist finance transaction, (2) evaluating, reviewing, and verify the
validity of exceptional reports of huge or unusual transactions, (3) review the quality of notification about suspected transactions, (4) evaluating the level of knowledge of customer service employees.

d) Develop and implement policies and procedures relevant to customer's acceptance and dealing with him, develop customer due diligence procedures, stipulated by article 15 of the Rules, taking into consideration the risks of money laundering and terrorist financing, according to the type of the customer, his transactions, and the working relation with him.

6. Anti-money laundering and counterterrorist finance policies and measures must clarify the following:

Money laundering steps
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.

The company must be aware that the insurance sector is exposed to transactions that might aim at money laundering and
terrorist financing. We mention some transactions as example:

- A lump sum added to the life insurance contract.
- A lump sum added to personal pension contracts.

The company must also be aware that the techniques adopted to finance terrorism are essentially the same techniques adopted to hide sources and usage of money laundering. However, the main differences between the two are:

- Small amounts of money are usually required to commit terrorist acts in an individual manner; therefore, it is difficult to track terrorist funds.
- Terrorists can be financed by incomes received in a legal manner, for that it is difficult to define the period during which legal funds became terrorist funds.

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

الإرهاب، ومن هذه العمليات على سبيل المثال لا الحصر ما يلي:

- مبلغ مقتطع يضاف إلى عقد تأمين على الحياة.
- مبلغ مقتطع يضاف إلى عقود التقاعد الشخصية.

كما ينبغي عليها كذلك إدراك أن التقنيات المستخدمة لتمويل الإرهاب هي بشكل أساسي التقنيات المتبعة لإخفاء مصادر واستخدامات الأموال، ولكن الفوارق الرئيسية بين الاثنين هي أن:

- غالبًا ما تكون المبالغ الصغيرة من الأموال مطلوبة لاقتراف أفعال إرهابية فردية، وتجعل من الصعب تفكي الأموال الإرهابية يمكن تمويل الإرهابيين من مداخل يتم الحصول عليها بشكل مشروع، إذ يكون من الصعب تحديد المرحلة التي أصبحت فيها الأموال الشرعية أمولاً إرهابية.

والإرهابيون يستطيعون الحصول على مداخيلهم من مجموعة متنوعة من المصادر، غالبًا ما تجمع بين التمويل النظامي وغير النظامي. ويمكن تصنيف أشكال التمويل على سبيل المثال في الأنواع التالية:

- الدعم المالي
  يمكن أن يأتي هذا التمويل على شكل هبات خيرية، والتماس مساعدة المجتمع المحلي ومبادرات أخرى لجمع الأموال قد تأتي من كيانات أو أفراد.
Companies must categorize operations and customer categories according to the level of risks relevant to the possibility of money laundering and terrorist finance. Moreover, the specific types of operations must comply with the identification of customers, in order to develop a comprehensive and integrated approach about money laundering and terrorist financing, and develop a customer identification sample specifying that.

Companies must set a minimum value for operations that require an inquiry about possible money laundering activity or terrorist financing, such as a transaction of more than 10,000 SR. Such operation requires a maximum effort to inquire about customers and the objective of the operation. Companies must put down the results of the inquiry in writing. Companies should not accept any cash amounts of more than 10,000 SR. Any such amount must be collected according to bank transactions such as checks, points of sale, direct transfer, etc.

Cooperation and communication means

Companies must develop policies and procedures that explain the
communication mechanism with SAMA. These policies and procedures must include the following at least:

a) Information about the ways of communication with the official responsible for anti-money laundering and counterterrorist finance measures at the company.

b) Communication processes adopted in cases of applications submitted by SAMA, as well as the ways of submitting reports to SAMA.

10. Companies must create effective communication networks with brokers and agents in order to exchange information at the required pace to combat money laundering and terrorist finance.

11. The Company, 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 counterterrorist finance measures.

12. When a company buys fully or partially another company or any third party in a foreign country, it must make sure that the acquired company or third party is or will be governed by customer due diligence procedures at the time of acquisition, according to the requirements of these rules, with the exception of the following two cases:

a) If the acquired company or third party keeps records of customer due diligence for all its customers including information relevant to the customer’s data, and if the company has no doubt about the relevance of available information.

b) Eجراءات الإتصال المتبقية في حالات معالجة الطلبات المقدمة من المؤسسة وكذلك طرق تقديم التقارير إلى المؤسسة.

10. على الشركات إنشاء قنوات إتصال فعالة مع الوسطاء والوكالات بهدف تبادل المعلومات وبالسرعة المطلوبة لكافحة غسل الأموال وتمويل الإرهاب.

11. على الشركة، في حال التعامل مع أطراف ثالثة خارج المملكة، التعامل فقط مع شركات التأمين وإعادة التأمين المرخصة ووسطاء ووكلاء التأمين المرخصين الذين يطبقون تدابير مكافحة غسل الأموال وتمويل الإرهاب.

12. يجب على الشركة عند قيامها باستحصال الكامل أو الجزئي على شركة أو أي من الأطراف الثالثة في دولة أجنبية، التأكد من أن الشركة أو الطرف الثالث التي تم الاستحواذ عليها تطبق أو سوف تطبق إجراءات العناية الواجبة تجاه عملائها عند الاستحواز وفقا لمتطلبات هذه القواعد، إلا في الحالتين الآتيتين:

ا) إذا كانت الشركة أو الطرف الثالث المستحوذ عليه يحتفظ بسجلات إجراءات العناية الواجبة لجميع العملاء بما في ذلك المعلومات المتعلقة ببيانات العمل، ولم يكن لدى الشركة أي شك في صحة أو ملاءمة المعلومات.
b) If the company inquires about the customer due diligence performed by the acquired company or third party, so that there will be no doubt about their compliance with anti-money laundering and counterterrorist finance measures and restrictions.

Working relation acceptance conditions, customer identification and customer due diligence procedures

13. The Company must conduct customer due diligence procedures in the following cases:
   a) Build a working relation

b) Have suspicion about any money laundering or terrorist finance activity

14. The Company must take all necessary measures enabling it to receiving of integral and real data about any customer and his insurance objectives. It must not provide products and services to persons having anonymous or illusionary names or persons with whom it is restricted to deal.

15. The Company must apply customer due diligence procedures on all customers, by taking the following steps:
   a) Inquiring about the identity of the customer, by using the required

c) Have suspicion about the relevance of pieces of information, data, or documents received from the customer to inquire about his identity.

Insurance Supervision Department

15. On the company applying the following steps:
   a) Implementing the initially due diligence procedures to ensure the accuracy of the customer's information,
   b) Implementing the following procedures:
   c) Implementing the following procedures:
   d) Implementing the following procedures:

Have suspicion about the relevance of the customer's information, whether it is accurate or not.

Customer identification and customer due diligence performed by the acquired company or third party, so that there will be no doubt about their compliance with anti-money laundering and counterterrorist finance measures and restrictions.

Insurance Supervision Department

15. Implementing the following steps:
   a) Implementing the initially due diligence procedures to ensure the accuracy of the customer's information,
   b) Implementing the following procedures:
   c) Implementing the following procedures:
   d) Implementing the following procedures:

Have suspicion about the relevance of the customer's information, whether it is accurate or not.

Customer identification and customer due diligence performed by the acquired company or third party, so that there will be no doubt about their compliance with anti-money laundering and counterterrorist finance measures and restrictions.
original documents according to anti-money laundering rules and regulations, and article 16 of this rules. This applies to all legal signatories on insurance transactions.

b) Inquiring about the actual beneficiaries and dominating parties on the insurance transaction according to anti-money laundering rules and regulations, and article 16 of this rules.

c) Receiving information about the purpose on the nature of the working relation according to the type of customer, the working relation or the operation, to enable the company of performing the customer due diligence procedures in a continuous manner.

d) Making sure of the compliance of customer due diligence procedures in a continuous manner, such as continuous audit in all operations concluded during the working relation period to guarantee that all operations comply with the knowledge and the data of the customer.

16. When inquiring about the identity of the customer and the actual beneficiary of the insurance operations, the company must get informed about effective original documents, as per the following:

a) Natural personalities

Saudi citizens:
- National identity card or family record.
- The address, the residence and the working place of the person.

Individual foreigners:
- Residency or five year residency card, GCC citizens passport, or diplomatic card for diplomats
- The address, the residence and the working place of the person.

المواطنون السعوديون

- بطاقة الهوية الوطنية أو سجل الأسرة.
- عنوان الشخص ومكان إقامتة ومحـمل عمله.

المواطنون الأفارد:
- إقامة أو بطاقة الإقامة الخاصة ذات
ب) Legal personalities:
It is necessary to acquire the biggest amount of information and documents to know the nature and the quality of the legal personality, according to the relation or the insurance transaction as it is mentioned below.

Licensed companies, enterprises, and shops:
• A copy of the commercial registration from the Ministry of Commerce and Industry
• A copy of the article of association, its annexes, or the memorandum of association, annexes and any modifications.
• A copy of the manager in charge identity card.

Non lucrative bodies and institutions:
• A copy of the license issued by a relevant governmental body
• A permit from the Board delivered to the persons who will be charged with building working relations with the company, such as the President, the V.P, or the financial manager, and copies of their identities

Governmental sectors:
A copy of all required documents according to the regulation and the administrative rules of the governmental body.

السنوات الخمس أو جواز السفر
لمواطني دول مجلس التعاون لدول الخليج العربي أو البطاقة الدبلوماسية للدبلوماسيين.

• العووان ومكان الإقامة و محل العمل.

B) الأشخاص الاعتباريون:
ينبغي الحصول على أكبر قدر ممكن من المعلومات والمستندات للتعرف على طبيعة نوعية الشخص الاعتباري حسب حجم العلاقة أو العملية التأمينية كما هو وارد أدناه.

الشركات والمؤسسات والمحال المخصصة:
• نسخة من السجل التجاري الصادر من وزارة التجارة والصناعة.
• نسخة من النظام الأساسي للشركة وملاحقه أو عقد التأسيس و ملحقه وأي تعديلات عليها.
• نسخة من بطاقة هوية المدير المسؤول.

الهيئات والمؤسسات غير الهادفة للربح:
• نسخة من الترخيص الصادر عن الجهات الحكومية ذات العلاقة.
• تفويض مجلس الإدارة إلى الأشخاص الذين سيؤلون إقامة علاقة عمل مع الشركة مثل الرئيس، نائب الرئيس أو المدير المالي، ونسخ من هوية كل منهم.
• نسخة من النظام الأساسي.

القطاعات الحكومية:
• نسخة من جميع الوثائق المطلوبة وفقاً لنظام الجهة الحكومية وتنظيمها الإداري.
17. If the company has reasons to doubt about the credibility of information provided by the customer, it has to use all the possible means to inquire about the relevance of the pieces of information, as calling the phone numbers of the house or work, etc.

18. Companies must make sure that applicants do not use fictitious names and that an insurance document for an anonymous person was not issued. The steps of determining customers must include the following at least:

a) Inquire about the identity of the applicant by using governmental documents (such as identity cards and passports, etc.), as stipulated in article 16 of the Rules.

b) Determine the beneficiary and inquire about his/her identity by using governmental documents, (such as identity cards and passports, etc.), as stipulated in article 16 of the Rules.

c) Receive information about the objective of building the working relation between the applicant and the company.

d) Receive a memorandum of association or similar justification on creation or existence, and receive information relevant to the formal form of the applicant, his address, his managers, his high management, as well as the provisions that the applicant commits to abide by.

19. The Company must make sure of the applicant/beneficiary address by using the appropriate measures (such as receiving a copy of an electricity or phone bill).
20. Companies must develop customers’ acceptance policies in order to determine the applicants who seems money launderers and terrorism financiers. Those aspects must be summarized in the risks document relevant to the applicants/customers.

Companies must introduce the following components at least in the risks document relevant to the customers:

a) The nature of the insurance document or documents.

b) Repetition and volume of activities.

c) The customer’s background (such as the place of birth, working place, etc.).

d) Customer’s file.

e) Working nature of the customer.

f) Complexity of the ownership structure of customers and legal beneficiaries.

g) Payment ways used by the customer.

h) The funds source and the income of the customer.

i) Determine the beneficiaries of the applications, whether it is the customer himself or a third party.

21. The Company must develop customers’ acceptance policies and measures in order to determine the type of the customer who might face more than medium risks relevant to anti-money laundering and counterterrorist finance measures. It must develop comprehensive and detailed policies and measures relevant to customer due diligence towards high risks customer, including the development of clear internal policies to approve the working relation with this customer.

22. The Company must update data that are received according to customer due
diligence measures towards the customer
to make sure of their accuracy and safety.
It must perform a periodic review or a
review according to the need for actual
records, especially customers or high risk
working relations records, when cases
requiring the update of those pieces of
information happen, such as:
• Application made by an actual
customer to build a new relation or
introduce a radical change on the
nature of the actual relation.
• The existence of unusual activities or
contradictory to the usual dealing
mode of the customer according to the
available information in the company.
• When the Company is not convinced
about the existence of sufficient
information on the customer, or when
it doubts about the relevance of data
previously received from the customer.

Operations Control

23. Companies must apply developed
measures that allow the most possible
efforts to inquire about the customer and
evaluate the risks level, in addition to the
measures stipulated in article 16 of the
Rules, in the following cases:

a) Working relations and indirect
operations (clarified in article 28 of the
Rules).

b) High risk categories of applicants,
working relations, or operations
(clarified in articles 60, 61, and 62 of
the Rules).

24. If applicants are legal personalities or are
unified by a formal agreement, companies
must take all necessary measures to:

- Review according to the need for actual

- Companies must apply developed
measures that allow the most possible
efforts to inquire about the customer and
evaluate the risks level, in addition to the
measures stipulated in article 16 of the
Rules, in the following cases:

- Working relations and indirect
operations (clarified in article 28 of the
Rules).

- High risk categories of applicants,
working relations, or operations
(clarified in articles 60, 61, and 62 of
the Rules).

- If applicants are legal personalities or are
unified by a formal agreement, companies
must take all necessary measures to:
a) Make sure that any person who intends to act on behalf of the applicant is charged to do so.

b) Know the ownership and responsibility structure of the applicants.

c) Determine natural personalities who fully own or dominate the applicant.

This inquiry must take place before or during the dealing period or during the period of activity of informal customers.

25. The Company must inquire about the identity of the customer, the possible customer, and the actual beneficiary before and during the working relation. Companies which are unable to make the maximum possible effort to inquire about the customers must not perform the required operations by the customer at the beginning of the relation. In such case, the Company must study the need to notify the Financial Intelligence Unit. The Company must not start dealing with any customers before completing all determination measures and inquiring about the customer.

26. To determine whether the customer is of high risks category, companies must develop monthly or quarterly reports which include a list of insurance activities and stress on the following:

a) Customer’s data and huge amounts of money

b) Amounts of money less than the minimum which requires the maximum possible effort to inquire and investigate about the customer to combat money laundering and terrorist finance

c) Payment way and usage of unusual payment ways

This should be done individually for each customer.

1) The customer must not perform the required operations by the customer at the maximum possible effort to inquire about the customer, and the actual beneficiary.

2) The customer must not perform the required operations by the customer at the maximum possible effort to inquire about the customer, and the actual beneficiary.

Insurance Supervision Department

لنا، [Bank Name]

This inquiry must take place before or during the dealing period or during the period of activity of informal customers.

25. The Company must inquire about the identity of the customer, the possible customer, and the actual beneficiary before and during the working relation. Companies which are unable to make the maximum possible effort to inquire about the customers must not perform the required operations by the customer at the beginning of the relation. In such case, the Company must study the need to notify the Financial Intelligence Unit. The Company must not start dealing with any customers before completing all determination measures and inquiring about the customer.

26. To determine whether the customer is of high risks category, companies must develop monthly or quarterly reports which include a list of insurance activities and stress on the following:

a) Customer’s data and huge amounts of money

b) Amounts of money less than the minimum which requires the maximum possible effort to inquire and investigate about the customer to combat money laundering and terrorist finance

c) Payment way and usage of unusual payment ways

This should be done individually for each customer.

1) The customer must not perform the required operations by the customer at the maximum possible effort to inquire about the customer, and the actual beneficiary.

2) The customer must not perform the required operations by the customer at the maximum possible effort to inquire about the customer, and the actual beneficiary.

Insurance Supervision Department

This inquiry must take place before or during the dealing period or during the period of activity of informal customers.

25. The Company must inquire about the identity of the customer, the possible customer, and the actual beneficiary before and during the working relation. Companies which are unable to make the maximum possible effort to inquire about the customers must not perform the required operations by the customer at the beginning of the relation. In such case, the Company must study the need to notify the Financial Intelligence Unit. The Company must not start dealing with any customers before completing all determination measures and inquiring about the customer.

26. To determine whether the customer is of high risks category, companies must develop monthly or quarterly reports which include a list of insurance activities and stress on the following:

a) Customer’s data and huge amounts of money

b) Amounts of money less than the minimum which requires the maximum possible effort to inquire and investigate about the customer to combat money laundering and terrorist finance

c) Payment way and usage of unusual payment ways

This should be done individually for each customer.
25

د) عدد العمليات بالنسبة لكل عميل خلال الفترة المذكورة ودرجة التعقيد.

ه) أي زيادة ملحوظة في عدد العمليات.

و) العلة والمصارف المستخدمة، في حال توفرها.

يجب الاحتفاظ بهذه السجلات لفترة خمس سنوات على الأقل وتقديمها إلى المؤسسة ووحدة التحريات المالية والمحققين عند الطلب.

27. على الشركات استمرار القيام بأقصى جهد ممكن للتحقق من العميل طوال فترة علاقة العمل مع الشركة وليس عند إنشاء العلاقة فقط. ويبعد البعد في عملية التحقق من العميل عند:

أ) تغيير المستفيد.

ب) زيادة كبيرة في المبلغ المؤمن أو قسط التأمين.

ج) استخدام الفوائد الورقية و/أ دفع أقساط التأمين الكبيرة.

د) مدفوعات من قبل طرف ثالث.

ه) مدفوعات مجهولة الهوية من خلال أدوات مصرفية مختصرة.

و) تغيير عنوان سكن المؤمن له أو المستفيد.

ز) دفع مبالغ مقطوعة غير مبرزة لصالح وثائق التأمين على الحياة أو خطط التقاعد.

ح) طلب التحصيل المسبق للمنافع.

ط) استخدام الوثيقة كضمان (على سبيل المثال لا الحصر، في الرهن العقاري).

ي) إلغاء الوثيقة في وقت مبكر أو تغيير مدتها.

ك) تغيير في نوع المنفعة.

Those records must be kept for a minimum of five years and submitted to SAMA, FIU, and auditors when necessary.

Companies must continue making their maximum possible efforts to inquire about the customer during the whole working relation period, and not only at its beginning. Customer’s inquiring process should start when:

a) The beneficiary changes.

b) There is a big increase in the insured amount or insurance premium.

c) Paper and/or huge insurance payments are used.

d) A third party settles payments.

e) Anonymous payments are settled through specialized bank instruments.

f) The address of the insured or the beneficiary is changed.

g) Unjustified lump sums for life insurance or pension plans are settled.

h) A pre-benefits collection demand is formulated.

i) A policy contract is used as guarantee (example of real estate mortgage).

j) A policy contract is annulled at an early stage or when its period is changed.

k) The type of utility is changed.
l) There is no sufficient information about the insured or beneficiaries.

The company must update the data of all customers in a regular manner.

28. If the company counts on a third party to perform customer due diligence procedures, it has to take the following measures:

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

b) The company can count on a third party to apply the customer due diligence measures, provided that relevant standards are compliant. In all cases, the responsibility of inquiring about the customer’s identity remains on the company and not on the third party.

c) The company can count on a third party to perform customer due diligence measures in the following cases only:

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

d) Before relying on a third party, the company have to make sure about its relevance regarding the application of customer due diligence procedures, as well as its ability to apply those

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

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

Before relying on a third party, the company have to make sure about its relevance regarding the application of customer due diligence procedures, as well as its ability to apply those
measures at the same level adopted by the company towards its customers. The company must develop clear policies to determine if the third party has an acceptable level to be relied on.

e) When relying on a third party, the company must do the following:

- Receive copies of documents and information relevant to customer due diligence measures of the third party.
- 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.
- 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.

f) 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.

g) The company must not rely 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.

Anti-money laundering and terrorist financing internal policies

Organisational structure and determination of responsibilities

29. As part of anti-money laundering and counterterrorist finance program, comprehensive anti-money laundering and counterterrorist finance policies and measures must be available for all employees on the different levels of the company (example: company's internal network). They must include customer due diligence procedures, records keeping, and notification about suspicious and unusual transactions.

30. The Company’s board is responsible for supervising the conception and adoption of the anti-money laundering and counterterrorist finance program, as well as the compliance officer. Below are some responsibilities:

a) Insure 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.
b) Promote internal and external anti-money laundering and counterterrorist finance measures and standards.

31. Companies must set the appropriate internal control measures to guarantee a continuous respect of those rules. The internal audit and/or inspection department at the company must review the effectiveness of the anti-money laundering and counterterrorist finance program in order to evaluate the compliance of applied measures and recommend the update of standards to comply with the development of anti-money laundering and counterterrorist finance ways and techniques. This review must be annually performed; its results must be submitted to the Board.

32. Companies must create an internal inspection team to determine, prevent and combat money laundering and terrorist finance. As for companies having less than 50 employees, the internal inspection team can be within the audit department or the internal inspection one. The internal inspection team must cooperate closely with compliance officer.

33. Internal inspection team and compliance officer responsibilities include the following:

a) Develop, preserve, and implement anti-money laundering and counterterrorist finance policies and measures, which are an integral part of the anti-money laundering and counterterrorist finance program.

b) Receive and follow-up reports relevant to any suspicious activities relative to money laundering and terrorist finance notified by the company’s employees, its agents or brokers.
c) Collaborate and follow-up replies relevant to activities which were detected as suspicious money laundering and terrorist finance activities, including:
   - Cooperation with Saudi FIU in order to determine and sanction suspicious party(ies).
   - Guarantee a regulatory protection of notifying parties when needed.
   - التسليق وقائمة الزود المتعلقة بأعمال تم التأكيد من أنها عمليات مشبوهة لغسل الأموال وتمويل الإرهاب، بما في ذلك:
   - التعاون مع وحدة التحريات المالية السعودية من أجل تحديد المشتبه به (أو)
   - المشتبه به وفرض العقوبات.
   - ضمان حصول المبلغين على حماية نظامية عند الحاجة.

d) Keep a 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).

e) Have access at the appropriate time and every time to customers' determination data and other information relevant to obligatory inquiry about customers, operations record, and other relevant pieces of information.

f) Test the extent of commitment relative to measures, policies, and internal restrictions in the field of combating money laundering and terrorist finance.

g) Continuously follow-up all what is new in anti-money laundering and counterterrorist finance regulations, techniques, and practices; and update anti-money laundering and counterterrorist finance indicators.

h) Develop continuous training plans for all employees with regard to anti-money laundering and counterterrorist finance measures.
Screening and training Employees

34. 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.

35. Companies must determine the main positions that might be targeted for money laundering and terrorist finance purposes. Employees who fulfil such positions must be closely controlled in order to guarantee their credibility as well as their continuous application of anti-money laundering and counterterrorist finance policies and measures.

36. Companies must educate and train its employees, managers, and Board members on combating money laundering and terrorist finance, as well as on anti-money laundering and counterterrorist finance rules and regulations, especially customer due diligence procedures, tracking, detecting and notifying about suspicious transactions.

Training framework must comply with the roles and responsibilities of the employees. Newly recruited employees must receive a basic training, and must receive a developed training at a later stage according to their job descriptions at least. The following training types must be provided:

a) New employees: Comprehensive background on money laundering and terrorist finance.

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

الفحص وتدريب الكوادر البشرية

34. على الشركات التأكد أن الأشخاص الذين سوف يوظفون فيها قد تم فحصهم من ناحية الخبرة والنزاهة والاستقامة والمهارات والقدرات. بالإضافة إلى ذلك، يجب التحقق من الهوية والبيانات الشخصية والسيرة الذاتية.

35. على الشركات تحديد المناصب الرئيسية التي قد تستهدف لأغراض غسل الأموال وتمويل الإرهاب. ويجب مراقبة الموظفين الذين يشغلون هذه المناصب عن كثب من أجل ضمان استقامتهم وتطبيقهم المستمر لسياسات وإجراءات مكافحة غسل الأموال وتمويل الإرهاب.

36. على الشركات تقييم وتدريب موظفيها ومداراتها وأعضاء مجلس إدارتها على مكافحة غسل الأموال وتمويل الإرهاب والأنظمة واللوائح الخاصة بمكافحة غسل الأموال وتمويل الإرهاب. ولاسيما إجراءات الالتباس الواجبة تجاه العميل وتقبع وكشف العمليات المشتبه فيها والإبلاغ عنها.

ويجب أن يكون نطاق التدريب متوافقًا مع دور الموظفين ومسؤولياتهم. كما يجب توفير التدريب الأساسي عند توظيف أي موظف جديد وتأمين تدريب متطور لهم في مرحلة تالية وفقًا للوصف الوظيفي الخاص بهم على الأقل، يجب توفير أنواع التدريب الاتجاهية للموظفي الشركة:

أ) الموظفون الجدد: خلفية شاملة عن غسل الأموال وتمويل الإرهاب.

ب) موظفو المبيعات والاستشارات:
   • القيام بأقصى جهد ممكن للتحقق من العميل (عرف عمليك) ومؤشرات غسل
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.

37. It is necessary to update training programs and hold sessions at least once a year, to update employees on the last developments and techniques used by money launderers.

Compliance procedures

38. Companies must designate a compliance manager, whose mission is to inquire and supervise the issues of compliance inside the company. The role of the compliance manager consists of determining and notifying about suspicious transactions and ensuring continuous follow-up of the company's compliance with anti-money laundering and counterterrorist finance policies, measures, and restrictions. The company's board as well as SAMA must be notified of any behaviour which does not comply with the laws and regulations.
not comply with the company's anti-money laundering and counterterrorist finance policies and measures.

39. Compliance manager must review the reports relevant to huge or unusual transactions (as per article 26 of the Rules), in addition to special reports prepared by customer services employees. Compliance manager must also keep a record which includes all internal reports relevant to anti-money laundering and counterterrorist finance measures. He has a full authority to access to customers' determination data and other pieces of information relevant to customer due diligence procedures, operations records, and any other relevant piece of information. Compliance manager must guarantee that all relevant details about suspicious transactions are submitted to FIU and SAMA. He must also fully cooperate with them in investigation cases.

Detection and notification about suspicious transactions

40. According to anti-money laundering rules and regulations, the company 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. The company must submit a copy of the notification to its insurance control department.

سياسات وإجراءات مكافحة غسل الأموال وتمويل الإرهاب التابعة للشركة يجب أن يبلغ إلى مجلس الإدارة والمؤسسة.

39. على مدير الإلتزام مراجعة التقارير المتعلق بالعمليات الكبيرة أو غير العادية (كما ورد في المادة 26 من هذه القواعد) فضلاً عن التقارير الخاصة التي يدعو موظفو علاقات العملاء. كذلك على مدير الإلتزام، الاحتفاظ بسجل يتضمن كافة التقارير الداخلية المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب. ولمدير الإلتزام صلاحية كاملة للوصول إلى بيانات تحديد القيادة والمعلومات الأخرى التي تتعلق بالتحقيق الواجب من العملاء وسجلات الأعمال وأي معلومات ذات الصلة. وعلى مدير الإلتزام ضمان أن كافة التفاصيل ذات الصلة والمتعلقة بالعمليات المشبوهة تُحال إلى وحدة التحريات المالية وكذلك إلى مؤسسة النقد. كما عليه أن يتعاون بالكامل مع هاتين الجهاتين عند التحقيق.

الكشف والإبلاغ عن العمليات المشبوهة

40. وفقًا للالتزامات المنصوص عليها في نظام مكافحة غسل الأموال ولائحته التنفيذية، يجب على الشركة إبلاغ وحدة التحريات المالية فوراً عن أي نشاط أو عملية أو صفقة معتادة أو ضمحة غير طبيعية أو عملية تثير الشكوك والشبهات حول ماهيتها والغرض منها، أو أي نشاط أو عملية لها علاقة أو يشيّه أن لها علاقة بشاشط إجرامي أو تمويل عمليات إرهابية أو تمويل إرهابيين أو منظمات إرهابية وتقديم نسخة من البلاغ إلى إدارة مراقبة التأمين بالمؤسسة.
41. The Company must submit a detailed report including all data and information about suspicious transactions and relevant parties to FIU, 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
- Doubt indicators and justifications with all supporting documents

42. 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.

43. The Company must ask all its employees to immediately submit 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 notification official who could submit a notification to FIU. The money laundering and terrorist finance notification must be a competent person who has a practical experience in combating money laundering and terrorist finance.

44. The money laundering and terrorist finance notification official is responsible for executing measures of notification

41. يجب على الشركة تقديم تقرير مفصل يتضمن جميع البيانات والمعلومات عن العمليات المشتبهة فيها والأطراف ذات الصلة إلى وحدة التحريات المالية خلال عشرة أيام تقويمية من تاريخ الإبلاغ، وأن يتضمن التقرير حداً أدنى الآتي:
- الوثائق الخاصة بالعملية التأمينية.
- نسخ من جميع المستندات والوثائق المطلوبة عند إقامة علاقة العمل.
- أي بيانات تتعلق بطبعة العمليات المبلغ عنها.
- مؤشرات ومسببات الشك مع جميع المستندات المؤيدة لها.

42. يجب الإبلاغ عن العمليات المشتبهة فيها بغض النظر عن تعلقها بقضايا أخرى. وإذا سبق تقديم تقرير إلى وحدة التحريات المالية يتعلق بعمليات مشتبهة فيها قام بها العمل إذا ذلك لا يمنع من تقديم تقرير جديد دون تأخير عند ظهور حالة اشتباه جديدة.

43. على الشركة إصدار تعليمات لجميع موظفيها بالحالة الفورية لأي عملية معقدة أو ضخمة أو غير طبيعية أو عملية تثير الشكوك والشبهات أو أي عملية لها علاقة أو يشتبه أن لها علاقة بنشاط إجرامي أو تمويل عمليات إرهابية أو تمويل الإرهابيين أو منظمات إرهابية إلى مسئول الإبلاغ عن غسل الأموال وتمويل الإرهاب الذي قد يرى إعداد بلاغ بشأنها لوحدة التحريات المالية. ويجب أن يكون مسئول الإبلاغ عن غسل الأموال شخصاً مؤهلاً ولديه خبرة عملية في مكافحة غسل الأموال وتمويل الإرهاب.

44. يكون مسئول الإبلاغ عن غسل الأموال وتمويل الإرهاب لدى الشركة هو المعني بتنفيذ إجراءات
submitted to FIU. He must regularly and effectively determine and notify about suspicious transactions, and review reports relevant to huge or unusual activities resulting from the company’s bylaws, or any case notified by any employee.

45. If any employee notifies the notification official about a money laundering and terrorist finance activity, the later must review the case conditions to determine the suspicion justifications. If the money laundering and terrorist finance notification official decides not to notify FIU, he must document the reasons in details.

46. The Company must keep a record of all reports submitted to the money laundering and terrorist finance notification official, with every internal remarks and every analysis of the operations. It must also keep a record including all notifications submitted to FIU, and all reports developed by employees, including notifications and reports which the money laundering and terrorist finance notification official decided not to submit to FIU.

47. The Company must use the FIU notification sample, in annex number (2), and should 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 notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.

The notification official decides not to notify laundering and terrorist finance activities resulting from the company’s bylaws, or any case notified by any employee.

In case of notification over the phone, it must confirm it by sending a written notification within no more than 24 hours.
48. The Company must confirm FIU receipt of any notification about a suspicious transaction. If no reply is sent by FIU about a suspicious transaction, the company must continue its control over the operation and the customer, studying the possibility of sending another notification.

49. Annex number (1) includes a list of the most important indicators showing unusual or suspicious transactions or activities that might need audit. This list does not include all indicators; therefore, the company must control any unusual or suspicious activities, whether their type is clarified in annex number (1) or not. The presence of one clarifying factor in the list means more control, but does not necessarily mean that the operation is suspicious.

50. When FIU asks additional pieces of information from any company in order to follow-up a suspicious transactions notification, this must go through SAMA, being the authority concerned with asking such information from the company, following-up its receipt, and submitting it to FIU.

51. 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.

52. According to article 25 of anti-money laundering and terrorist financing Law, board members, officials, and employees (permanent and interim) are exempted from any criminal, civil, and administrative responsibility resulting from a contravention consisting of disclosing restricted information as per a contract or text set by a legal, regulatory, or administrative authority, in case FIU is notified with good intention about unusual or suspicious transactions or activities. They also benefit from this protection even if they are not fully aware about the nature of the suspicious activity, whether the illegal activity took place or not.

53. Companies must attach a particular attention 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 which necessitates the application of the measures stipulated in article (61) of the rules.

وبخلافًا للنظام، وفي حال تم إرسال البلاغ إلى وحدة التحريات المالية، وجب على الشركة توخي الحرص الناتم لضمان عدم علم العميل بإرسال البلاغ ومواصلة تعاملها مع العميل بالشكل المعتاد حتى وعود تعليمات من إدارة مراقبة التأمين في المؤسسة.

52. بناءً على المادة (الخامسة والعشرين) من نظام مكافحة غسل الأموال يعفي أعضاء مجلس إدارة الشركة ومسؤولوها وموظفوها (الدائنين والموقتين) من المسؤولية الجنائية والمدنية والإدارية الموجهة إلى مخالفة أي قيد على الإفصاح عن المعلومات يفرضه عقد أو نص من أي جهة تشريعية أو تنظيمية أو إدارية في حال إبلاغهم وحدة التحريات المالية بحسن نية عن عمليات أو أنشطة غير عادلة أو مشتبه فيها. وتتوفر لهم هذه الحماية حتى في حال علمهم بشكل دقيق عن طبيعة النشاط المشتبه فيه سواء وقع النشاط غير النظامي أم لم يقع.

53. على الشركات إبداء اهتمام خاص بالعلاقات والعمليات التجارية مع الشركات والأفراد بما في ذلك المستفيدين الذين يعملون داخل أو من خلال بلدان لا تطبق تعويضات مجموعة العمل المالي (FATF) أو تطبق بطريقة غير كافية. إذا تبين وجود معاملة ليس لها أي هدف اقتصادي أو نظمي واضح، يجب التحقق من خلفيتها وترؤد وحدة التحريات المالية بناءً على التحقق خطياً. وإذا أبلغت المؤسسة الشركة أن تلك الدولة لا تطبق بشكل كاف تعويضات مجموعة العمل المالي، فإن على الشركة أن تعد جميع علاقات العمل والعمليات الصادرة عن تلك الدول من قنوات المخاطر المالية التي تستوجب تطبيق الإجراءات
54. The Company must have a clear idea about the persons included in the UN terrorism list. Therefore, the company has to make sure of the following:

a) The implementation of effective measures to immediately determine the identity of a customer (s), including real beneficiaries of persons included on terrorism lists published by the UN commission established as per UNSCR 1267 ("1267 Commission") and other relevant resolutions.

b) If the company determines a customer or a possible customer, whose name is included on the UN terrorism list, or if a party of an activity is included in this list, it must immediately notify FIU and send a copy of the notification to SAMA. According to anti-money laundering Law and regulations, it must seize any funds of any person whose name is included on the terrorism list, and the company has to keep his due payments seized until receiving instructions from SAMA.

c) Before building a working relation, the Company must make sure of the possible customer's name and should compare it with those included in UNSC terrorism list. It should daily update its list by daily checking the UNSC website, and compare it with the list of all its customers (www.un.org).
Records keeping

55. Companies must keep documents for ten years or more, as of the end date of the activity or the working relation with insured parties, real beneficiaries, and data collected by the customer due diligence procedures, provided that the documents include paper or electronic copies of the following:

a) The contacts or contracts or any amendments on the contract (if available).

b) Adopted determination documents (for those insured and beneficiaries).

c) Essential correspondence documents with the customer.

The contacts or contracts or any amendments on the contract (if available).

(www.un.org)

If the competent authority in the Kingdom decided to seize the funds of any person according to UNSCR 1373 or any other resolution, SAMA is the relevant institution which notifies all companies about that. Companies must immediately cease insurance operations and products of this person.

e) In case seizure on the funds of a certain customer is lifted, after removing his name from terrorism list, or after discovering that his name was mistakenly included, or according to a decision of the competent authority ordering the lifting of his funds for legal or humanitarian reasons, SAMA will notify the companies about that.

On the dates and the end date of the activity or the working relation with insured parties, real beneficiaries, the following documents:

55. Companies must keep documents for ten years or more, as of the end date of the activity or the working relation with insured parties, real beneficiaries, and data collected by the customer due diligence procedures, provided that the documents include paper or electronic copies of the following:

a) The contacts or contracts or any amendments on the contract (if available).

b) Adopted determination documents (for those insured and beneficiaries).

c) Essential correspondence documents with the customer.

(www.un.org)

If the competent authority in the Kingdom decided to seize the funds of any person according to UNSCR 1373 or any other resolution, SAMA is the relevant institution which notifies all companies about that. Companies must immediately cease insurance operations and products of this person.

e) In case seizure on the funds of a certain customer is lifted, after removing his name from terrorism list, or after discovering that his name was mistakenly included, or according to a decision of the competent authority ordering the lifting of his funds for legal or humanitarian reasons, SAMA will notify the companies about that.

On the dates and the end date of the activity or the working relation with insured parties, real beneficiaries, the following documents:

55. Companies must keep documents for ten years or more, as of the end date of the activity or the working relation with insured parties, real beneficiaries, and data collected by the customer due diligence procedures, provided that the documents include paper or electronic copies of the following:

a) The contacts or contracts or any amendments on the contract (if available).

b) Adopted determination documents (for those insured and beneficiaries).

c) Essential correspondence documents with the customer.

55. Companies must keep documents for ten years or more, as of the end date of the activity or the working relation with insured parties, real beneficiaries, and data collected by the customer due diligence procedures, provided that the documents include paper or electronic copies of the following:
d) Operations record.

e) Any piece of information relevant to customer due diligence procedures.

f) Dealing details, including the volume of flowing funds.

g) Activity funds sources, insurance operation funding ways, benefiting ways, and the identity of applicants.

h) Any other relevant document.

In case an investigation was launched concerning the customer’s records and his relations, or in case he was the subject of a suspicious transactions report, or in case a demand was submitted by a competent authority, the company must keep the records and information until the end of the case, even if it takes ten years.

56. Companies must keep appropriate records for all local and international operations, for a ten year period, to confirm its commitment to the rules, such as detection and prevention against money laundering measures.

57. Companies should make sure that appropriate measures to support records management, maintenance, and archiving are adopted. Access to records should be limited to competent employees.

58. Companies must provide SAMA and FIU with all records and information at the appropriate time.

59. The Company should keep sufficient records allowing the restructuring of any insurance transaction, in order to provide justifying proves on the criminal activity.
to take legal action, if necessary.

Customers' categories and risks level assessment

High risks customers

60. Are considered as high risks cases:

a) Any complex legal arrangements having no clear regulatory or economic purpose.

b) Any person (companies and enterprises) from or in any country that does not or partially apply FATF's recommendations, such as the country or the countries specified by FATF as non compliant countries.

c) High risks political persons due to their positions.

d) Non-profitable organizations.

61. The Company must develop policies, procedures, and internal restrictions for obligatory care measures towards any high risks customer. What follows are some measures that should be taken into consideration:

a) Receive a written statement from the real beneficiaries about managers' identities and main contributors, and the relation with them.

b) 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.

c) 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.

d) Hold direct interviews with customer's higher management in a regular manner throughout the relation with him.
e) Have the approbation of the company at the beginning of the working relation.

62. The customer categorized in one of the risks levels must be considered as "high risks" customer, with the possibility of amending the categorization to a less level of risks, if the situation of the customer is acceptable, the amendment is suggested by the responsible person, and was approved by the higher management of the company. In case a customer was categorized as "high risks" customer, but the company sees that it is necessary to keep the relation, it should lift the customer due diligence procedures and put him under permanent control, and review the level of risks on a yearly basis, and after having the approbation of the higher management.

Political customers

63. Concerning the dealings with political personalities, companies should make the maximum possible effort regrading customer due diligence procedures, and should also:

a) Develop risks management systems to know if the customer is a political personality.
b) Have the company's higher management approbation before launching a working relation of this kind with the customers.
c) Take logical measures to determine the source of revenue as well as the source of funds.

The customer categorized in one of the risks levels must be considered as "high risks" customer, with the possibility of amending the categorization to a less level of risks, if the situation of the customer is acceptable, the amendment is suggested by the responsible person, and was approved by the higher management of the company. In case a customer was categorized as "high risks" customer, but the company sees that it is necessary to keep the relation, it should lift the customer due diligence procedures and put him under permanent control, and review the level of risks on a yearly basis, and after having the approbation of the higher management.

Political customers

63. Concerning the dealings with political personalities, companies should make the maximum possible effort regrading customer due diligence procedures, and should also:

a) Develop risks management systems to know if the customer is a political personality.
b) Have the company's higher management approbation before launching a working relation of this kind with the customers.
c) Take logical measures to determine the source of revenue as well as the source of funds.

The customer categorized in one of the risks levels must be considered as "high risks" customer, with the possibility of amending the categorization to a less level of risks, if the situation of the customer is acceptable, the amendment is suggested by the responsible person, and was approved by the higher management of the company. In case a customer was categorized as "high risks" customer, but the company sees that it is necessary to keep the relation, it should lift the customer due diligence procedures and put him under permanent control, and review the level of risks on a yearly basis, and after having the approbation of the higher management.

Political customers

63. Concerning the dealings with political personalities, companies should make the maximum possible effort regrading customer due diligence procedures, and should also:

a) Develop risks management systems to know if the customer is a political personality.
b) Have the company's higher management approbation before launching a working relation of this kind with the customers.
c) Take logical measures to determine the source of revenue as well as the source of funds.

The customer categorized in one of the risks levels must be considered as "high risks" customer, with the possibility of amending the categorization to a less level of risks, if the situation of the customer is acceptable, the amendment is suggested by the responsible person, and was approved by the higher management of the company. In case a customer was categorized as "high risks" customer, but the company sees that it is necessary to keep the relation, it should lift the customer due diligence procedures and put him under permanent control, and review the level of risks on a yearly basis, and after having the approbation of the higher management.

Political customers

63. Concerning the dealings with political personalities, companies should make the maximum possible effort regrading customer due diligence procedures, and should also:

a) Develop risks management systems to know if the customer is a political personality.
b) Have the company's higher management approbation before launching a working relation of this kind with the customers.
c) Take logical measures to determine the source of revenue as well as the source of funds.
d) Control the working relation in continuous manner.

e) Ask more documents in addition to customer's identification process.

f) Ask the ratification of documents by competent authorities.

Non-profitable organizations

64. The Company must develop policies, procedures, and internal restrictions to guarantee the commitment to SAMA requirements, with regard to building a working relation, providing insurance services and products to non-profitable organizations. When tackling any operation for such organizations, the following requirements should be taken into consideration:

a) Having an official license from a specialized governmental body defining its purposes and activities.

b) Such bodies and organizations should be categorized as high risks customers, and obligatory care measures shall be lifted when dealing with them.

Policies and procedures relative to the company's activities outside the Kingdom

65. The Company 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) The company should attach a special attention to the application of paragraph (one) of this article on its...
branches and subsidiaries in countries which do not apply or insufficiently apply the FATF's recommendations, including those considered as non compliant countries.

c) In case there is any difference between anti-money laundering and counterterrorist finance requirements in the Kingdom with hosting countries of the company's branches or subsidiaries, the company 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, headquarters must notify SAMA about that and abide by any instructions that might be issued in this regard.

d) 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, the company should immediately notify SAMA.

66. When evaluating a country's application of FATF's anti-money laundering and counterterrorism standards, the company must do the following:

a) Evaluate the requirements applied to combat money laundering and terrorist finance. The company can benefit from available information and data on the concerned country from

وشركاتها التابعة لها الواقعة في دول لا تطبق أو لا تطبق بشكل كافٍ توصيات مجموعة العمل المالي، بما في ذلك الدول المحددة من مجموعة العمل المالي على أنها دول لا تطبق تلك التوصيات.

ج) في حال وجود أي اختلاف بين متطلبات مكافحة غسل الأموال وتمويل الإرهاب المطبقة في المملكة مع الدول المضيفة لفروع الشركة أو شركاتها التابعة لها يجب على الشركة تطبيق أفضل المتطلبات على فروعها أو شركاتها التابعة لها إلى الحد الذي تسمح به قوانين وأنظمة الدولة المضيفة. وفي حالة تعارض قوانين الدولة المضيفة مع الأنظمة واللوائح والقواعد الصادرة في المملكة كأن يكون الفرع أو الشركة التابعة لها غير قادرة على الالتزام بالتعليمات، يجب على المقر الرئيسي للشركة إبلاغ المؤسسة بذلك والالتزام بأي توجيهات أخرى تصدر لها في هذا الشأن.

د) إذا لم يتمكن الفرع الخارجي أو الشركة التابعة من الالتزام لأفضل المتطلبات نحو مكافحة غسل الأموال وتمويل الإرهاب لأن قوانين وأنظمة الدولة المضيفة لا تسمح بذلك أو لأي سبب آخر، وجب عليها تلبية المؤسسة بذلك فوراً.

16. يجب على الشركة عند تقييم تطبيق دولة لمعايير مجموعة العمل المالي الخاصة بتمكّن غسل الأموال وتمويل الإرهاب، القيم بالأتي:

ا) تقييم المتطلبات المطبقة لمكافحة غسل الأموال وتمويل الإرهاب، ونمكن للشركة الاستفادة من المعلومات والبيانات المتوافرة

---

44
stakeholders. Customer due diligence procedures when building a relation with customer in the concerned country is higher whenever risks are high.

b) Attach a special attention to reports evaluating the level of commitment of the concerned country to FATF's recommendations, developed by FATF, annexed regional task forces, IMF, or World Bank.

c) 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 its customers work.

Regulatory sanctions

67. Non-complying with the requirements stipulated in these rules contradicts Insurance Implementing Regulations, Anti-Money Laundering Law and Regulations, as well as licensing conditions, and might expose the company to the regulatory sanctions stipulated in the Law of Supervision of Cooperative Insurance Companies and its Implementing Regulations, and in Anti-Money Laundering Law and Regulations.

العقوبات النظامية

67. يعتبر عدم الالتزام بالمتطلبات المنصوص عليها في هذه القواعد مخالفة لنظام مراقبة شركات التأمين التعاونية ولاحتها التنفيذية ونظام مكافحة غسل الأموال و لاحتها التنفيذية وشروط التصريح ويمكن أن يُعرض الشركة للعقوبات النظامية المنصوص عليها في نظام مراقبة شركات التأمين التعاوني ونظام مكافحة غسل الأموال.
<table>
<thead>
<tr>
<th>Annex 1: Typical Insurance Money Laundering and Terrorism Financing Indicators</th>
<th>الملحق 1: مؤشرات تموذجية على غسل الاموال وتمويل الإرهاب في مجال التأمين</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Indicators</strong></td>
<td><strong>مؤشرات عامة</strong></td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td>• Insurance Party(^1) delays the provision or is reluctant to provide information to enable verification to be completed</td>
</tr>
<tr>
<td></td>
<td>• تأخر طرف التأمين أو ترده في إعطاء المعلومات من أجل السماح بإنهاء التحقق من العميل</td>
</tr>
<tr>
<td><strong>Jurisdiction</strong></td>
<td>• Insurance party is introduced by an agent/intermediary operating in an unregulated or loosely regulated jurisdiction</td>
</tr>
<tr>
<td></td>
<td>• يُعرَف طرف التأمين من قبل وكيل/ وسيط يعمل في سوق غير منظم أو قليل التنظيم</td>
</tr>
<tr>
<td><strong>Payment</strong></td>
<td>• Insurance party pre-pays insurance premiums unprecedentedly</td>
</tr>
<tr>
<td></td>
<td>• يدفع طرف التأمين أقساط التأمين مسبقًا بشكل غير متوقع</td>
</tr>
<tr>
<td></td>
<td>• Large amounts of money are transferred through several non-resident accounts</td>
</tr>
<tr>
<td></td>
<td>• نقل مبالغ كبيرة من المال من خلال عدة حسابات لغير المقيمين</td>
</tr>
<tr>
<td></td>
<td>• Insurance party requests a large purchase of a lump sum contract when the party usually makes small, regular payments</td>
</tr>
<tr>
<td></td>
<td>• يطلب طرف التأمين شراء جزء كبير من عقد مبلغ مقطوع بينما عادةً يُقدَم الطرف دفعات صغيرة ومتتالية</td>
</tr>
<tr>
<td><strong>Beneficiary</strong></td>
<td>• Insurance party transfers the benefit of a product to an apparently unrelated third party</td>
</tr>
<tr>
<td></td>
<td>• يستبدل طرف التأمين المستفيد الأول بطرف ثالث ليس له صلة ظاهرة به</td>
</tr>
<tr>
<td></td>
<td>• Insurance party substitutes the ultimate beneficiary with an apparently unrelated third party</td>
</tr>
<tr>
<td></td>
<td>• يُغيّر طرف التأمين المستفيدين المخصصين من دون معرفة المؤمن أو موافقته</td>
</tr>
<tr>
<td></td>
<td>• Insurance party changes the designated beneficiaries without knowledge or consent of the insurer</td>
</tr>
<tr>
<td></td>
<td>• يغيّر طرف التأمين المستفيدين من خلال مجرد</td>
</tr>
<tr>
<td></td>
<td>• Insurance party changes beneficiaries simply by</td>
</tr>
</tbody>
</table>

---

\(^1\) Party: Any entity involved in insurance operation, i.e., applicants, clients, policyholders, etc...

* طرف التأمين: أي كيان له علاقة في عملية التأمين، أي المقدمين والعملاء و الؤمنين لهم... الخ
<table>
<thead>
<tr>
<th>Annex 1: Typical Insurance Money Laundering and Terrorism Financing Indicators</th>
<th>ظروف مالية متشابهة للشريحة المالية وتمويل الإرهاب في مجال التأمين</th>
</tr>
</thead>
<tbody>
<tr>
<td>signing an endorsement on the policy</td>
<td>توقيع ملحق على الوثيقة</td>
</tr>
<tr>
<td>• Insurance party terminates a product early at a loss, and the refund check goes to a third party</td>
<td>• ينهي طرف التأمين منتجًا في مرحلة مبكرة في حال حصول خسارة و يوجه شيك الاسترداد إلى طرف ثالث</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pre-Sale Indicators</th>
<th>مؤشرات ما قبل البيع</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct</td>
<td>السلوك</td>
</tr>
<tr>
<td>• Applicant shows no concern for the performance of the policy but much interest in the early cancellation of the contract</td>
<td>• لا يبدى المتقدم اهتمامًا بداء الوثيقة ولكن الإهتمام الأكبر يكون في إنهاء المبكر للعقد</td>
</tr>
<tr>
<td>• Applicant is reluctant to provide background information when applying for a policy</td>
<td>• يتردد المتقدم في تقديم المعلومات الأساسية عند تقديم طلب الوثيقة</td>
</tr>
<tr>
<td>• Applicant provides minimal or fictitious information</td>
<td>• يعطي المتقدم معلومات محدودة أو وهمية</td>
</tr>
<tr>
<td>• Applicant provides information that is difficult or expensive for the institution to verify</td>
<td>• يعطي المتقدم معلومات من الصعب أو من المكلف على شركة التأمين التحقق منها</td>
</tr>
<tr>
<td>• Applicant uses a mailing address outside the insurance supervisor’s jurisdiction</td>
<td>• يستخدم المتقدم عنواناً بريدياً خارج نطاق مشرفي التأمين</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment/Cash Value</th>
<th>الدفع/القيمة</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applicant attempts to use cash to complete a proposed transaction when other payment methods are normally used</td>
<td>• يحاول المتقدم استخدام النقد من أجل إتمام عملية غير مناسبة بتصريف الدفع الأخرى</td>
</tr>
<tr>
<td>• Applicant attempts to use a third party check to purchase a policy</td>
<td>• يحاول المتقدم استخدام شيكات ثالث من أجل شراء وثيقة</td>
</tr>
<tr>
<td>• Applicant requests to make a lump sum payment (instead of using installments) by wire transfer or with foreign currency</td>
<td>• يطلب المتقدم دفع مبلغ مقطوع (عوضًا عن استخدام الأقساط) عن طريق تحويل برقي أو بعملة أجنبية</td>
</tr>
<tr>
<td>• Applicant purchases policies in amounts considered</td>
<td>• يشتري المتقدم وثائق بمبالغ تعتبر أكبر من طاقته</td>
</tr>
</tbody>
</table>
### Annex 1: Typical Insurance Money Laundering and Terrorism Financing Indicators

<table>
<thead>
<tr>
<th>Conduct</th>
<th>Post-Sale Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applicant borrows the maximum cash value of a single premium policy soon after paying for the policy</td>
<td>• An apparent purpose is considered confidential.</td>
</tr>
<tr>
<td>• Applicant appears to have policies with several insurance companies</td>
<td>• An insurance product that has no apparent purpose.</td>
</tr>
<tr>
<td>• Applicant cancels a large insurance policy within a short time and requests the return of the cash value payable to a third party</td>
<td>• A customer requests an insurance product that has no apparent purpose.</td>
</tr>
</tbody>
</table>

### 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 a transaction that results in a conspicuous increase of insurance

### الملف 1: مؤشرات تموينية على غسل الأموال وتمويل الإرهاب في مجال التأمين

<table>
<thead>
<tr>
<th>الطاهرة</th>
<th>المؤشرات ما بعد البيع</th>
</tr>
</thead>
<tbody>
<tr>
<td>• يفترض المتقدم أهميّة قيمة نقديّة من قيّمة الوثيقة المدفوعة بضعت واحد بعد وقت وجيز من دفع ثمن الوثيقة</td>
<td>• تظهر أنّ المتقدم يملك وثائق مع عدد من شركات التأمين</td>
</tr>
<tr>
<td>• يлечّ المتقدم وثيقة تأمين كبيرة بعد وقت قصير ويطلب باسترداد القيمة النقدية الواجبة السداد إلى الطرف الثالث</td>
<td>• يقدّم العميل طلبًا للقيام بأعمال خارج إطار عمله الأساسي</td>
</tr>
<tr>
<td>• يقدّم العميل طلبًا للحصول على وثيقة في مكان بعيد كثيرة عن موقع سكنه الجغرافي حيث تتوفر وثائق مشابهة</td>
<td>• يطلب العميل منتجاً تأمينياً ليس له هدف واضح</td>
</tr>
<tr>
<td>• يقدّم العميل طلبًا للحصول على وثيقة في مكان بعيد كثيرة عن موقع سكنه الجغرافي حيث تتوفر وثائق مشابهة</td>
<td>• يتراجع أقساط وثائق التأمين للعمل على وثيقة في مكان بعيد كثيرة عن موقع سكنه الجغرافي حيث تتوفر وثائق مشابهة</td>
</tr>
<tr>
<td>• لا تتناسب قيم وثائق التأمين مع حاجات العميل التأمينية</td>
<td>• لا تتناسب قيم وثائق التأمين مع حاجات العميل التأمينية</td>
</tr>
</tbody>
</table>

---

Saudi Arabian Monetary Agency
Insurance Supervision Department

مؤسسة النقد العربي السعودي
إدارة مراقبة التأمين
<table>
<thead>
<tr>
<th>Annex 1: Typical Insurance Money Laundering and Terrorism Financing Indicators</th>
<th>الملحق ١: مؤشرات نموذجية على غسل الأموال وتمويل الإرهاب في مجال التأمين</th>
</tr>
</thead>
<tbody>
<tr>
<td>investment contributions</td>
<td>المساهمات الاستثمارية</td>
</tr>
<tr>
<td>• Customer conducts transaction involving an undisclosed party</td>
<td>• أن يجري العمليّة علیة مساعدة أطراف غير معلّنة</td>
</tr>
<tr>
<td></td>
<td>• أن يدفع العميل قسط التأمين الأول من حساب مصرف في خارج البلاد</td>
</tr>
<tr>
<td>• Customer pays his first premium from a bank account outside the country</td>
<td></td>
</tr>
</tbody>
</table>
### Annex 2: Suspicious Transaction Report Form

<table>
<thead>
<tr>
<th>الملحق ٢: نموذج البلاغات</th>
</tr>
</thead>
<tbody>
<tr>
<td>نموذج البلاغات باللغة العربية</td>
</tr>
</tbody>
</table>

**Suspicious Transaction Report Form in English**
نموذج البلاغات

للإبلاغ عن عملية مالية مشبوهة يجب تعبئة هذا
النموذج وإرساله إلى وحدة التحريات المالية على
العنوان التالي:
الرياض - طريق الملك فهد جنوب مبنى وزارة
الداخلية

فاكس: 0141776665 0141279866

للإبلاغ هاتفي الاتصال على مدار الساعة على الرقم
المجاني: 8001222224

لاستفسار الاتصال على الرقم: 13128100

(سري)

بلاغ عن عملية مالية مشبوهة

القسم أ - معلومات عن جهة البلاغ

القسم أ.1 - معلومات عن الشركة

<table>
<thead>
<tr>
<th>نوع الشركة</th>
<th>تأمين</th>
<th>إعادة تأمين</th>
<th>مهن حرة</th>
</tr>
</thead>
<tbody>
<tr>
<td>اسم الشركة</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>المدين</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>المدين</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

القسم أ.2 - معلومات عن المبلغ

<table>
<thead>
<tr>
<th>اسم</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>رقم الهاتف</td>
<td></td>
</tr>
<tr>
<td>العنوان</td>
<td></td>
</tr>
</tbody>
</table>
القسم ب – مضمون البلاغ

القسم 1 - معلومات عن وثيقة التامين

<table>
<thead>
<tr>
<th>نوع وثيقة التامين</th>
<th>رقم العلاقة التامينية</th>
</tr>
</thead>
<tbody>
<tr>
<td>مبلغ العملية</td>
<td>مدة الأقساط</td>
</tr>
<tr>
<td>طريقة الدفع</td>
<td>تاريخ إصدار وثيقة التامين</td>
</tr>
<tr>
<td>إلغاء وثيقة التامين</td>
<td>تاريخ الإلغاء</td>
</tr>
<tr>
<td>تسوية المطالبات</td>
<td>مقدار المبلغ الذي تم تسويته بالآرقام رياضي سعودي كتابة</td>
</tr>
</tbody>
</table>

القسم 2 - معلومات عن العملية المشبوهة

<table>
<thead>
<tr>
<th>تاريخ تنفيذ العملية</th>
<th>نوع العملية</th>
</tr>
</thead>
<tbody>
<tr>
<td>مقدار المبلغ</td>
<td>رقم</td>
</tr>
<tr>
<td>كتابة</td>
<td>نوع العملية</td>
</tr>
</tbody>
</table>

معلومات عن المؤمن له (المستفيد)

الاسم
مزود: 

رقم الهوية
الجنسية

معلومات عن منفذ العملية إذا كان مختلفًا عن المؤمن له:

الاسم
رقم الهوية
الجنسية

أسباب الالتباس:

المستندات المؤيدة:

على الجهة المبلغة أن ترفق مع البلاغ المستندات المؤيدة ذات الصلة بالعمليات التأمينية المشروعة بما فيها:

- أي مستند متعلق بعمليات الدفع (على سبيل المثال، الحصر، إيصال، شيكات، إرساليات، إلخ).
- بطاقة هوية المؤمن له.
- نسخة عن وثيقة التأمين.
سعادة مدير إدارة التحريات المالية

السلام عليكم ورحمة الله وبركاته:

تحدون أعلاه بلاغنا رقم تاريخ عن عملية مالية مشتته بها. أمل الإطلاع واتخاذ ما ترونه.

الوظيفة:

الختم الرسمي:
# Suspicious Transaction Report

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

## Section A - Reporting Party Information

### Section A.1 - Company Information

<table>
<thead>
<tr>
<th>Type of Company</th>
<th>Insurance</th>
<th>Reinsurance</th>
<th>Insurance Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head Quarter</td>
<td>City</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch Name</td>
<td>City</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Number</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Section A.2 - Informant Contact Information

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Number</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
</tbody>
</table>

(Confidential)

Reporting of a Suspicious Financial Transaction
### Section B - Report Content

#### Section B.1 - Policy Information

<table>
<thead>
<tr>
<th>Type or Class of Policy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number</td>
<td></td>
</tr>
<tr>
<td>Premium Amount</td>
<td></td>
</tr>
<tr>
<td>Payment Period</td>
<td></td>
</tr>
<tr>
<td>Payment Method</td>
<td></td>
</tr>
<tr>
<td>Policy Issuing Date</td>
<td>Day</td>
</tr>
<tr>
<td>Canceled?</td>
<td>Yes</td>
</tr>
<tr>
<td>Cancellation Date</td>
<td>Day</td>
</tr>
<tr>
<td>Claims Paid?</td>
<td>Yes</td>
</tr>
<tr>
<td>Claims Amount</td>
<td>In numbers SAR</td>
</tr>
</tbody>
</table>

#### Section B.2 - Suspicious Transaction Information

<table>
<thead>
<tr>
<th>Transaction Execution Date</th>
<th>Day</th>
<th>Month</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Amount</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Numbers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Letters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Currency Type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policyholder/ beneficiary Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID Number</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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: