بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

إدارة التفتيش البنكي — المركز الرئيسي

الرقم: ٩٢٠١/م ا ت/ ١٨١٤ — التاريخ: ٤ ربيع الثاني ١٤٣٣

المرفقات: دليل قواعد — "تعميم" — الموافق:

المحترم

سعادة/

البنك/

شركة/

الإدارة العامة/

بعد التحية:

الموضوع: قواعد مكافحة غسل الأموال وتمويل الإرهاب للبنوك ومحلات الصرافة وفروع البنوك الأجنبية العاملة في المملكة العربية السعودية (التحديث الثالث).

استناداً إلى نظام مؤسسة النقد العربي السعودي الصادر بموجب المرسوم الملكي الكريم رقم ٢٣ وتاريخ ١٣٧٧/٥/٢٣هـ وماورد في الفقرة (ج) من المادة الأولى والفقرة (د) من المادة الثالثة، وإلى نظام مراقبة البنوك الصادر بموجب المرسوم الملكي الكريم رقم م/٥ وتاريخ ١٣٨٦/٢/٢٢هـ وماورد في الفقرة (٣) من المادة السادسة عشر منه، وإلى قرار معالي وزير المالية رقم ٩٢٠/٣ وتاريخ ١٤٠٢/٢/١٦هـ بشأن تنظيم أعمال مهنة الصرافة، وقرار معالي وزير المالية رقم ٢١٤٩/٣ وتاريخ ١٤٠٦/١٠/١٤هـ بشأن قواعد تطبيق أحكام نظام مراقبة البنوك، وكون المؤسسة الجهة النظامية المعنية بالإشراف والرقابة على القطاع المصرفي في المملكة.

وإلحاقاً لتعميم المؤسسة رقم ٠٠٠٤٢/م أت/٨٢٩ وتاريخ ١٤٢٩/١٢/٢٩هـ المرافق به قواعد مكافحة غسل الأموال وتمويل الإرهاب التحديث الثاني، وتماشياً مع التطورات والمتطلبات الدولية في هذا المجال قامت المؤسسة بتحديث هذه القواعد وفق المستجدات، والواجب على البنوك ومحلات الصرافة وفروع البنوك الأجنبية العاملة في المملكة تطبيقها اضافة إلى تطبيق ما سبق أن صدر عن المؤسسة من أدلة وتعليمات ذات علاقة والعمل بموجبها وتضمينها في السياسات والإجراءات الداخلية إعتباراً من تاريخه. وفي هذا السياق تعتزم مؤسسة النقد العربي السعودي التحقق من تطبيق هذه القواعد من قبل البنوك ومحلات الصرافة وفروع البنوك الأجنبية العاملة في المملكة العربيّة السعودية وذلك من خلال عمليات التفتيش الميدانية التي تقوم بها المؤسسة ومن خلال تقارير وشهادات الالتزام المعدة من قبل مدققي حسابات خارجيين.

ص.ب ٢٩٩٢ الرياض ١١١٦٩ ، برقياً مركزي ، تلكس ٤٠٤٤٠٠ تلفون ٤٦٦٢٤٤٠ فاكس ٤٦٦٢٨٦٥

بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

إدارة التفتيش البنكي — المركز الرئيسي

الرقم: ..... / م أ ت / ..... التاريخ: .....

المرفقات: ..... الموافق: .....

نرفق لكم طيه نسخة من قواعد مكافحة غسل الأموال وتمويل الإرهاب للبنوك ومحلات الصرافة وفروع البنوك الأجنبية (التحديث الثالث). وآمل إفادة المؤسسة (إدارة التفتيش البنكي) حيال ما تم اتخاذه لتطبيق القواعد خلال ثلاثة أشهر من تاريخه.

وتقبلوا تحياتي،،،

فهد بن عبدالله المبارك

المحافظ

المعتمد

نطاق التوزيع:

- جميع البنوك العاملة بالمملكة.
- محلات الصرافة فئة (أ).
- إدارات المؤسسة.
- فروع المؤسسة.
- المعهد المصرفي.

المديفر

ص.ب ٢٩٩٢ الرياض ١١١٦٩ ، برقياً مركزي ، تلكس ٤٠٤٤٠٠ تلفون ٤٦٦٢٤٤٠ فاكس ٤٦٦٢٨٦٥

مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Agency

إدارة التفتيش البنكي
Banking Inspection Department

قواعد
مكافحة غسل الأموال وتمويل الإرهاب

للبنوك ومحلات الصرافة وفروع البنوك الاجنبية
العاملة بالمملكة العربية السعودية

التحديث الثالث
فبراير ٢٠١٢م

RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

For all banks and money exchangers and foreign banks' branches operating in the Kingdom of Saudi Arabia

Third Update
February 2012

قواعد مكافحة غسل الأموال وتمويل الإرهاب

RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

TABLE OF CONTENTS

Section	Content Description	Page No.
1	Introduction	5
1.1	Saudi Arabia Initiatives	5
1.1.1	International Level	5
1.1.2	Regional & Group Level	5
1.1.3	National Level	6
1.2	SAMA Initiatives	6
1.2.1	AML / CTF Regulations	6
1.2.2	Account Opening Regulations for Banks	7
1.2.3	Other Relevant Regulations	7
1.3	Objectives	8
1.4	General Developments & Trends	8
2	Legal Framework & Regulatory Requirements	8
2.1	The Saudi AML Law & Bylaws	8
2.2	SAMA - Regulatory & Supervisory Body	9
2.3	Domestic Banks & Money Exchangers & Foreign Banks' Branches Operating in the Kingdom	10
2.4	Overseas Branches & Subsidiaries of Saudi Bank & MEs	10
2.5	Legal Responsibilities Of Banks / MEs & Employees	10
2.6	Financial Intelligence Unit (FIU)	10
2.7	Cooperation Among Authorities & Banks/ MEs	11
2.7.1	Cooperation With Local Authorities	10
2.7.2	Cooperation Among Banks/ MEs Operating in the Kingdom	11
2.7.3	International Cooperation	12
3	Money Laundering & Terrorist Financing	12
3.1	Money Laundering	12
3.1.1	Definition of Money Laundering	12
3.1.2	Processes of Money Laundering	13
3.2	Terrorist Financing	13
3.2.1	Definition of Terrorist Financing	13
3.2.2	Processes of Terrorist Financing	14
3.3	Typologies	14

المحتويات

القسم	وصف المحتوى	رقم الصفحة
١	المقدّمة	٥
١,١	مبادرات المملكة العربية السعودية	٥
١,١,١	المستوى الدولي	٥
٢,١,١	المستوى الإقليمي	٥
٣,١,١	المستوى المحلي	٦
٢,١	مبادرات مؤسسة النقد العربي السعودي	٦
١,٢,١	قواعد مكافحة غسل الأموال وتمويل الإرهاب	٦
٢,٢,١	قواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها	٧
٣,٢,١	تعليمات أخرى ذات صلة	٧
٣,١	الأهداف	٨
٤,١	التطورات والاتجاهات العامّة	٨
٢	الإطارالنظامي والمتطلبات التنظيميّة	٨
١,٢	نظام مكافحة غسل الأموال في المملكة العربية السعودية	٨
٢,٢	مؤسسة النقد العربي السعودي – الجهة التنفيذية ولإشرافية	٩
٣,٢	البنوك المحلية ومحلات الصرافة وفروع البنوك الأجنبية العاملة في المملكة	١٠
٤,٢	الفروع والشركات التابعة للبنوك السعودية ومحلات الصرافة	١٠
٥,٢	المسؤولية القانونية على البنوك ومحلات الصرافة وموظفيها	١٠
٦,٢	وحدة التحريات المالية	١٠
٧,٢	التعاون بين السلطات والبنوك ومحلات الصرافة	١١
١,٧,٢	التعاون مع السلطات المحلّية	١١
٢,٧,٢	التعاون بين البنوك ومحلات الصرافة العاملة في المملكة	١١
٣,٧,٢	التعاون الدولي	١٢
٣	غسل الأموال وتمويل الإرهاب	١٢
١,٣	غسل الأموال	١٢
١,١,٣	تعريف غسل الأموال	١٢
٢,١,٣	عمليّات غسل الأموال	١٣
٢,٣	تمويل الإرهاب	١٣
١,٢,٣	تعريف تمويل الإرهاب	١٣
٢,٢,٣	عمليّات تمويل الإرهاب	١٤
٣,٣	الأنماط	١٤

4	Policies & Standards	16	١٦	السياسات والمعايير	٤
4.1	Risk-Based Approach	16	١٦	الأسلوب المرتكزعلى المخاطر	١,٤
4.1.1	Business Risk Assessment	17	١٧	تقييم مخاطر الأعمال	١,١,٤
4.2	AML/CTF Compliance Programs	18	١٨	برامج الالتزام الخاصة بمكافحة غسل الأموال وتمويل الإرهاب	٢,٤
4.3	Know Your Customer Standards	19	١٩	مبدأ "اعرف عميلك"	٣,٤
4.3.1	Customer Identification Process	20	٢٠	عمليّة تحديد هويّة العملاء	١,٣,٤
4.4	Customer Due Diligence (CDD)	21	٢١	العناية الواجبة للعملاء (CDD)	٤,٤
4.4.1	Beneficial Owners (Natural & Legal)	22	٢٢	المستفيدون الحقيقيون (الطبيعيون والإعتباريون)	١,٤,٤
4.4.2	Customer & Transaction Profiling	23	٢٣	ملفات معلومات العملاء والعمليات	٢,٤,٤
4.4.3	Name Checking of Designated Persons	24	٢٤	التحقق من أسماء الأشخاص المدرجين على القوائم	٣,٤,٤
4.5	Customer Risk Assessment	25	٢٥	تقييم مخاطر العميل	٥,٤
4.6	Customer Risks	25	٢٥	مخاطر العميل	٦,٤
4.6.1	Individual Personal Accounts	26	٢٦	الحسابات الشخصية الفردية	١,٦,٤
4.6.2	Private Banking Customers	27	٢٧	عملاء الحسابات الخاصّة	٢,٦,٤
4.6.3	Commercial Entities Accounts	28	٢٨	حسابات المنشآت التجاريّة	٣,٦,٤
4.6.4	Politically Exposed Persons	30	٣٠	الأشخاص المعرّفون سياسياً	٤,٦,٤
4.6.5	Walk-In Customers	30	٣٠	العملاء العارضون (العابرون)	٥,٦,٤
4.6.6	Charity & Non-Profit Organizations	31	٣١	الجمعيات والمنظمات الخيرية والجهات غير الهادفة للربح	٦,٦,٤
4.6.7	Trustees, Nominees & Intermediaries Accounts	32	٣٢	حسابات الأمناء، والموكّليين والوسطاء	٧,٦,٤
4.6.8	Insurance Companies Accounts	33	٣٣	حسابات شركات التأمين	٨,٦,٤
4.6.9	Introduced & Referred Businesses	34	٣٤	الأعمال المقدمة والمحاله من جهات أخرى	٩,٦,٤
4.6.10	Correspondent Banking Relationships	35	٣٥	علاقات البنوك المراسلة	١٠,٦,٤
4.7	Operations Monitoring	36	٣٦	مراقبة العمليات	٧,٤
4.7.1	Monitoring Process	36	٣٦	عمليّة المراقبة	١,٧,٤
4.7.2	Financial Investigation Process	38	٣٨	عمليّة التتبع المالي (التحقق)	٢,٧,٤
4.7.3	Transaction Monitoring Reinforcement	39	٣٩	تعزيز مراقبة العمليات	٣,٧,٤
4.8	Suspicious Transaction	39	٣٩	العمليات المشتبه بها	٨,٤
4.8.1	Reporting Suspicious Transactions	39	٣٩	الإبلاغ عن المعاملات المُشتبه بها	١,٨,٤
4.8.2	Reporting Requirements	40	٤٠	متطلّبات الإبلاغ	٢,٨,٤
4.8.3	Tipping Off	40	٤٠	التلميح وتنبيه العملاء	٣,٨,٤
4.8.4	Money Laundering Control Unit (MLCU)	41	٤١	وحدة مراقبة غسل الأموال	٤,٨,٤
4.9	Internal Controls	42	٤٢	الرقابة الداخليّة	٩,٤
4.9.1	Internal Control Procedures	42	٤٢	إجراءات الرقابة الداخليّة	١,٩,٤
4.9.2	Assessment of Internal Controls	43	٤٣	تقييم إجراءات الرقابة الداخليّة	٢,٩,٤
4.10	Staff Training & Hiring	43	٤٣	تدريب الموظفين وتعيينهم	١٠,٤
4.10.1	Staff Training & Awareness	43	٤٣	تدريب الموظّفين ورفع مستوى الوعي لديهم	١,١٠,٤
4.10.2	Staff Hiring & Appointment of Senior Positions	44	٤٤	تعيين الموظفين وإختيارهم في مناصب رفيعة	٢,١٠,٤
4.11	Record Keeping & Retention	44	٤٤	حفظ بالسجلات	١١,٤
5	AML/CTF Other Risks	46	٤٦	المخاطر الأخرى لمكافحة غسل الأموال وتمويل الإرهاب	٥
5.1	Product/ Service Risks	46	٤٦	مخاطر المنتج / الخدمة	١,٥
5.1.1	Cash	46	٤٦	المال النقدي	١,١,٥
5.1.2	Wire Transfers	47	٤٧	التحويل البرقي	٢,١,٥
5.1.3	Alternative Remittances	50	٥٠	التحويلات البديلة	٣,١,٥
5.1.4	Money Exchangers	51	٥١	محلات ومؤسسات الصرافة	٤,١,٥
5.1.5	Electronic Banking	51	٥١	العمليّات البنكيّة الإلكترونيّة	٥,١,٥

5.1.6	International Trade	52	٥٢	التجارة الدوليّة	٦,١,٥
5.2	Country Geographic Risks	52	٥٢	مخاطر البلد /المخاطر الجغرافية	٢,٥
5.3	Risk Variables	54	٥٤	تغيّرات المخاطر	٣,٥
6	Glossary	55	٥٥	(التعاريف)	٦
7	Appendices	58	٥٨	روابط وملحقات	٧
7- A	Saudi AML Law & Bylaws	58	٥٨	النظام السعودي لمكافحة غسل الأموال ولائحته التنفيذية	٧– أ
7- B	FATF 40 Recommendations on Anti-Money Laundering	58	٥٨	التوصيات الأربعون لمجموعة العمل المالي (فاتف)	٧– ب
7- C	FATF Member Countries	58	٥٨	الدول الأعضاء في مجموعة العمل المالي (فاتف),	٧– ج
7- D	Basel Committee Standards	58	٥٨	معايير لجنة بازل	٧– د
7- E	UN Security Council Resolutions	58	٥٨	قرارات مجلس الأمن التابع للأمم المتحدة	٧– هـ
7- F	Other Useful Resources & Links	58	٥٨	مصادر وروابط أخرى مفيدة	٧– و
8	Suspicious Transaction Report (STR)	59	٥٩	نموذج الابلاغ عن العمليات المشتبه بها	٨
9	Cash Declaration Form	61	٦١	نموذج الإقرار النقدي	٩
10	Red Flag Indicators	63	٦٣	مؤشرات لعمليات قد تكون مشبوهة	١٠

1. Introduction

1.1 Saudi Arabia Initiatives

The past few years have seen rapid and far-reaching developments in the international financial sector involving a comprehensive and coordinated fight against money laundering and terrorist financing. Consequently, the Kingdom of Saudi Arabia has adopted a variety of initiatives involving legislative and other measures that are responsive to international developments. Some of these initiatives adopted by Saudi Arabia are listed below:

1.1.1 International Level

- Saudi Arabia signed and ratified the United Nations Convention on Illicit Traffic of Narcotic Drugs & Psychotropic Substances (1988, Vienna).
- Saudi Arabia has signed and ratified the International Convention for the Suppression of the Financing of Terrorism (1999, New York).
- Saudi Arabia has signed and ratified the United Nations Convention against Transnational Organized Crime (2000, Palermo).
- The Kingdom of Saudi Arabia signed the UN Convention Against Corruption in January 2004.
- Saudi Arabia has implemented all relevant United Nations Security Council (UNSC) Resolutions, such as Resolutions # 1267 (1999), 1333 (2000), 1373 (2001).
- Saudi Arabia is a member country of the Gulf Cooperation Council (GCC), which is a full member of the Financial Action Task Force (FATF).
- In September 2003, Saudi Arabia completed the Mutual Evaluation by a team of FATF assessors, based on the 40+8 FATF Recommendations and was one of the first countries evaluated under this new methodology. The result of this evaluation was discussed in February 2004 Plenary Meeting in Paris and was highly positive.
- The Kingdom of Saudi Arabia underwent a joint Assessment conducted by the Middle East and North Africa Financial Action Task Force (MENAFATF) in participation with FATF, based on the 40+8 FATF Recommendations. The result of this assessment was discussed in May 2010 in the MENAFATF meeting in Tunisia and was also discussed in the plenary meeting of FATF held in June 2010 in Amsterdam where the Kingdom achieved a very positive result. The assessment report of the Kingdom can be found on the websites of (MENAFATF and FATF).

1.1.2 Regional & Group Level

- At a meeting held in April 1998, Saudi Arabia signed and ratified the Arab Anti-Terrorism Agreement under the auspices of the Arab League.
- In July 1999, Saudi Arabia signed and ratified the Organization of Islamic Conference (OIC) Agreement for the suppression of international terrorism.
- In May 2004, Saudi Arabia signed and ratified the GCC Anti-Terrorism Agreement.
- Saudi Arabia is a founding member of the Middle East-North Africa FATF (MENA-FATF), which was created in November 2004 with the purpose of promoting and implementing international AML/CTF standards in the region, and adopting the FATF 40+9 Recommendations on Anti-Money Laundering and Combating Terrorist Financing.

١. المقدّمة

١,١ مبادرات المملكة العربيّة السعوديّة

لقد شهدت السنوات القليلة الماضية تطوّرات سريعة وبعيدة المدى والنطاق على صعيد القطاع المالي الدولي بما في ذلك تنسيق الجهود للعمل على مكافحة غسل الأموال وتمويل الإرهاب. وبالتالي تبنت المملكة العربية السعودية مجموعة من المبادرات المختلفة والتي شملت تدابير قضائية ومعايير أخرى استجابة للتطوّرات الدولية في هذا المجال. وفيما يلي مجموعة من هذه المبادرات :

١,١,١ المستوى الدولي

- وقّعت المملكة العربيّة السعوديّة وأقرّت اتفاقيّة الأمم المتّحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية (فيينا ١٩٨٨م)
- وقّعت المملكة العربيّة السعوديّة وأقرّت الاتفاقيّة الدوليّة لقمع تمويل الإرهاب (نيويورك١٩٩٩م).
- وقّعت المملكة العربيّة السعوديّة وأقرّت اتفاقيّة الأمم المتّحدة لمكافحة الجريمة المنظّمة (باليرمو ٢٠٠٠م).
- وقعت المملكة العربية السعودية على اتفاقية الأمم المتحدة لمكافحة الفساد في شهر يناير ٢٠٠٤م.
- طبقت المملكة العربيّة السعوديّة جميع القرارات ذات الصلة الصادرة عن مجلس الامن التابع للامم المتحدة، مثل رقم : ١٢٦٧ (١٩٩٩م)، و١٣٣٣ (٢٠٠٠م)، و١٣٧٣ (٢٠٠١م)، الخ.
- تشارك المملكة العربيّة السعوديّة في مجموعة العمل المالي (فاتف) من خلال عضوية مجلس التعاون الخليجي في هذه المجموعة.
- في شهر سبتمبر ٢٠٠٣م، خضعت المملكة العربيّة السعوديّة للتقييم المشترك من قبل فريق من مجموعة العمل المالي (فاتف) وفقاً لتوصيات فريق العمل المالي (فاتف) الأربعين والتوصيات الثمانية الخاصة في ذلك الوقت، وكانت من بين الدول الأوائل التي قُيمت وفقاً لهذه المنهجيّة الجديدة. وقد تمت مناقشة هذا التقييم في الجلسة العامّة التي عُقدت في شهر فبراير ٢٠٠٤م في باريس وكانت نتيجته إيجابيّة جداً.
- خضعت المملكة العربية السعودية للتقييم المشترك من قبل مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (مينافاتف) وبمشاركة مجموعة العمل المالي (فاتف) وفقاً لتوصيات مجوعة العمل المالي (فاتف) الأربعين والتوصيات التسع الخاصة، وقد تم مناقشة هذا التقييم في اجتماع مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (مينافاتف) في تونس شهر مايو ٢٠١٠م كما نوقش خلال اجتماع مجموعة العمل المالي (فاتف) في الجلسة العامة التي عقدت في شهر يونيو ٢٠١٠م في أمستردام وحصلت المملكة على نتيجة إيجابية جداً. ويمكن الإطلاع على تقرير تقييم المملكة في كل من الموقع الالكتروني لـ(المينافاتف و الفاتف).

٢,١,١ المستوى الإقليميّ

- وقّعت المملكة العربية السعودية وأقرّت الاتفاقية العربية لمكافحة الإرهاب برعاية جامعة الدول العربيّة على هامش مؤتمر عُقد في شهر أبريل ١٩٩٨م.
- في شهر يوليو ١٩٩٩م، وقّعت المملكة العربيّة السعودية وأقرت اتفاقية منظّمة المؤتمر الإسلاميّ لمكافحة الإرهاب الدولي.
- في شهر مايو ٢٠٠٤م، وقّعت المملكة العربيّة السعوديّة وأقرّت اتفاقيّة دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب.
- تعد المملكة العربيّة السعوديّة عضواً مؤسساً لمجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (مينافاتف) والتي أنشئت في شهر نوفمبر ٢٠٠٤م بغرض نشر وتطبيق المعايير الدوليّة لمكافحة غسل الأموال وتمويل الإرهاب في المنطقة، والتي تبنّت التوصيات الأربعين والتوصيات التسع الخاصة لمجموعة العمل المالي (فاتف) لمكافحة

غسل الأموال وتمويل الإرهاب.

٣,١,١ المستوى المحلي

- تم إصدار نظام لمكافحة غسل الأموال ولائحته التنفيذية في المملكة العربيّة السعوديّة بموجب قرار مجلس الوزراء رقم ١٦٧ تاريخ ١٤٢٤/٦/٢٠ هـ وبموجب المرسوم الملكيّ رقم م/٣٩ تاريخ ١٤٢٤/٦/٢٥ هـ، وتم اعتماده كأساس قانوني لتجريم أنشطة غسل الأموال وتمويل الإرهاب.
- بموجب المادّة ١١ من نظام مكافحة غسل الأموال تم إنشاء وحدة التحريات الماليّة السعوديّة تحت اشراف وزارة الداخليّة لتكون السلطة المركزيّة التي تتلقّى وتحلّل تقارير العمليات المشتبه بها والمتعلّقة بأنشطة غسل الأموال وتمويل الإرهاب.
- أنشأت المملكة العربيّة السعوديّة لجنتين وطنيتين دائمتين من وزارات ومؤسسات حكوميّة مختلفة، بما في ذلك مؤسسة النقد العربي السعودي للتعامل مع المواضيع المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب في المملكة.

٢,١ <u>ميادرات مؤسسة النقد العربي السعودي</u>

قامت مؤسسة النقد العربي السعودي منذ تأسيسها في العام ١٩٥٢م بإصدار العديد من التعليمات إلى البنوك ومحلات الصرافة والتي تتعلّق بتحديد هويّة العملاء ومعلومات العميل الأخرى، وبالتقيّد بتعلميات العناية الواجبة عند التعامل مع العملاء، وحفظ المستندات والملفات ذات الصلة بالإضافة إلى تبليغ السلطات المختصّة بالعمليات المشتبه بها وقد أدرجت هذه التوجيهات في عدد من الأدلّة التنظيميّة الرئيسيّة من بينها ما يلي:

١,٢,١ قواعد مكافحة غسل الأموال وتمويل الإرهاب

في شهر نوفمبر ١٩٩٥م أصدرت مؤسسة النقد العربي السعودي أولى التعليمات المتعلّقة بأنشطة مكافحة غسل الأموال إلى جميع البنوك العاملة في المملكة العربيّة السعوديّة. وإدراكاً منها للجهود الدوليّة والقانونيّة المبذولة لمكافحة أنتشار ظاهرة غسل الأموال وتمويل الإرهاب أصدرت المؤسسة في شهر مايو من عام ٢٠٠٣م التحديث الأول لقواعد مكافحة غسل الأموال وتمويل الإرهاب".

وقد أتى التحديث الأول الذي صدر في شهر مايو ٢٠٠٣م بتحسينات جوهريّة على الأنظمة والقواعد السابقة وقد شمل أيضاً أحكاماً تتعلّق بمكافحة تمويل الإرهاب. كما قدّم معايير وإجراءات أساسيّة من الواجب اتخاذها لمنع واكتشاف ومراقبة العمليات والتبليغ عن أنشطة غسل الأموال وتمويل الإرهاب. ومنذ ذلك الحين وفي إطار جهود المؤسسة المستمرّة والمتواصلة لإدخال تحسينات إضافيّة على الأنظمة والأحكام، أتي التحديث الثاني لهذه القواعد في شهر ديسمبر ٢٠٠٨م، ولمواكبة التطورات المحلية والإقليمية والدولية في هذا المجال أصدرت مؤسسة النقد العربي السعودي هذا التحديث الثالث للقواعد الخاصة بمكافحة غسل الأموال وتمويل الإرهاب.

لذا فإنه يجب على البنوك ومحلات الصرافة أن يجعلوا هذه الأنظمة والأحكام الواردة بها جزءاً لا يتجزّأ من أنظمتهم وإجراءاتهم التي تهدف إلى مراقبة واكتشاف ومنع العمليات والتبليغ عن

1.1.3 National Level

- Saudi Arabia passed the Anti-Money Laundering Law and Bylaws, under Royal Decree # M/39 dated 25/6/1424H, ratifying the Council of Ministers Decision # 167 dated 20/6/1424H, providing a statutory basis for criminalizing money laundering and terrorist financing activities.
- In accordance with the Saudi AML Law Article 11, the Saudi Financial Intelligence Unit (SAFIU) was established under the control of the Ministry of Interior, as the central authority for receiving and analyzing suspicious transaction reports relating to money laundering and terrorist financing activities.
- Saudi Arabia has set up two National Permanent Committees from different Ministries and Government Agencies, including SAMA, to respectively deal with money laundering and terrorist financing issues in the Kingdom.

1.2 <u>SAMA Initiatives</u>

Since its inception in 1952, the Saudi Arabian Monetary Agency (SAMA) has been issuing various directives to banks and money exchangers relating to establishing customers' identity and other information, observing necessary due diligence when dealing with customers, record keeping of relevant documents and files as well as reporting of suspicious transactions to the competent authorities. These directives have since been put together into a number of major regulatory manuals, including:

1.2.1 AML/CTF Regulations

In November 1995, SAMA issued its first set of guidelines relating to AML activities to all banks operating in Saudi Arabia. Consequently, in recognition of the international and legal supervisory efforts to combat the spread of money laundering, And terrorist financing SAMA further updated the initial 1995 AML Guidelines and in May 2003, issued a more extensive set of "Rules Governing Anti-Money Laundering & Combating Terrorist Financing".

The First Update issued in May 2003 provided a substantial improvement to the initial regulations and also included regulations relating to combating terrorist financing. It provided basic measures and actions to be taken to prevent, detect, control and report money laundering and terrorist financing activities. Since then, in SAMA's continued efforts to further improve and refine the regulations, the second Update was issued in December 2008. And to cope with the local, regional and global developments, SAMA has issued this Third Update.

Banks and money exchangers are required to make these regulations and provisions an integral part of their systems and procedures aimed at controlling, detecting, preventing,

and reporting suspicious activities. In this regard, SAMA intends to verify the implementation of these rules by banks and money exchangers operating in Saudi Arabia through SAMA's on-site inspections, receipt of regular compliance reports and certificates prepared by external auditors.

1.2.2 Account Opening Regulations for Banks

In May 2002, SAMA issued its first set of "Rules Governing Opening of Bank Accounts & General Operation Guidelines". The new rules, in addition to consolidating all the previous SAMA circulars on the subject, were significantly improved with new requirements to facilitate implementation and conform to the best international banking practices in line with the Basel Committee principles. The rules outlined the standard requirements applicable to all banks to serve as a regulatory instrument to strengthen internal controls with regards to opening and operation of bank accounts maintained by customers, with a view of protecting the banking industry against illegal financial activities.

In order to cope with ongoing developments and to provide more explanation and clarification to the issues raised by local banks, the initial rules were further enhanced in the First Update released in April 2003. The Second Update of the rules was issued by SAMA in February 2007, the Third Update in December 2008, and the Fourth Update in February 2012 in keeping with the domestic, regional and international developments in this field. SAMA is continuously reviewing and updating the Account Opening regulations and will be issuing new updates to banks and money exchangers in future.

1.2.3 Other Relevant Regulations

SAMA has also issued a number of other regulations in support of its efforts to combat money laundering, terrorist financing and other financial crime activities. Therefore, these AML/CTF Rules should be read in conjunction with the following documents issued by SAMA, in addition to the AML Law and Bylaws issued by the Saudi Government:

- Manual for Combating Embezzlement & Fraudulent Transactions,(second issue) in August 2008
- Designation Requirements for the Leading Professions in the Workin in KSA, issued in April 2005
- Guidelines Manual for Banks in Saudi Arabia for Regulating Audit Committees, issued in July 1996
- Internal Control Manual for Banks Operating in the Kingdom, issued in December 1989
- Manual of Compliance with Regulations for Banks operating in the Kingdom of Saudi Arabia issued in December 2008.
- Rules of Electronic Banking Services issued by SAMA in April 2010.
- Risk Based on- sit Inspection "Policy Framework & Procedures" issued by SAMA in April 2011.
- Risk Based Approach for AML/CFT Supervision issued by SAMA in February 2012.
- Other relevant SAMA Regulatory Circulars.

الأنشطة المشتبه بها. وفي هذا السياق تعتزم مؤسسة النقد العربي السعودي التحقق من تطبيق هذه القواعد من قبل البنوك ومحلات الصرافة العاملة في المملكة العربيّة السعوديّة وذلك من خلال عمليّات التفتيش الميدانيّة التي تقوم بها المؤسسة ومن خلال تقارير وشهادات الالتزام المعدة من قبل مدقّقي حسابات خارجيين.

٢,٢,١ قواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها

في شهر مايو ٢٠٠٢م، أصدرت مؤسسة النقد العربي السعودي مجموعتها الأولى من " قواعد فتح الحسابات البنكية في البنوك التجارية العاملة في المملكة العربية السعودية والقواعد العامة لتشغيلها ". إضافةً إلى توحيد جميع التعاميم السابقة لمؤسسة النقد العربي السعودي بخصوص الحسابات وقد أدخلت المؤسسة متطلّبات جديدة لتسهيل تنفيذ افضل الممارسات البنكيّة الدوليّة المتعارف عليها ولتطبيق الالتزام مع مبادئ لجنة بازل. كما وحددت هذه القواعد المعايير الأساسية التي تنطبق على جميع البنوك بحيث تكون أداة تنظيميّة تعزز من الضوابط الداخليّة فيما يتعلّق بفتح وتشغيل الحسابات البنكيّة للعملاء بغرض حماية القطاع المصرفي من الأنشطة الماليّة غير المشروعة.

ومن أجل مواكبة التطوّرات المستمرّة وتقديم تفسير وتوضيح للمسائل التي تواجه البنوك المحليّة، تم تحسين القواعد الأوّليّة في التحديث الأوّل الذي صدر في شهر أبريل ٢٠٠٣م. أمّا التحديث الثاني للقواعد فقد صدر عن مؤسسة النقد العربي السعودي في شهر فبراير ٢٠٠٧م كما أصدرت التحديث الثالث في شهر ديسمبر ٢٠٠٨م، والتحديث الرابع في شهر فبراير ٢٠١٢م متماشياً مع التطورات المحلية والإقليمية والدولية في هذا المجال. وستقوم مؤسسة النقد العربي السعودي باستمرار بمراجعة وتنقيح هذه القواعد وتحديثها مستقبلاً وإحاطة البنوك ومحلات الصرافة بها.

٣,٢,١ تعليمات أخرى ذات صلة

أصدرت مؤسسة النقد العربي السعودي أيضاً عدداً من التعليمات والقواعد التي تدعم جهودها في مكافحة أنشطة غسل الأموال وتمويل الإرهاب والجرائم الماليّة الأخرى. ولذلك فإن التعليمات والقواعد التالية يجب أن يعمل بها جنباً إلى جنب مع نظام مكافحة غسل الأموال ولائحتة التنفيذية:

- دليل مكافحة الاختلاس والاحتيال المالي (الإصدار الثاني) الصادر في أغسطس ٢٠٠٨م.
- متطلبات التعيين في الوظائف القيادية في البنوك العاملة في المملكة العربية السعودية الصادر في أبريل ٢٠٠٥م.
- الدليل الاسترشادي لتنظيم لجان المراجعة في البنوك المحلية الصادر في يوليو ١٩٩٦م.
- دليل ارشادات الرقابة الداخليّة للبنوك العاملة في المملكة العربية السعودية الصادر في ديسمبر ١٩٨٩م.
- دليل الالتزام بالانظمة للبنوك العاملة في المملكة العربية السعودية الصادر في ديسمبر ٢٠٠٨م.
- قواعد تنظيم تقديم الخدمات المصرفية الإلكترونية الصادر عن المؤسسة في إبريل ٢٠١٠م.
- دليل فحص البنوك المبني على تقييم معدل المخاطر الصادر عن المؤسسة في إبريل ٢٠١١م.
- دليل فحص البنوك المبني على تقييم معدل المخاطر الخاص بغسل الاموال وتمويل الارهاب الصادر من مؤسسة النقد في شهر فبراير ٢٠١٢م.
- التعاميم التنظيمية الأخرى ذات العلاقة الصادرة من مؤسسة النقد العربي السعودي.

1.3 Objectives

The core objectives of SAMA in issuing these regulations are as follows:

1. To ensure compliance of banks and money exchangers in Saudi Arabia with regulations and instructions related to combating money laundering and terrorist financing in general and the Saudi AML Law & Bylaws in particular.
2. To help banks and money exchangers operating in Saudi Arabia to comply with the Banking Control Law, AML Law, SAMA Regulations, and all relevant United Nations Security Council Resolutions.
3. To implement policies, standards, procedures and systems for the prevention, detection, control and reporting of money laundering and terrorist financing activities in accordance with the Basel Committee Principles and the FATF Recommendations on AML/CTF.
4. To protect banks and money exchangers operating in Saudi Arabia from being exploited as channels for passing illegal transactions arising from money laundering, terrorist financing and any other criminal activities.
5. To maintain, enhance and protect the credibility, integrity and reputation of the Saudi Arabian banking and financial systems.
6. To provide the highest degree of protection for costumers.

٣,١ الأهداف

ان الأهداف الأساسية لمؤسسة النقد العربي السعودي من إصدار هذه التعليمات والقواعد هي كما يلي :

١. ضمان التزام البنوك ومحلات الصرافة العاملة في المملكة العربيّة السعوديّة بالانظمة والتعليمات ذات العلاقة بمكافحة غسل الأموال وتمويل الإرهاب بصفة عامة وبنظام المملكة العربية السعودية لمكافحة غسل الأموال ولائحته التنفيذية بصفة خاصة.
٢. مساعدة البنوك ومحلات الصرافة العاملة في المملكة العربيّة السعوديّة على التقيّد بنظام مراقبة البنوك ونظام مكافحة غسل الأموال وتعليمات مؤسسة النقد العربي السعودي, وجميع القرارات ذات الصلة الصادرة من مجلس الأمن التابع للأمم المتحدة.
٣. تطبيق السياسات، والمعايير، والإجراءات والأنظمة لمنع واكتشاف ومراقبة العمليات والتبليغ عن أنشطة غسل الأموال وتمويل الإرهاب وفقاً لمبادئ لجنة بازل والتوصيات الصادرة من مجموعة العمل المالي (فاتف) حول مكافحة غسل الأموال وتمويل الإرهاب.
٤. حماية البنوك ومحلات الصرافة العاملة في المملكة العربيّة السعوديّة من أن تُستغل كقنوات لتمرير العمليات غير المشروعة والناشئة عن أنشطة غسل الأموال وتمويل الإرهاب وأيّة جرائم أخرى.
٥. تعزيز وحماية الثقة بنزاهة وسمعة الأنظمة البنكية والمالية السعودية والمحافظة عليها.
٦. توفير أفضل درجات الأمن والحماية للعملاء.

1.4 General Developments & Trends

At the global level, money laundering activities, particularly those related to drugs now constitute a multi-million dollar business annually. It is inconceivable and unlikely that such large amounts of money can be saved or moved without the cooperation or voluntary participation of many international financial institutions and banking systems. In many quarters, money laundering is considered a serious threat to the integrity of many international banks and even banking systems.

Money laundering has become a widespread phenomenon involving highly sophisticated techniques to penetrate different banking systems. This has led lawmakers, law enforcement agencies and supervisory authorities in many countries to cooperate, locally and internationally, to combat this phenomenon. In this respect, the FATF was created and it has carried out extensive work and issued Recommendations to counter the spread of money laundering and terrorist financing.

The techniques used by money launderers constantly evolve to match the sources and volume of funds to be laundered, and the legal, regulatory, law enforcement environment of the market place in which the money launderers operate.

٤,١ التطورات والاتجاهات

على الصعيد العالمي تدر أنشطة غسل الأموال لا سيّما تلك المتعلّقة بالمخدرات ملايين الدولارات سنوياً، ومن غير المحتمل أن تدّخر هذه المبالغ الكبيرة أو تنقل من دون تعاون أو مشاركة طوعيّة للعديد من المؤسسات الماليّة الدوليّة والأنظمة البنكيّة. وتشكل عمليات غسل الأموال تهديداً خطيراً لنزاهة عدد كبير من البنوك الدوليّة والأنظمة البنكيّة.

لقد أصبحت عمليات غسل الأموال ظاهرة منتشرة بشكل كبير وتشتمل على تقنيّات معقّدة جداً لاختراق الأنظمة البنكيّة المختلفة. وقد دفع هذا الأمر بالمشرعين ومؤسسات انفاذ القوانين وسلطات الإشراف في دول عديدة إلى التعاون محلياً ودولياً لمكافحة هذه الظاهرة. وفي هذا الخصوص أنشئت لجنة العمل المالي (فاتف) وقامت بأعمال مهمة وأصدرت التوصيات للحد من أنتشار جرائم غسل الأموال وتمويل الإرهاب.

وتتطور باستمرار التقنيّات والأساليب التي يستخدمها غاسلو الأموال لتتناسب مع مصادر وحجم الأموال التي يتم غسلها وبيئة العمل القانونيّة، والتنظيميّة وسلطات انفاذ القانون في الأسواق التي يعملوا بها.

2. Legal Framework & Regulatory Requirements

٢. الإطار النظامي والمتطلّبات التنظيميّة

2.1 The Saudi AML Law & Bylaws

The Kingdom of Saudi Arabia, in its contributions towards the international initiatives to combat money laundering and terrorist financing crimes, has enacted the Anti-Money Laundering Law in August 2003. The Law criminalizes money laundering and terrorist financing acts and has created offenses, responsibilities and penalties for violation, aimed at preventing these crimes.

١,٢ نظام مكافحة غسل الأموال في المملكة العربية السعوديّة

قامت المملكة العربيّة السعوديّة إنطلاقاً من مساهماتها نحو المبادرات الدوليّة لمكافحة جرائم غسل الأموال وتمويل الإرهاب بإصدار نظام مكافحة غسل الأموال في شهر أغسطس ٢٠٠٣م. ويُجرّم النظام أفعال غسل الأموال وتمويل الإرهاب في المملكة وقد حدد الجرائم والمسؤوليّات والعقوبات المترتبة على مخالفة هذا النظام بهدف الحد من اقتراف هذه الجرائم.

ويطبق نظام مكافحة غسل الأموال من خلال مواده ولائحته التنفيذية على جميع البنوك

The AML Law, through its Articles and the Bylaws, is applicable to all banks and money exchangers and requires all financial institutions to have in place adequate policies, systems, measures and controls in place, relating to customer identification, know your customer/ due diligence, risk assessment, monitoring and reporting suspicions, training and record keeping to deter and prevent money laundering and terrorist financing acts.

ومحلات الصرافة ، كما ويطلب من جميع المؤسسات الماليّة أن تضع سياسات وأنظمة وإجراءات وضوابط مناسبة تتعلّق بتحديد هويّة العميل، ومبادئ لمعرفة العميل وبذل العناية الواجبة، وتقييم للمخاطر، ومراقبة العمليات، والتبليغ عن حالات الاشتباه، والتدريب وحفظ السجلات بغرض منع ومكافحة أنشطة غسل الأموال وتمويل الإرهاب.

2.2 SAMA – Regulatory & Supervisory Authority

The Saudi Arabian Monetary Agency (SAMA), in accordance with the authority and powers vested on it under relevant Saudi laws, is the legislative body responsible for exercising regulatory and supervisory control over banks and money exchangers, issuing general rules and overseeing that all banks and money exchangers comply with and effectively implement the following relevant laws and regulations:

1. The Charter of Saudi Arabian Monetary Agency .
2. The Banking Control Law.
3. Decision of the Minister of Finance & National Economy on Regulating Money Changing Business.
4. The Anti-Money Laundering Law.

SAMA regards the adoption and implementation by all banks and money exchangers of effective policies, procedures and controls for the deterrence and prevention of money laundering, terrorist financing and other financial crimes as very vital. SAMA expects all banks and money exchangers and their employees to conduct business in accordance with these rules and all applicable laws by applying the highest ethical standards. SAMA will use these rules and other standards to measure the adequacy of each bank's or money exchanger's implementation strategies. SAMA will take appropriate disciplinary measures and actions against banks and money exchangers for any violations, in accordance with the Banking Control Law Article 25 (Rules for Enforcing Provision of the Banking Control Law).

As the regulatory and supervisory authority for banks and money exchangers, SAMA has a duty not only to ensure banks and money exchangers maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system. Therefore, SAMA will exercise the following responsibilities:

1. Monitoring that banks and money exchangers are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis.
2. Ensuring that appropriate internal controls are in place and banks and money exchangers are in compliance with supervisory and regulatory requirements.
3. SAMA examination will include review of bank's and money exchanger's policies and procedures, customer files including sampling of some accounts, documentation related to accounts maintained and the analysis made to detect unusual or suspicious transactions.
4. Taking appropriate action against banks or money exchangers and their officers and employees who demonstrably fail to follow the required procedures and regulatory requirements.

٢,٢ مؤسسة النقد العربي السعودي – الجهة التنفيذية والإشرافية

ان مؤسسة النقد العربي السعودي، ووفقاً للصلاحيّة والسلطات المنوطة بها بموجب الانظمة ذات الصلة تعد الجهة التنظيمية المسؤولة عن ممارسة التنظيم والرقابة والإشراف على البنوك ومحلات الصرافة بحيث تصدر القواعد العامّة وتحرص على ان تطبّق جميع البنوك ومحلات الصرافة الأنظمة والتعليمات ذات الصلة بشكل فعّال وذلك طبقاً لما يلي:

١. نظام مؤسسة النقد العربي السعودي .
٢. نظام مراقبة البنوك.
٣. قرار وزير المالية والاقتصاد الوطني حول تنظيم أعمال مهنة الصرافة.
٤. نظام مكافحة غسل الأموال .

وان تبنّي جميع البنوك ومحلات الصرافة للسياسات، والإجراءات والضوابط الفعّالة لمكافحة ومنع عمليات غسل الأموال وتمويل الإرهاب والجرائم الماليّة الأخرى وتنفيذها يُشكّل بنظر مؤسسة النقد العربي السعودي أمراً حيوياً وأساسياً جداً. وتتوقّع المؤسسة من جميع البنوك ومحلات الصرافة وموظّفيهم القيام بالأعمال وفقاً لهذه القواعد وجميع الانظمة ذات الصلة عبر تطبيق أعلى المعايير الأخلاقيّة. وسوف تستخدم مؤسسة النقد العربي السعودي هذه القواعد والمعايير الأخرى لقياس مدى كفاءة استراتيجيّات التنفيذ الخاصّة بكلّ بنك أومحل صرافة. وسوف تتخذ المؤسسة التدابير والإجراءات الجزائية المناسبة ضد البنوك ومحلات الصرافة عند حصول أي مخالفات وذلك وفقاً للمادة ٢٥ من نظام مراقبة البنوك (قواعد تطبيق أحكام نظام مراقبة البنوك).

وبما ان مؤسسة النقد العربي السعودي تعد الجهة المعنية بالتنظيم والإشراف على البنوك ومحلات الصرافة، فإن دورها لا يقتصر على ضمان محافظة البنوك ومحلات الصرافة على أعلى المعايير لتطبيق مبدأ أعرف عميلك لحماية أمنهم وسلامتهم وانما تقوم أيضاً بحماية نزاهة النظام البنكي المحلي وبالتالي فإن مؤسسة النقد العربي السعودي ستقوم انطلاقاً من مسؤليتها بما يلي:

١. مراقبة مدى تطبيق البنوك ومحلات الصرافة للإجراءات السليمة لمبادئ اعرف عميلك والمحافظة على المعايير الأخلاقيّة والمهنيّة.
٢. التأكد من مناسبة الضوابط الداخليّة الموضوعة ومن التزام البنوك ومحلات الصرافة بالمتطلّبات الإشرافية والتنظيمية.
٣. تشمل عمليّات المراقبة والإشراف التي تقوم بها مؤسسة النقد العربي السعودي مراجعة سياسات وإجراءات البنوك أو محلات الصرافة، وملفات العملاء بما في ذلك أخذ عيّنات من بعض الحسابات، والمستندات المتعلقة بالحسابات وعمليات التحليل التي تُجرى لاكتشاف العمليات غير الاعتياديّة أو المشتبه بها.
٤. اتخاذ الإجراء المناسب ضدّ البنوك أومحلات الصرافة وموظّفيهم الذين ثبت اخفاقهم في اتّباع الإجراءات المطلوبة والمتطلّبات التنظيميّة.

2.3 Domestic Banks & Money Exchangers & Foreign

٣,٢ البنوك المحلية ومحلات الصرافة و فروع البنوك الأجنبية العاملة في

Banks' Branches Operating in the Kingdom

The provisions of these rules shall apply to domestic banks, money exchangers, and foreign banks' branches operating in the Kingdom. All banks and money exchangers and foreign banks' branches shall have in place effective policies, procedures and controls to combat and prevent money laundering and terrorist financing and other financial crimes. Foreign banks' branches operating in the Kingdom must apply the requirements compatible with regulations and rules applicable in the Kingdom as a minimum and the requirements of the country of origin if such requirments are stronger. They must also inform SAMA in case of being unable to comply with the requirements, or for reasons imposed by the laws of the country of origin.

المملكة

تسري أحكام هذه القواعد على البنوك المحلية ومحلات الصرافة وفروع البنوك الأجنبية العاملة في المملكة ولتطبيق أحكام هذه القواعد يجب أن تضع جميع البنوك ومحلات الصرافة وفروع البنوك الأجنبية السياسات والإجراءات والضوابط الفعّالة لمكافحة ومنع عمليات غسل الأموال وتمويل الإرهاب والجرائم الماليّة الأخرى، كما يجب على فروع البنوك الأجنبية العاملة في المملكة تطبيق المتطلبات المتوافقة مع الانظمة والتعليمات المتبعة في المملكة كحد ادنى ، والاخذ بتعليمات بلد المنشأ في حال كانت المتطلبات أشد. كما يجب عليها إبلاغ مؤسسة النقد العربي السعودي في حال عدم قدرتها الالتزام بالمتطلبات أو لاسباب تفرضها قوانين بلد المنشأ.

2.4 Overseas Branches & Subsidiaries of Saudi Banks & Money Exchangers

As per the Saudi AML Law, these regulations are also applicable to overseas branches and subsidiaries of all Saudi banks and domestic money exchangers, banks and money exchangers should ensure all their foreign branches and subsidiaries apply the requirements of both the Saudi AML Law and these Rules.
In addition, banks and money exchangers should ensure the following:

1. Paying particular attention to their foreign branches and subsidiaries located in countries that do not or insufficiently apply FATF Recommendations.
2. Ensuring their foreign branches and subsidiaries apply higher requirements of either the host country or the ho country in case the requirements of the host and ho countries differ.
3. Informing SAMA when a foreign branch or subsidiary is unable to observe appropriate AML/ CTF requirements because it is prohibited by its local laws, regulations or other measures.

٤,٢ الفروع والشركات الخارجية التابعة للبنوك السعودية ومحلات الصرافة

تنطبق هذه القواعد على الفروع الخارجية والشركات التابعة للبنوك ومحلات الصرافة المحلية وذلك وفقًا لنظام مكافحة غسل الأموال ولائحته التنفيذية الفقرة ، وبالتالي يجب أن تضمن البنوك ومحلات الصرافة تطبيق متطلّبات نظام مكافحة غسل الأموال وهذه القواعد على جميع فروعهم في الخارج وشركاتهم التابعة. بالإضافة إلى ذلك يجب على البنوك ومحلات الصرافة ما يلي :

١. توجيه اهتمام خاص بفروعهم في الخارج وشركاتهم التابعة الموجودة في الدول التي لا تقوم أو لا تطبّق بشكل كافٍ توصيات لجنة العمل المالي (فاتف).
٢. ضمان أن فروعهم في الخارج وشركاتهم التابعة تطبّق المتطلّبات القصوى للبلد المضيف أو البلد المنشأ في حال كانت تختلف متطلّبات البلد المضيف عن متطلبات البلد المنشأ.
٣. تبليغ مؤسسة النقد العربي السعودي عندما يكون فرع في الخارج أو شركة تابعة غير قادرة على الالتزام بالمتطلبات المناسبة لمكافحة غسل الأموال وتمويل الإرهاب لاسباب تفرضها القوانين المحليّة لذلك البلد، أو أنظمته أو تدابيره الأخرى.

2.5 Legal Responsibilities of Banks/ Money Exchangers & Employees

The Saudi AML Law and Bylaws stipulate responsibilities, offenses, violations and penalties that have direct or indirect implications on financial institutions -including banks and money exchangers- and on their staff personally. This is in addition to the responsibilities stupiulated in the Banking Control Law and the Decision Regulating Money Changing Business applicable to practitioners of banking activities such as banks, money exchangers and their employees.

(For full details of the AML Law and Bylaws, refer to Appendix7- A):

٥,٢ المسؤولية القانونيّةعلى البنوك ومحلات الصرافة وموظفيها

حدد نظام مكافحة غسل الأموال ولائحته التنفيذية في المملكة العربية السعودية المسؤوليّات والجرائم والمخالفات والعقوبات التي لها تأثير مباشر أو غير مباشر على المؤسسات المالية بما فيها البنوك ومحلات الصرافة أو موظّفيها بصفة شخصية. إضافةً إلى ما تضمنه نظام مراقبة البنوك وقرار تنظيم أعمال مهنة الصرافة من مسئوليات تترتب على ممارسي الأنشطة المصرفية من بنوك ومحلات صرافة وموظفيها.
(نظام مكافحة غسل الأموال ولائحته التنفيذية موجودة في الملحق ٧-أ) .

2.6 Financial Intelligence Unit (FIU)

The FIU shall receive reports of suspected transactions related to money laundering and terrorist financing for their verification and analysis and preparing reports thereof to authorities concerned to effectively carry out their role in combating and preventing money laundering, terrorist financing and other financial crimes. To this end, countries around the world have created specialized governmental agencies, known as Financial Intelligence Units, to be the central entities for receiving such suspicion reports.

Similarly, Saudi Arabia, According to the Saudi AML Law, has formed a Financial Intelligence Unit (SAFIU) to be responsible for receiving, analyzing and reporting to competent authorities on suspicious activities.

٦,٢ وحدة التحريات الماليّة

تقوم وحدة التحريات المالية بعملية تلقي بلاغات الإشتباه عن العمليات المرتبطة بقضايا غسل الأموال وتمويل الإرهاب لتقوم بتحليلها واعادة توجيهها وإعداد التقارير عنها للسلطات المعنيّة لتقوم بشكل فعّال بدورها في مكافحة ومنع غسل الأموال وتمويل الإرهاب والجرائم الماليّة الأخرى، واستجابة لذلك استحدثت الدول وكالات حكوميّة متخصصة تعرف باسم وحدات التحريات الماليّة، لتكون الجهات المركزية التي تتلقي بلاغات الاشتباه.

وعلى نحو مشابه قامت المملكة العربية السعودية ووفقاً لنظام مكافحة غسل الأموال بإنشاء وحدة تحريات ماليّة تكون مسؤولة عن تلقي تقارير العمليات المشتبه بها من المؤسسات المالية وغير المالية وتحليلها واحالتها للسلطات المعنيّة.

2.7 Cooperation Among Authorities & Banks/ Money Exchangers

Cooperation among banks/ money exchangers and various competent authorities, in the exchange and sharing of relevant information, is very vital in the AML/CTF initiatives. However, such information exchange and sharing should be coordinated and achieved only through SAMA because of the importance and sensitivity of maintaining confidentiality of banking and financial operations and strengthening customer confidence in the Saudi banking system.

2.7.1 Cooperation With Local Authorities

Under the Saudi AML Law, financial institutions are authorized and required to cooperate and share relevant information with local competent authorities, such as FIU and law enforcement authorities, for matters relating to money laundering, terrorist financing and other financial crimes. Banks and money exchangers should, therefore, have in place appropriate policies and procedures, as follows:

1. Establishment of a Money Laundering Control Unit (MLCU) or appointing a designated Compliance Officer within the bank or money exchanger, responsible - among other things- for receiving internal reports (from branches or other department within the bank or money exchanger) and informing FIU of suspected money laundering or terrorist financing activities. (Refer to **Rule 4.8.4** of these Rules for details about the tasks and responsiblities of MLCU).
2. The manner and method in which the MLCU/ designated Compliance Officer should contact the authorities and pass relevant transactional information to them.
3. Where records are to be provided to the authorities, establishing the form of such records (original or copies) and the receipt and forms to be used for providing and receiving information by the MLCU/ designated Compliance Officer.
4. When information is to be provided verbally to authorities, the manner and form of such information shall be defined.
5. In some cases, depending upon the case, a new or a different procedure may need to be followed. For example, in the event of a large cash transfer, telephone notification may be quicker than filing a report especially if immediate decision to prevent the transfer is required.

2.7.2 Cooperation Among Banks & Money Exchangers Operating in the Kingdom

Banks and money exchangers should cooperate locally and abroad through their representatives in the Financial Crimes & Money Laundering Committee (FCML) for AML/CTF matters. This should be done through the exchange of information with banks' and money exchangers' officers, and SAMA, about cases and transactions that they may discover, or suspect to be of money laundering or terrorist financing nature as required by the Saudi AML Law and Bylaws. However, at the same time they must strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy. Banks and money exchangers must coordinate in advance with SAMA in case they agree to mutually assist or exchange information.

٧,٢ التعاون بين السلطات والبنوك ومحلات الصرافة

يعد التعاون بين البنوك ومحلات الصرافة والسلطات المختصّة المختلفة في عمليات تبادل المعلومات ذات الصلة أمراً حيوياً في مبادرات مكافحة غسل الأموال وتمويل الإرهاب. ويجب تنسيق عمليّة تبادل المعلومات والتعاون بين البنوك ومحلات الصرافة والسلطات المختصة من خلال مؤسسة النقد العربي السعودي وذلك لأهمية وحساسية المحافظة على سرية التعاملات المصرفية والمالية وتدعيم ثقة المتعاملين بالنظام المصرفي السعودي.

١,٧,٢ التعاون مع السلطات المحليّة

يسمح للمؤسسات المالية بل ويطلب منها بموجب نظام مكافحة غسل الأموال التعاون وتبادل المعلومات ذات الصلة مع السلطات المحلّية المختصّة، مثل وحدة التحريات الماليّة وسلطات انفاذ القانون وذلك فيما يتعلّق بالمسائل الخاصة بغسل الأموال وتمويل الإرهاب والجرائم الماليّة الأخرى ، وبالتالي فإنه يجب أن يكون لدى البنوك ومحلات الصرافة سياسات وإجراءات مناسبة بهذا الشأن وذلك على النحو التالي:

١. إنشاء وحدة مراقبة غسل الأموال أو تعيين مسؤول التزام داخل البنك أومحل الصرافة يكون ضمن مسئوليتها تلقي البلاغات داخلياً (من الفروع والادارات الاخرى داخل البنك او محل الصرافة) وإبلاغ وحدة التحريات الماليّة عند الاشتباه بوجود أنشطة لغسل الأموال أو تمويل الإرهاب. (توجد تفاصيل عن مهام ومسئوليات وحدة مراقبة غسل الأموال في القاعدة ٤,٨,٤ من هذه القواعد).
٢. تحديد الطريقة والأسلوب الذي يجب أن تتبعه وحدة مراقبة غسل الأموال أو مسؤول الالتزام المكلف في البنك او محل الصرافه عند الاتصال بتلك السلطات ونقل المعلومات ذات الصلة إليها حول هذه العمليات.
٣. تحديد السجلات (الأصليّة أوالنسخ عنها), وإيصالات الاستلام والنماذج المستخدمة لتسليم واستلام المعلومات من قبل وحدة مراقبة غسل الأموال / مسؤول الالتزام المكلف في حالة وجوب تزويد السلطات المعنية بالسجلاّت.
٤. تحديد الطرق والنماذج المستخدمة في حال وجوب تزويد المعلومات شفوياً إلى السلطات.
٥. قد تدعو الحاجة في بعض الحالات إلى اتباع إجراءات مختلفة وذلك بحسب الحالة فعلى سبيل المثال في حال وجود عمليّة تحويل لمبلغ كبير من المال قد يكون الإخطار الهاتفي أسرع من تقديم تقرير, خصوصاً في حال كان القرار الفوري بمنع التحويل مطلوباً.

٢,٧,٢ التعاون بين البنوك ومحلات الصرافة العاملة في المملكة

يجب على البنوك ومحلات الصرافة التعاون محلياً وخارجياً فيما يتعلّق بشؤون مكافحة غسل الأموال وتمويل الإرهاب وذلك من خلال ممثليهم في اللجنة المصرفية لمكافحة الجرائم الماليّة وغسل الأموال. كما أن تبادل المعلومات مع مسؤولي البنوك ومحلات الصرافة ومؤسسة النقد العربي السعودي بشأن الحالات والعمليات التي قد يكتشفونها أو يشتبهون بأنها عملية غسل أموال أو تمويل إرهاب يعد مطلباً أساسياً كما تضمنه نظام مكافحة غسل الأموال ولائحته التنفيذية. ولكن في الوقت ذاته يتعيّن عليهم أن يتقيّدوا بشكل تام بالإجراءات التنظيميّة والتعليمات التي تهدف إلى حماية سرّية معلومات العملاء وعملياتهم المصرفية. ويجب التنسيق مسبقاً مع مؤسسة النقد العربي السعودي في حال اتفقت البنوك ومحلات الصرافة على التعاون أو تبادل المعلومات فيما بينهم.

2.7.3 International Cooperation

In recognition for the need to cooperate with the international community in combating and preventing money laundering, terrorist financing and other financial crimes, Saudi Arabia has included provisions for this matter in its AML Law, taking into consideration the agreed conventions and reciprocity agreements. In accordance with the Saudi AML Law allowing, after prior coordination with SAMA, cooperation with international governmental authorities for cases involving money laundering and terrorist financing, any exchange of information with a foreign party whether another bank (affiliation, branch, correspondent) or a foreign governmental authority. for strictly follow the legal and regulatory procedures that aim to protect customer confidentiality and banking secrecy.

٣,٧,٢ التعاون الدولي

تضمن نظام مكافحة غسل الاموال أحكاماً للتعاون مع الدول الأخرى وذلك اعترافاً من المملكة العربيّة السعوديّة وإقراراً منها بالحاجة للتعاون مع المجتمع الدولي في مكافحة ومنع أنشطة غسل الأموال وتمويل الإرهاب والجرائم المالية الأخرى مع مراعاة المعاهدات المُبرمة واتفاقيات المعاملة بالمثل. وذلك وفقاً لنظام مكافحة غسل الأموال اللتين تسمحان بالتعاون مع السلطات الحكومية الدولية فيما يتعلّق بالحالات التي تشمل غسل الأموال وتمويل الإرهاب، عليه فانه يمكن تبادل المعلومات مع طرف أجنبيّ سواء مع بنك آخر (تابع، فرع، بنك مراسل) أو سلطة حكوميّة أجنبيّة بعد التنسيق المسبق مع مؤسسة النقد العربي السعودي وذلك لضمان التقييد بشكل تام بالإجراءات التنظيميّة والتعليمات التي تهدف إلى حماية سرّية معلومات العملاء وعملياتهم المصرفية.

3. Money Laundering and Terrorist Financing

٣. غسل الأموال وتمويل الإرهاب

3.1 Money Laundering

١,٣ غسل الأموال

3.1.1 Definition of Money Laundering

The Saudi AML Law defines money laundering as: any actual or attempted act aims at concealing or camouflaging the nature or illegally or illegitimately earned property to make it look as proceeds from legal sources. The AML Law's Implanting Regulations states the underlying crimes relating to money laundering.

FATF defines money laundering as: the process by which proceeds from criminal activities are disguised to conceal their illegal origin in order to legitimize the illegal gains thereof.

Criminal activities, such as drug trade, illegal arms sales, smuggling, human trafficking, prostitution, corruption, embezzlement, and other activities of organized crimes, tend to generate large amounts of profits for the individuals or groups carrying out such acts. By using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds.

The United Nations Vienna Convention (1988) and the United Nations Palermo Convention (2000) provisions describe money laundering as the process by which proceeds from a criminal activity are disguised to conceal their illicit origin, and may encompass three distinct, alternative acts:

1. The exchange or transfer of proceeds, knowing that they are a result of a crime;
2. The concealment or disguise of the real nature, source, location, placement, movement or ownership of or rights with respect to proceeds, knowing that they are a result of a crime;
3. The acquisition, possession or use of proceeds, knowing, at the time of the receipt, that they are a result of a crime.

١,١,٣ تعريف غسل الأموال

عرّف نظام مكافحة غسل الأموال عملية غسل الأموال بأنها ارتكاب أي فعل أو الشروع فيه يقصد من ورائه إخفاء أو تمويه أصل حقيقة أموال مكتسبة خلافاً للشرع أو النظام وجعلها تبدو كأنها مشروعة المصدر. وتنصّ اللائحة التنفيذية لنظام مكافحة غسل الأموال على الجرائم الضمنيّة المتعلّقة بغسل الأموال.

وتعرّف مجموعة العمل المالي (فاتف) غسل الأموال كعمليّة إخفاء العائدات من الأنشطة الإجراميّة من أجل تمويه أصلها غير المشروع بغرض إضفاء الشرعية على الأرباح غير القانونيّة من الجريمة.

فالأنشطة الإجراميّة، مثل الاتّجار بالمخدّرات، وبيع الأسلحة غير المشروع، وعمليّات التهريب، والاتّجار بالبشر، والدعارة، والفساد، والاختلاس، والأنشطة الأخرى للجرائم المنظّمة تؤدي إلى إدرار مبالغ كبيرة من الأرباح للأفراد أو المجموعات التي تقوم بالعمل الجنائي ويخاطر المجرمون عند استخدام الأموال مباشرة من هذه المصادر غير المشروعة خشية لفت انتباه السلطات للنشاط الإجرامي الذي أدى للحصول على هذه المبالغ وتعريض أنفسهم للمحاكمة الجنائيّة. وكذلك من أجل الاستفادة بحريّة من حصيلة جريمتهم يقومون بإخفاء المصدر غير المشروع لهذه الأموال.

وتصف أحكام اتفاقيّة الأمم المتّحدة – فيينا (١٩٨٨م) واتفاقيّة الأمم المتّحدة – باليرمو (٢٠٠٠م) غسل الأموال كعمليّة يتمّ بموجبها إخفاء المتحصلات من الأنشطة الإجرامية بغرض حجب أصلها غير المشروع، وقد تشمل ثلاثة أفعال أساسية ومختلفة :

١. التغيير والتحويل، مع العلم بان هذه العوائد هي حصيلة جريمة.
٢. إخفاء أو حجب الطبيعة الحقيقيّة، أو المصدر، أو الموقع، أو إحلال، أو النقل، أو الملكيّة أو الحقوق فيما يتعلّق بالعوائد، مع العلم بان هذه العوائد هي حصيلة جريمة .
٣. حيازة، أو امتلاك أو استخدام العوائد ، علماً أنه في وقت استلامها كانت هذه العوائد حصيلة جريمة.

3.1.2 Processes of Money Laundering

There are three stages of money laundering, explained as

٢,١,٣ عمليّات غسل الأموال

تمر عمليات غسل الأموال بثلاث مراحل وذلك وفقاً للتالي:

follows:

1. Placement
Placement involves the introduction of illegally obtained funds into the financial system, usually through banks. This is achieved through cash deposits, purchase of monetary instruments for cash, currency exchange, purchase of shares or insurance contracts, check cashing services, retail (through cash purchases), and smuggling of cash between countries.

2. Layering
The stage II of money laundering is the layering, which usually consists of a series of transactions, through transferring and movement of funds, designed to conceal their origin. This may involve sending wire transfers to other banks, purchase and sale of investments, financial instruments, and insurance contracts, fraudulent investments or trade schemes, and the like.

3. Integration
The last stage is integration, which involves the re-entering of the funds into the legitimate economy. This is accomplished through the purchase of assets, shares/ financial assets, or luxury goods, and investment in real estate or projects.

١.الإيداع/ الإحلال
يشمل الإيداع عملية إدخال الأموال الناتجة من مصدر غير مشروع إلى النظام المالي ويتم ذلك عادة عبر البنوك ويتحقق هذا الأمر من خلال الإيداعات النقدية، وشراء الأوراق المالية مقابل النقد، وتبديل العملات، وشراء الأسهم أو عقود التأمين، وخدمات صرف الشيكات، والبيع بالتجزئة (من خلال عمليّات الشراء النقديّة)، وتهريب النقد بين الدول.

٢.التغطية
المرحلة الثانية لعملية غسل الأموال هي عملية التغطية والتي تتألّف عادة من مجموعة من العمليات، من خلال تحويل ونقل الأموال بغرض إخفاء أصل الأموال، وقد يشمل هذا الأمر إرسال حوالات برقيّة (تلكس) إلى بنوك أخرى، وشراء وبيع الاستثمارات والأوراق الماليّة وعقود التأمين، والاستثمارات الوهمية أو الخطط التجاريّة وما إلى ذلك.

٣.الدمج
المرحلة الأخيرة هي الدمج وتشمل إعادة إدخال الأموال مرة أخرى في النظام الإقتصادي المشروع ، ويتم هذا الأمر من خلال شراء الأصول والأسهم / الأصول الماليّة أو السلع الثمينة والاستثمار في العقارات أو المشاريع.

3.2 Terrorist Financing

٢,٣ تمويل الإرهاب

3.2.1 Definition of Terrorist Financing

١,٢,٣ تعريف تمويل الإرهاب

The Article 1 of the Saudi AML Law defines criminal activity as: any activity sanctioned by Shariah or law including the financing of terrorism, terrorist acts and terrorist organizations. The Article 2 of the AML Law's Implementing Regulations 2.1 describes "financing terrorism, terrorist acts and terrorist organizations includes even funds obtained from legitimate sources".

The International Convention for the Suppression of the Financing of Terrorism adopted by the UN in 1999 describes terrorist financing as follows:

"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex.
b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

Saudi Arabia is committed to all relevant UN Security Council's resolutions directed towards combating terrorist financing and criminalizes financing of terrorism, terrorist acts and terrorist organizations.

SAMA requires to all banks, money exchangers, and foreign banks' branches operating in the Kingdom strict compliance with the resolutions of the UN and recommendations of the FATF. If a bank or money exchanger has any reason to believe that an individual, commercial institution or organization is, by any means, directly or indirectly, providing or collecting funds in the knowledge that such funds will be used for illegal purposes, it must refrain from entering into

تعرّف المادّة الاولى من نظام مكافحة غسل الأموال النشاط الإجرامي على انه أيّ نشاط يشكل جريمة معاقب عليها وفق الشرع أو النظام بما في ذلك تمويل الإرهاب، والأعمال الإرهابيّة والمنظّمات الإرهابيّة. وتصف اللائحة التنفيذية ١,٢ من المادّة ٢ من نظام مكافحة غسل الأموال " تمويل الإرهاب والأعمال الإرهابية والمنظّمات الإرهابيّة، من انه يشمل الاموال المتأتية من المصادر المشروعة ".

وان الاتفاقيّة الدوليّة للأمم المتّحدة لعام ١٩٩٩م لقمع تمويل الإرهاب تصف تمويل الإرهاب كما يلي:

"أيّ شخص يرتكب جريمة ضمن معنى هذه الاتفاقيّة في حال كان هذا الشخص، وبواسطة أيّة وسيلة، مباشرة أو غير مباشرة، **بصورة غير قانونية أو بملء ارادته** ، يقدّم أو يجمع أموالاً بنيّة أن تستخدم أو بمعرفة مُسبقة بانها ستستخدم، كلياً أو جزئياً من أجل تنفيذ :

أ. عمل يشكّل جريمة ضمن النطاق وكما هو معرّف في إحدى المعاهدات المذكورة في الملحق.
ب. أيّ عمل آخر يُراد به التسبب بوفاة أو إصابة خطرة تلحق بمواطن مدنيّ، أو أيّ شخص آخر لا يشارك على نحو فعّال في الأعمال العدائيّة في حالة النزاع المسلّح، عندما يكون الغرض من هذا العمل، بطبيعته أو معناه، إرهاب السكان، أو إرغام حكومة أو منظّمة دوليّة على القيام أو الامتناع عن القيام بأيّ فعل".

وتلتزم المملكة العربيّة السعوديّة بجميع قرارات الامم المتحدة–مجلس الأمن– الخاصة بمكافحة تمويل الإرهاب، كما قد قامت بتجريم تمويل الإرهاب، والأعمال الإرهابيّة والمنظّمات الإرهابيّة.

وتطلب مؤسسة النقد العربي السعودي من كافة البنوك ومحلات الصرافة وفروع البنوك الاجنبية العاملة بالمملكة الالتزام التام بتطبيق القرارات الصادرة من الأمم المتّحدة والتوصيات الصادرة من مجموعة العمل المالي (فاتف). وفي حال توفر لبنك أومحل صرافة أيّ سبب ليظنّ بان فرداً، أو مؤسسة تجاريّة أو منظّمة ما تقدم أو تجمع الأموال بواسطة أيّة وسيلة مباشرة أو غير مباشرة وهي تعرف ان هذه الأموال ستستخدم لأغراض غير شرعيّة يتوجّب عليهم الامتناع عن الدخول في التعامل مع هؤلاء مع إبلاغ السلطات المختصّة بشأنها.

transactions and report to the competent authorities on such case.

3.2.2 Processes of Terrorist Financing

The techniques and methods used to finance terrorism are essentially similar to those used to conceal the sources of money laundering and its uses, however, the main differences between the two are that (a) small amounts are often required to commit individual terrorist acts, making it difficult to track terrorist funds; and (b) terrorists can be financed by legitimately obtained funds, making it difficult to identify the stage at which legitimate funds become terrorist funds. Terrorists may derive their finance from a variety of sources, often combining both lawful and unlawful funding. The forms of financing can be categorized into the following types:

1. Financial Support
This finance could be in the form of charitable donations, community solicitation and other fund raising initiatives, which may come from entities or individuals.

2. Illegitimate Sources
This finance is often derived from criminal activities such as money laundering, fraud and other financial crimes.

3. Legitimate Source
This form of finance may fully or partially originate from legitimate business activity.

3.3 Typologies

The various techniques or methods used to launder money or finance terrorism are generally referred to as *typologies.* A typological study is a useful tool to examine in depth a particular issue of concern to provide a view and knowledge on emerging interconnected risks and how they should be addressed.

FATF and MENA-FATF regularly issue studies relating to typologies of money laundering and terrorist financing. They can be found on

www.fatf.org/pages

http://www.menafatf.org/images/UploadFiles/ML-TF_Trends_and_Indicators_in_the_MENA_Region_Arabic.pdf

SAMA also issued circulation No. 5403/MAT/12263 dated 6/3/1432H. to all financial institutions, , regarding typologies of money laundering and terrorist financing. Banks and money exchangers should update their systems with the new typologies applicable to their businesses. The following are examples of the typologies relating to money laundering and terrorist financing:

٢,٢,٣ عمليّات تمويل الإرهاب

تتشابه الأساليب والتقنيّات المستخدمة لتمويل الإرهاب بشكل أساسيّ مع التقنيّات المتّبعة لإخفاء مصادر واستخدامات عمليات غسل الأموال، ولكنّ الفروق الرئيسيّة بين العمليتين هي انه (أ) غالبًا ما تكون الأموال المطلوبة لاقتراف الأعمال الإرهابيّة الفرديّة صغيرة، مما يصعّب عملية تتبع أموال العمليات الإرهابيّة و(ب) من الممكن تمويل الإرهابيين باستخدام أموال يتمّ الحصول عليها بشكل مشروع وبالتالي يكون من الصعب تحديد المرحلة التي أصبحت فيها الأموال المشروعة أموالاً إرهابيّة يستطيع الإرهابيون الحصول على مداخيلهم من مجموعة منوّعة من مصادر غالباً ما تجمع بين التمويل من مصادر مشروعة ومن مصادر غير مشروعة, ويمكن تصنيف مصادر تمويل الإرهاب كما يلي:

١. الدعم المالي

يمكن أن يأتي هذا التمويل على شكل تبرعات خيريّة، وطلب مساعدات أفراد المجتمع أو من خلال إستخدام وسائل أخرى لجمع الأموال من المؤسسات أو الأفراد.

٢. المصادر غير المشروعة

غالباً ما يأتي هذا التمويل من خلال ممارسة الأنشطة الإجرامية مثل غسل الأموال، والاحتيال والجرائم الماليّة الأخرى.

٣. المصادر المشروعة

قد يأتي هذا النوع من التمويل بشكل كامل أو جزئي من خلال ممارسة انشطة أو أعمال مشروعة.

٣,٣ الأنماط

يشار إلى التقنيّات أو الطرق المختلفة المستخدمة لغسل الأموال أو تمويل الإرهاب عادةً بعبارة الأنماط (typologies). وتعد دراسة الأنماط أداة مفيدة للبحث بعمق في مسألة معينة بقصد تقديم رؤية ومعرفة عن المخاطر المتداخلة الناشئة وكيفية معالجتها.

تصدر مجموعة العمل المالي (فاتف) ومجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (مينا فاتف) بشكل منتظم دراسات متعلّقة بأنماط غسل الأموال وتمويل الإرهاب ويمكن الرجوع إليها على الرابط:

www.fatf.org/pages

http://www.menafatf.org/images/UploadFiles/ML-TF_Trends_and_Indicators_in_the_MENA_Region_Arabic.pdf

كما أصدرت مؤسسة النقد العربي السعودي ورقة متعلقة بأنماط غسل الأموال وتمويل الإرهاب تم تعميمها برقم ١٢٢٦٣/م أت/٥٤٠٣ وتاريخ ١٤٣٢/٣/٦هـ، ويتعيّن على البنوك ومحلات الصرافة تحديث أنظمتهم لتتواكب مع الأنماط الجديدة التي تنطبق على أعمالهم. فيما يلي أمثلة عن الأنماط المتعلّقة بغسل الأموال وتمويل الإرهاب:

- **Alternative remittance services (hawala, hundi, etc.)**: Informal mechanisms rely on trust-based networks for remitting funds. They often work in parallel with the traditional banking sector but they are illegal. They are exploited by money launderers and terrorist financiers to move funds without detection and to obscure the identity of those controlling them.
- **Structuring (smurfing)**: A method involving multiple transactions (deposits, withdrawals, transfers), executed often by various people and high volumes of small transactions and sometimes various accounts to avoid financial institutions' obligations of threshold reporting.
- **Currency exchanges**: Used to assist with smuggling funds to another jurisdiction, exploit low reporting obligations on currency exchange houses, and minimize risk of detection, e.g., purchasing of travelers checks to transport funds to another country.
- **Cash couriers/ currency smuggling**: Concealed movement of currency across borders to avoid transaction/ cash reporting measures.
- **Use of credit cards, checks, etc.**: Used as instruments to access funds held in bank accounts, often in another jurisdiction.
- **Purchase of valuable assets (e.g., real estate, vehicles, shares, etc.)**: Criminal proceeds are invested in high-value negotiable goods, taking advantage of reduced reporting requirements to obscure the source of such proceeds.
- **Use of wire transfers**: To electronically transfer funds between banks and often to another jurisdiction to avoid detection and confiscation.
- **Trade-based money laundering**: Usually involves invoice manipulation and uses trade finance methods and commodities to avoid financial transparency laws and regulations.
- **Abuse of non-profit organizations**: Non-profit organizations may be misused to raise funds for terrorist purposes, obscure the source and nature of funds and to distribute funds to finance terrorism.
- **Investment in capital markets**: Obscuring the source of criminal activities' proceeds by purchasing negotiable instruments, often exploiting relatively low reporting requirements.
- **Mingling (business investment)**: A key step in money laundering involves combining proceeds of crime with legitimate business funds to obscure their source.
- **Use of shell companies/ corporations**: A technique used to obscure the identity of persons controlling funds and to exploit relatively low reporting requirements.
- **Use of offshore businesses, including trust company service providers**: To obscure the identity of people controlling funds and to move monies away from monitoring measures of domestic authorities.
- **Use of legal arrangements, brokers, trustees, or third parties, etc**: To obscure the identity of persons controlling illicit funds.
- **Use of foreign bank accounts**: To move funds away from measures of domestic authorities and obscure the identity of persons controlling illicit funds.
- **Identity fraud/ false identity**: Used to obscure identity of those involved in money laundering and terrorist financing.
- **Use professional services (lawyers, accountants, brokers, etc.)**: To obscure identity of beneficiaries and the source of illicit funds. This may also include corrupt professionals who offer 'specialist' money laundering services to criminals.

- **خدمات التحويل البديلة (الحوالة، السند الإذني، إلخ):** وسائل تحويل غير رسميّة ترتكز على شبكات تعتمد على الثقة لتحويل الأموال. وغالباً ما تعمل بشكل متوازٍ مع القطاع البنكي التقليديّ لكنّها غير نظامية ويستغلها غاسلو الأموال ومموّلو الإرهاب لنقل الأموال بدون أن يتم تتبعها ولإخفاء هوية المسيطرين على تلك الأموال.
- **التنظيم (التركيب او التجزئة):**طريقة تشمل عمليات عديدة (الإيداعات، والسحوبات، والتحويلات)، وغالباً ما تضم مجموعة من الأشخاص، وأعداداً هائلةً من العمليات الصغيرة القيمة وأحياناً حسابات متعددة تتم بهذا الشكل لتفادي التزامات المؤسسات المالية بالتبليغ عن العمليات المالية التي تتجاوز حدود معينة.
- **تبديل العملة:** تستخدم هذه الطريقة للمساعدة في عمليّة تهريب الأموال بين الدول أو لاستغلال ضعف التزامات التبليغ المتبعة من مؤسسات تبديل العملات وللتقليل من مخاطر الكشف عن هذه العمليات، ومن أمثلتها شراء الشيكات السياحية لنقل الأموال بين الدول.
- **ناقلو النقد/ تهريب العملة:** نقل العملات بالطريقة الخفية عبر الحدود لتفادي إجراءات الافصاح عن العمليات/ المال النقدي.
- **استخدام بطاقات الائتمان، والشيكات، إلخ:** تستخدم كأدوات للوصول إلى الأموال المودعة في حسابات البنوك، والتي تكون غالباً في دولة أخرى.
- **شراء أصول قيّمة (مثل العقارات، والسيّارات، والأسهم، إلخ):** تستثمر عائدات الأنشطة الإجراميّة في شراء السلع العالية القيمة والتي يمكن تداولها بسهولة للاستفادة من قلة متطلّبات التبليغ مما يخفي مصدر هذه العائدات.
- **استخدام التحويلات البرقيّة (التلكس):** تحويل الأموال إلكترونياً بين البنوك وغالباً ما يكون ذلك إلى دولة أخرى لتفادي الاكتشاف والمصادرة.
- **غسل الأموال عن طريق التجارة:** يشمل عادة التلاعب بالفواتير واستخدام طرق التمويل التجاريّ والسلع لتفادي قوانين وأنظمة الشفافيّة الماليّة.
- **الاستخدام السيء للمنظمات غير الهادفة للربح:** قد يُساء استخدامها لجمع الأموال لأغراض إرهابيّة، وإخفاء مصدر وطبيعة الأموال ولتوزيع الأموال لتمويل الإرهاب.
- **الاستثمار في أسواق المال:** إخفاء مصدر عائدات الأنشطة الإجرامية من خلال شراء السندات القابلة للتداول، وغالباً ما يتمّ استغلال متطلّبات التبليغ الأقل نسبياً.
- **الخلط (الاستثمار في الأعمال):** خطوة رئيسيّة في عملية غسل الأموال تشمل الجمع بين عائدات الأنشطة الإجرامية والأموال التجاريّة المشروعة لإخفاء مصدر الأموال.
- **استخدام المؤسسات والشركات الصورية:** أسلوبٌ لإخفاء هويّة الأشخاص الذين يتحكمون بالأموال, ولاستغلال متطلبات التبليغ الأقل نسبياً.
- **استخدام الأعمال الخارجية أوفشور، بما في ذلك الجهات المقدمة لخدمات الأمانة:** لإخفاء هويّة الأشخاص المتحكمين بالأموال وإبعاد الأموال عن إجراءات المراقبة المعمول بها من السلطات المحليّة.
- **استخدام الترتيبات القانونية والوسطاء والأمناء أو أطراف ثالثة، إلخ :** لإخفاء هويّة الأشخاص الذين يتحكمون بالأموال غير المشروعة.
- **استخدام حسابات البنوك الخارجيّة :** لإبعاد الأموال عن إجراءات التي تطالها السلطات المحليّة وإخفاء هويّة الأشخاص الذين يتحكمون بالأموال غير المشروعة.
- **سرقة الهويّة / الهويّات غير الصحيحة (المزورة):** تستخدم لإخفاء هوية الأشخاص المتورّطين في القيام بعمليات غسل الأموال وتمويل الإرهاب.
- **استخدام الخدمات المهنية (المحامون، والمحاسبون، والوسطاء، إلخ) :** لإخفاء هويّة المستفيدين ومصدر الأموال غير المشروعة قد تشمل أيضاً أصحاب المهن المستقلة الفاسدين والذين يقدّمون خدمات "متخصصة" في مجال غسل الأموال للمجرمين.

4. Policies and Standards

4.1 Risk-Based Approach

Banks and money exchangers shall adopt a risk-based approach in designing their Anti-Money Laundering (AML) and Combating Terrorist Financing (CTF) programs to ensure that measures used to mitigate money laundering and terrorist financing are commensurate to the risks identified in their organizations. This will also allow resources to be allocated in the most efficient ways. Some of the benefits of utilizing the risk-based approach is verification of levels of due diligence measures by banks or money exchangers as follows:

1. Allowing banks and money exchangers to differentiate between risks of customers in a particular business by focusing on the highest risks of them, thus improving the overall outcome of the process;
2. While establishing minimum standards, allowing a bank or money exchanger to apply its own approach to systems, controls and arrangements in particular circumstances, thus allowing more flexibility as risks evolve; and
3. Helping to create the best management of risks and cost effective system.

It should be born in mind that application of a risk-based approach does not release any type of business or customers from verification of (KYC) basic requirements or from meeting customers due diligence (CDD) requirements used to restrain transactions of money laundering and terrorist financing.

A risk-based approach will serve to balance the burden placed on banks and money exchangers and on their customers, along with a realistic assessment of risks of business being used in money laundering or terrorist financing by focusing efforts on areas where they are needed and have the most impact.

Banks and money exchangers may face some challenges that must be considered while implementing the risk-based approach. These challenges should be regarded as offering opportunities to implement a more effective system in combating activities of money laundering and terrorist financing. Some of these challenges can be summarized as follows:

1. Risk Assessment Methodology: Identifying appropriate information to conduct a precise risk analysis and overall assessment.
2. Judgmental Decisions: Greater needs for more specialist staff capable of making sound decisions regarding identification and evaluation of risks.
3. Transitional Costs: Costs relating to transition from prescription method to risk based method.
4. Cautious Factor: Regulatory entity's response to diversity of methods of doing business.

The risk-based approach requires certain actions to be taken in assessing the best cost effective methods and their appropriateness to the management and in mitigation the risks of money laundering and terrorist financing faced by a bank. These actions are:

1. Identifying risks of money laundering and terrorist financing that are relevant to the bank or money exchanger to ensure a well-built foundation for the approach used and well-understood risks.

٤. السياسات والمعايير

١,٤ الأسلوب المرتكز على المخاطر

يجب على البنوك ومحلات الصرافة اعتماد الأسلوب المرتكز على المخاطر عند تصميم ووضع البرامج الخاصة بمكافحة غسل الأموال وتمويل الإرهاب لضمان تماشي الإجراءات المستخدمة للحد من حالات غسل الأموال وتمويل الإرهاب مع المخاطر المحددة في هذه البنوك ومحلات الصرافة. كما يساعد هذا الأسلوب في توجيه الموارد بالطرق الأكثر فاعلية. ومن بعض منافع استخدام الأسلوب المرتكز على أساس المخاطر تحقيق البنوك أو محلات الصرافة مستوى متقدم بمجال التعرف على عملائهم وتطبيق إجراءات العناية الواجبة بشان تعاملاتهم وذلك على النحو التالي:

١. السماح للبنوك ومحلات الصرافة بالتفريق بين مخاطر العملاء في أعمال محدّدة عبر التركيز على أكثرهم خطورة وبالتالي تحسين المردود الإجمالي للعملية.
٢. السماح للبنك أو محل الصرافة عند وضع المعايير الدنيا بتطبيق أسلوبه الخاص على الأنظمة والضوابط والترتيبات في حال الظروف المحدّدة، وبالتالي السماح بمرونة أكبر عند تغير المخاطر.
٣. المساعدة في إنشاء أفضل إدارة للمخاطر ونظام فعّال من حيث التكاليف.

علماً أن تطبيق الإسلوب المرتكز على المخاطر لا يعنى أعفاء أي نوع من الاعمال أو العملاء من إجراءات التحقق من المتطلبات الأساسية لمعرفة العملاء (KYC) أو من القيام بمتطلبات العناية الواجبة (CDD) والمستخدمة للحد من حالات غسل الأموال وتمويل الإرهاب.

كما يساعد الأسلوب المرتكز على المخاطر في موازنة العبء الملقى على البنوك ومحلات الصرافة وعلى عملائهم مع تقييم واقعيّ لمخاطر الأعمال المستخدمة فيما يتعلّق بغسل الأموال أو تمويل الإرهاب عبر تركيز الجهود على المجالات التي تحتاجها والتي يكون لها التأثير الأكبر.

وربما تواجه البنوك ومحلات الصرافة بعض التحديات التي يجب أخذها في الاعتبار لذا يجب أن تؤخذ هذه التحديات كفرصة لتنفيذ نظام أكثر فاعلية في مكافحة أنشطة غسل الأموال وتمويل الإرهاب ويمكن تلخيص بعض هذه التحديات كالتالي:

١. منهجيّة تقييم المخاطر: تحديد المعلومات المناسبة لإجراء تحليل مخاطر دقيق وتقييم كلي.
٢. القرارات التقديرية: تزداد الحاجة لوجود موظّفين متخصصين لديهم القدرة على اتّخاذ القرارات المناسبة والصحيحة بشأن تحديد المخاطر وتقييمها.
٣. التكاليف الانتقاليّة: التكاليف المتعلّقة بالانتقال من أسلوب الملاحظة إلى الأسلوب المرتكز على المخاطر.
٤. عامل الحيطة: استجابة الجهة التنظيميّة لتنوّع طرق ممارسة العمل.

ويتطلب الأسلوب المرتكز على المخاطر اتخاذ بعض الإجراءات في تقييم أفضل الطرق من حيث فاعلية التكلفة وتناسبها للإدارة وتخفيف مخاطر غسل الأموال وتمويل الإرهاب التي يواجهها البنك وهذه الإجراءات هي:

١. تحديد مخاطر غسل الأموال وتمويل الإرهاب ذات الصلة بالبنك أو محل الصرافة من أجل ضمان الأساس الصحيح للأسلوب المتبع والتأكد من أن المخاطر مفهومة جيّداً.
٢. تقييم المخاطر المحدّدة من قبل البنوك أو محلات الصرافة من جميع الأوجه التالية:
   أ. العملاء.
   ب. المنتجات والخدمات.

ج. قنوات تقديم الخدمة.

د. المنطقة الجغرافيّة.

وقد تختلف الأهميّة المعطاة إلى أوجه المخاطر المذكورة أعلاه عند تقييم المخاطر الإجمالية لغسل الأموال وتمويل الإرهاب من بنك أو محل صرافة إلى آخر، وذلك بحسب الظروف الخاصّة بكل بنك أو محل صرافة وبالتالي سيكون على كل بنك أو محل صرافة أن يقوم بتحديد مقياسه الخاص لمختلف المخاطر.

٣. إنشاء وتنفيذ الضوابط الرقابية للتخفيف من هذه المخاطر.

٤. مراقبة وتطوير فعالية تشغيل عمل هذه الضوابط.

٥. تسجيل ما تم إنجازه بشكل مناسب مع تفسير الأسباب والمبررات.

كما يمكن أن يساعد الأسلوب المرتكز على المخاطر في التعرّف على النشاطات المشتبه بها على النحو الآتي:

١. توجيه الموارد الإضافية نحو المجالات التي حدّدها البنك أو محل الصرافة بأنها عالية المخاطر.

٢. يعتمد مدى التوسع في عملية التحقيق بحسب المخاطر المحددة.

٣. يستخدم البنك ومحل الصرافة المعلومات التي تقدمها السلطات للتعرّف على النشاط المشتبه به.

٤. يجب على البنك أومحل الصرافة إجراء تقييم دوري لمدى ملائمة نظامه الخاص بالتعرّف على العمليات المشتبه بها والإبلاغ عنها.

كما تصدر مجموعة العمل المالي (فاتف) بشكل منتظم دراسات متعلّقة بالأسلوب المرتكز على المخاطر ويمكن الاطلاع عليها على الرابط التالي:
http://www.fatf-gafi.org/dataoecd/45/1/43249256.pdf

2. Assessing the risks identified by bank's or money exchanger from all the following aspects:
   a. Customers;
   b. Products and services;
   c. Service delivery channels;
   d. Geographical area of operation.

   The weight given to the above risk aspects in assessing the overall risk of money laundering and terrorist financing may vary from one bank or money exchanger to another, depending on their respective circumstances. Consequently, each bank or money exchanger will have to make its own standard of assessing the varieties of risk.
3. Establishing and implementing monitoring controls to mitigate these assessed risks.
4. Monitoring and improving the effective operation of such controls.
5. Recording appropriately what has been done and explaining the reasons and rationale.

The Risk-based approach may contribute to identifying suspicious activities as follows:

1. Directing additional resources towards areas identified by a bank or money exchanger as high-risk areas.
2. Expansion in investigation process is dependent on the risks identified.
3. A bank or money exchanger shall use information provided by authorities to identify and report suspicious activities.
4. A bank or money exchanger must periodically assess the adequacy of its identification system of suspicious transactions and reporting thereof.

FATF regularly issues studies on risk-based approach. Such studies can be viewed at:
http://www.fatf-gafi.org/dataoecd/45/1/43249256.pdf

١,١,٤ تقييم مخاطر الأعمال

يجب على البنوك ومحلات الصرافة إجراء عمليّة تقييم مخاطر الأعمال المذكورة سابقاً وتوثيقها مع تحديث هذا التقييم سنوياً لتحديد التغييرات التي طرت على مجال أعمالهم (مثل الهيكل التنظيمي) وعملائهم والدول التي يرتبط بها عملاؤهم ومنتجاتهم وخدماتهم وطرق تقديم هذه المنتجات والخدمات. ويجب على البنوك ومحلات الصرافة وضع برامج الالتزام الخاصة بهم لمكافحة غسل الأموال وتمويل الإرهاب بناءً على نتائج تحديد المخاطر عند تقييم مخاطر الأعمال. كما يجب على البنك أومحل الصرافة إثبات انه قد أخذ في الاعتبار تعرّضه لمخاطر غسل الأموال وتمويل الإرهاب لأجل الوصول إلى تقييم مناسب من خلال الأخذ في الاعتبار ما يلي:

١. تغطية جميع المخاطر التي يسببها غسل الأموال وتمويل الإرهاب والمتعلّقة بالأعمال المختلفة داخل البنك أومحل الصرافة.

٢. مراعاة العوامل التنظيميّة التي قد تزيد مستوى التعرّض لمخاطرغسل الأموال وتمويل الإرهاب، مثل حجم الأعمال والقدرة الاستيعابية وتفويض الاخرين بادارة الحسابات.

٣. مراعاة طبيعة الأعمال وحجمها وتعقيداتها، وتنوّع العمليّات (بما في ذلك التنوع الجغرافي)، وحجم ومقدار العمليات، ودرجة المخاطر المتّصلة بكلّ مجالات العمل.

٤. نوع وطبيعة العملاء وأعمالهم والتركيز على المعرف منها بانه/بانها ذات مخاطر عالية (السياسيين، الجمعيات الخيرية، محلات الذهب والمجوهرات،..الخ).

٥. مراعاة وجود أيّة مخاطر إضافيّة ناتجة عن الدول الأخرى التي يتّصل بها العملاء (بما في ذلك الوسطاء ومقدمي الخدمات). وذلك لتأثر المخاطر التي يتعرض لها البنك بسبب العلاقات ذات الصلة مع دول أخرى بالعديد من العوامل مثل المستويات العالية للجريمة المنظّمة، والتعرّض المتزايد للرشوة والفساد ونطاقات العمل غير الفعالة لمنع واكتشاف جرائم غسل الأموال وتمويل الإرهاب.

4.1.1 Business Risk Assessment

Banks and money exchangers shall conduct and document the above business risk assessment and update this assessment on an annual basis to identify changes in their business areas (e.g. organizational structure), their customers and the jurisdictions with which customers are connected, and their products and services and how they should be delivered. Banks and money exchangers shall build their AML/CTF compliance programs based on the conclusions of the business risk assessment. To achieve an adequate assessment, banks or money exchangers shall consider the possibility of exposure to money laundering and terrorist financing risks by:

1. Covering all risks posed by money laundering and terrorist financing relating to different businesses within the bank or money exchanger.
2. Considering organizational factors that may increase the level of exposure to the risk of money laundering and terrorist financing, e.g., business volumes, capacity issues, and authorisation of others for account management.
3. Considering the nature, scale and complexity of business, the diversity of their operations (including geographical diversity), the volume and size of their transactions, and the level of risk associated with all areas of their business.
4. Considering the type and nature of customers and their businesses, focusing on the ones defined as high risk (political persons, charity associations, jewelry shops, etc. ..).
5. Considering any additional risks posed by the jurisdictions with which customers (including brokers and

service providers) are connected. Risks exposed to by banks in their relationships with other jurisdictions are sensitive to a number of factors such as high levels of organized crime, increased vulnerabilities to bribe and corruption, and inadequate scopes of work for preventing and detecting money laundering and financing of terrorism.

6. Considering the characteristics of the products and services provided by banks or money exchangers and assessing the associated vulnerabilities posed by each product and service, including service delivery methods. For example:
   a. Current accounts and money transfers, which are more vulnerable because they allow funds to be transferred to and from third parties, including cash transactions.
   b. The use of third parties such as a group entities, service providers and brokers to obtain information about the customer.
   c. Brokers' combined accounts are more vulnerable because of the anonymity of the source of funds due to the mingling of assets or funds belonging to several customers by the broker.
   d. Conversely, products that do not permit third party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable.
7. Considering how they establish and deliver products and services to their customers as risks are likely to be greater when relationships are established remotely (non-face-to-face), or when transactions are controlled remotely by the customer (straight-through processing of transactions).
8. Recording, updating and retaining their business risk assessment.

٦. مراعاة خصائص المنتجات والخدمات التي يقدّمها البنك أو محل الصرافة وتقييم نقاط الضعف من ناحية التعرض لعمليات غسل الأموال وتمويل الارهاب لدى كلّ منتج وخدمة، بما في ذلك طرق تقديم الخدمة. والتي من أمثلتها:
   أ. الحسابات الجارية وعلاقة التحويل المالي وهي أكثر عُرضة لانها تسمح بحركة الأموال من وإلى أطراف ثالثة بما في ذلك العمليات النقديّة.
   ب. استخدام أطراف ثالثة مثل مجموعة من المؤسسات ومقدمي الخدمات والوسطاء للحصول على معلومات عن العميل.
   ج. تعتبر الحسابات التجميعية للوسطاء اكثر ضُعفاً، بسبب تجاهل مصدر الأموال نتيجة دمج الأصول أو الأموال التي تعود لعملاء عديدين من خلال الوسيط.
   د. وعلى نحو معاكس تعتبر المنتجات التي لا تسمح بعمليّات تحويل الاموال من وإلى طرف ثالث أو حيث تكون عملية الاسترداد مسموحاً بها فقط إلى الحساب ليتم منه تمويل الاستثمار أقل تعرضاً لعمليات غسل الأموال وتمويل الارهاب.
٧. مراعاة كيفية تأسيس وتقديم المنتجات والخدمات إلى العملاء. كون ان المخاطر تكون عادة أكبر عند تأسيس العلاقات عن بُعد (ليس وجهاً لوجه)، أو عند إمكانية التحكم بها عن بُعد من قبل العميل (التنفيذ المباشر للعمليات).
٨. تسجيل، وتحديث والحفاظ على تقييم مخاطر الأعمال.

4.2 AML / CTF Compliance Programs

٢,٤ برامج الالتزام الخاصة بمكافحة غسل الأموال وتمويل الإرهاب

The Saudi AML Law requires financial institutions to develop appropriate AML/CTF programs which should include, as a minimum, the following:

1. Internal AML/CTF policies, measures and controls and informing the staff thereof including ID verification and due diligence measures, maintaining records, monitoring of transaction and compliance with the requirement of reporting suspicious transactions.
2. Appropriate arrangements for compliance management and appointing a compliance officer to ensure compliance with AML/CTF requirements. He should work independently, have the power to communicate with a superior management level, and have the right to view customers' identity data, due diligence information and other related transaction records.
3. Establishing an independent accounting and auditing unit provided with adequate resources for testing compliance with such measures, policies and controls in accordance with the risk-based approach.
4. Developing ongoing training programs for all employees and the specialized to keep them informed of new laws, instructions and any updates in the area of combating money laundering to upgrade their skills in identifying such operations, their patterns and the method of combating them.
5. Application of test measures to ensure availability of highly efficient standards for appointment of employees.

Therefore, banks and money exchangers should prepare adequate AML/CTF compliance programs, basically covering the following elements:

يقضي نظام مكافحة غسل الأموال بأن على المؤسسات المالية وضع برامج لمكافحة غسل الأموال وتمويل الإرهاب والتي يجب أن تتضمن على الأقل ما يلي:

١. سياسات وإجراءات وضوابط داخلية لمكافحة غسل الأموال وتمويل الإرهاب، وإبلاغ موظفيها بها تتضمن إجراءات التحقق من هوية العملاء وإجراءات العناية الواجبة، والاحتفاظ بالسجلات، ومراقبة العمليات، والالتزام بالإبلاغ عن العمليات المشبوهة.
٢. ترتيبات ملائمة لإدارة الالتزام وتعيين مسئولاً عن الالتزام بمعايير مكافحة غسل الأموال وتمويل الإرهاب على مستوى الإدارة ويعمل بصورة مستقلة وله الحق بالاتصال بمستوى إداري أعلى وحق الإطلاع في الوقت المناسب على بيانات هوية العملاء ومعلومات العناية الواجبة، وعلى سجلات العمليات الأخرى ذات الصلة.
٣. إنشاء وحدة تدقيق ومراجعة مستقلة ومزودة بموارد كافية لاختبار الالتزام بهذه الإجراءات والسياسات والضوابط وفقاً لمعيار معدل المخاطر.
٤. إعداد برامج تدريبية مستمرة لعامة الموظفين وللمختصين لإحاطتهم بالأنظمة والتعليمات المتعلقة بمكافحة غسل الأموال وبالمستجدات في هذا المجال، بما يرفع من قدراتهم في التعرف على تلك العمليات وأنماطها وكيفية التصدي لها.
٥. تطبيق إجراءات للفحص لضمان وجود معايير كفاءة عالية عند تعيين الموظفين.

وبالتالي يجب أن تعمل البنوك ومحلات الصرافة على إعداد برامج مناسبة لمكافحة غسل الأموال وتمويل الإرهاب تغطّي بشكل أساسيّ العناصر التالية:

١. وضع عناصر تفصيلية لبرنامج الالتزام كما هو مذكور أعلاه وخطط واستراتيجيات البنوك أو محلات الصرافة لضمان الالتزام بتطبيق سياساتهم وإجراءاتهم المكتوبة لتغطّي بشكل فعّال متطلّبات مكافحة غسل الأموال وتمويل الإرهاب.

1. Setting out, as mentioned above, detailed elements for the compliance program and plans and strategies by banks or money exchangers for ensuring compliance with their written policies and measures to effectively cover AML and CTF requirements.
2. Including review plan and self-assessment to monitor effectiveness of AML and CTF controls.
3. Detailing assigned responsibilities and identifying actions to be taken during the year in addition to any pending correction actions stemming from accounting and auditing operations.
4. Including appropriate staff awareness programs and training plans over the year.
5. Preparing and revising the compliance program on an annual basis to ensure its effectiveness and inclusion of the changing typologies of money laundering and terrorist financing risks.

The program should also include what has been achieved in the risk-based approach and the rationale of such achievement. Therefore, each bank or money exchanger should appropriately tailor policies and measures of AML/CTF program to identify:

1. How a bank or money exchanger assesses threats and risks it exposed to in money laundering or terrorist financing.
2. How a bank or money exchanger applies appropriate law or takes appropriate actions based on risk assessment, including due diligence requirements.
3. How a bank or money exchanger monitors enhancement of the effectiveness of its system and procedures.
4. Reporting process to senior management on performance of control measures.

٢. ان تشتمل على خطة مراجعة وتقييم ذاتي لمراقبة فاعليّة ضوابط مكافحة غسل الأموال وتمويل الإرهاب.
٣. تفصيل المسؤليات وتحديد الإجراءات التي يجب اتخاذها خلال السنة بالإضافة إلى أية إجراءات تصحيحيّة معلقة تنتج عن عمليّات التدقيق والمراجعة.
٤. برامج توعية الموظّفين وخطط التدريب خلال السنة.
٥. يجب إعداد ومراجعة برنامج الالتزام على أساس سنوي، وذلك لضمان فاعليته وللتأكد من تضمنه للأنماط المتغيرة لمخاطر غسل الأموال وتمويل الإرهاب.

كما يجب أن يتضمن البرنامج ما تم إنجازه مع المبررات وذلك فيما يتعلّق بالأسلوب المرتكز على المخاطر. وبالتالي يجب أن يعدُ كلّ بنك أو محل صرافة بحسب ما هو مناسباً سياسات وإجراءات برنامج مكافحة غسل الأموال وتمويل الإرهاب لتحديد ما يلي :

١. كيفية تقييّم المخاوف والمخاطر التي يتعرض لها البنك أو محل الصرافة فيما يتعلّق بغسل الأموال أو تمويل الإرهاب.
٢. كيفية قيام البنك أو محل الصرافة بتطبيق أو تنفيذ النظام والإجراءات المناسبة بما في ذلك متطلبات العناية الواجبة بناءً على تقييم المخاطر.
٣. كيفية قيام البنك أو محل الصرافة بمراقبة تحسين فعالية النظام وإجراءاته.
٤. عملية رفع التقارير للإدارة العليا فيما يتعلّق بعمل إجراءات المراقبة الخاصّة به.

4.3 Know Your Customer Principle (KYC)

٣,٤ مبدأ إعرف عميلك

The KYC principle is intended to enable a bank or money exchanger to have an appropriate perspective that it knows the true identity of each customer with an appropriate degree of confidence and knows the types of business and transactions the customer is likely to undertake. In order to follow that principle, measures of banks and money exchangers should include the following arrangements:

1. Identification and verification of all permanent and casual customers and beneficiaries owner on a continuous basis and in accordance with the Rules Governing the Opening of Bank Accounts and the General Operational Guidelines.
2. Identification and verification of beneficiaries owner of all transactions executed by customers to an extent that ensures their perfect understanding.
3. Assessing risks connected with different types of customers and taking proper measures for enhancing requirements of identification and verification of customers or beneficiaries owner.
4. Adopting proper measures that ensure updating requirements of identification and verification of customers and beneficiaries owner on a continuous basis.
5. Following up changes in the identity of customers and beneficiaries owner and taking the necessary decision on their impact on control and supervision requirements.
6. Making records of identification of customers and beneficiaries owner available to the compliance officer

إن الغرض من تطبيق مبدأ إعرف عميلك هو تمكين البنك أو محل الصرافة من تكوين تصور مناسب بأنه يعرف الهويّة الحقيقيّة لكلّ عميل مع درجة مناسبة من الثقة وأنه يعرف أنواع الأعمال والعمليات التي يحتمل أن يقوم بها العميل مع البنك أو محل الصرافة ، ويجب أن تشمل إجراءات البنك ومحل الصرافة اتخاذ التدابير التالية من أجل تحقيق ذلك المبداء:

١. التعرف والتحقق من هويّة جميع العملاء الدائمين والعرضيين والمستفيدين الحقيقيين بصفة مستمرة ، وبما يتوافق مع ما تضمنته قواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها.
٢. التعرف والتحقق من هوية المستفيدين الحقيقين لكافة العمليات التي يجريها العملاء وبالمستوى الذي يحقق الفهم والمعرفة التامة عنهما.
٣. تقييم المخاطر المرتبطة بمختلف أنواع العملاء وإتخاذ الإجراءات المناسبة بشأن تعزيز متطلبات التعرف والتحقق من هوية العملاء أو المستفيدين الحقيقين من تعاملاتهم.
٤. اتخاذ الإجراءات الكفيلة بتحديث متطلبات التعرف والتحقق من هوية جميع العملاء والمستفيدين الحقيقين بصفة مستمرة.
٥. متابعة التغيرات في هوية العملاء والمستفيدين الحقيقين واتخاذ اللازم بشأن تأثيرها على متطلبات الرقابة والإشراف.
٦. ينبغي أن تكون سجلات تحديد هوية العملاء والمستفيدين الحقيقين متاحة للمسئول عن اللإلتزام بمعايير مكافحة غسل الأموال وتمويل الإرهاب والمسئولين المختصين ذوي الصلة.
٧. أن يتم التحقق من هوية العملاء والمستفيدين الحقيقين من مصادر موثوقة ومستقلة.

entrusted with ensuring compliance with AML/CTF requirements and to other relevant officials.
7. Verification of the identity of customers and beneficiaries owner from authenticated and autonomous sources.

4.3.1 Customer Identification Process

The Saudi AML Law and its Implementing Regulations require financial institutions not to carry out any financial, commercial or similar operations under anonymous or fictitious names. Banks are also prohibited from opening or dealing with numbered accounts. Banks and money exchangers must verify the identity of the customer and beneficiaries owner depending on official documents provided at the start of dealing with such customer or upon concluding commercial transactions therewith in person or in proxy. Banks and money exchangers must further verify legal person's official documents that indicate the name of the entity, its address, names and addresses of its owners, managing directors, and any other relevant data.

Banks and money exchangers should , as a minimum, apply the following rules for appropriate identification of customers and beneficiaries owner:

1. Establishing valid identification by reference to proper and official documents provided for in the SAMA's Rules Governing the Opening of Bank Accounts and the General Operational Guidelines in Saudi Arabia.
2. At the outset of the relationship or account, obtaining a copy of the customer identification documents and verifying them against their original.
3. Obtaining SAMA approval for opening accounts or establishing relationships with non-residents, except with GCC citizens.
4. Not to open accounts for or establish relationships with any non-face-to-face customers (refer to SAMA's Rules Governing the Opening of Bank Accounts), and subject all accounts to interview and identity verification.
5. Identification is not limited to customers having accounts at the bank; it should also include those who benefit from other banking or financial services, such as credit cards, express remittances, large transfers/ transactions, foreign exchange transactions and safe deposit boxes. It should also cover owners, authorized signers, holders of powers of attorney, directors, trustees and partners.
6. Setting a systematic measure for identifying customers and not to establish any relationship or process any transaction until the personal or commercial valid identity of the individual or legal entity has been verified satisfactorily.
7. Obtaining customer personal information, such as name, address, signature, contact telephone numbers, occupation, source of funds/ income or wealth, and other information depending on the type of customer, as stated in the SAMA's Rules Governing the Opening of Bank Accounts.
8. Requesting from the customer to provide information about any existing bank accounts or relationships with other local banks, which should be followed up if suspicions arise.
9. Conducting further due diligence and efforts if there are doubts about the integrity or accuracy of previously obtained customer identification data and, in such case, re-verifying the identity of the customer and re-assessing the relationship.
10. Not to accept any transactions from walk-in customers, with the exception of transactions stated in the SAMA's Rules Governing the Opening of Bank Accounts.

11. No new accounts, business relationships or transactions

١,٣,٤ عمليّة تحديد هويّة العملاء

يقتضي نظام مكافحة غسل الأموال ولائحته التنفيذية بأن لا تقوم المؤسسات الماليّة بأيّة عمليّات ماليّة أو تجاريّة أو غيرها باستخدام أسماء مجهولة أو وهمية. كما يُحضر على البنوك فتح أو التعامل بحسابات مرقّمة. ويتوجّب على البنوك ومحلات الصرافة التحقق من هوية العميل والمستفيد الحقيقي، بناءً على المستندات الرسميّة المقدمة عند بداية التعامل مع العميل أو عند إنجاز معاملات تجاريّة له شخصياً أو بالوكالة. كما يتوجّب أيضاً على البنوك ومحلات الصرافة التحقق من المستندات الرسميّة للشخص الاعتباري والتي تبين اسم المؤسسة, أو الشركة، وعنوانها واسماء المالكين، والأعضاء المنتدبين أو أية بيانات أخرى ذات صلة.

ويجب على البنوك ومحلات الصرافة تطبيق القواعد التالية كحدّ أدنى لتحديد هويّة العملاء والمستفيدين الحقيقيين:

١. التحديد الصحيح للهوية بالإشارة إلى المستندات الرسميّة الصحيحة والمقبولة وفقاً للقواعد الخاصة بفتح الحسابات الصادرة عن مؤسسة النقد العربي السعودي.
٢. الحصول على نسخة من مستندات تحدد هوية العميل, والتأكد من مطابقتها للمستندات الأصليّة عند بدء العلاقة أو فتح الحساب.
٣. الحصول على موافقة مؤسسة النقد العربي السعودي لفتح الحسابات أو تأسيس العلاقات للأشخاص غير المقيمين، باستثناء مواطني دول مجلس التعاون لدول الخليج العربية.
٤. عدم فتح حسابات أو تأسيس علاقات لعملاء لم تتم مقابلتهم وجهاً لوجه (راجع القواعد الخاصّة بفتح الحسابات الصادرة عن مؤسسة النقد العربي) وإخضاع جميع الحسابات للمقابلة والتحقق من هويّة العملاء.
٥. لا يقتصر التحقق من الهويّة على العملاء الذين يملكون حسابات في البنك بل يجب أن يشمل أيضاً أولئك الذين يستفيدون من خدمات مصرفية أو مالية أخرى، مثل بطاقات الائتمان، والتحويلات الماليّة السريعة، وعمليّات التحويل والعمليات بمبالغ كبيرة، وعمليات صرف وتبديل العملات الأجنبية, واستئجار خزائن الايداع، وكذلك يجب أن تشمل المالكين، والمفوضين بالتوقيع، وأصحاب الوكالات، والمدراء، والأمناء والشركاء.
٦. وضع إجراء منظّم لتحديد هويّة العملاء وعدم إنشاء أي علاقة أو تنفيذ عملية إلا بعد أن يتمّ تحديد الهويّة الصحيحة الشخصية أو التجارية للفرد أو الكيان القانوني مع التحقق منها بشكل مرضي.
٧. الحصول على معلومات شخصية عن العميل مثل اسمه، وعنوانه، وتوقيعه، وأرقام الهاتف، والمهنة، ومصدر الأموال/الدخل أو الثروة، ومعلومات أخرى بناءً على تصنيف العميل، كما ورد في القواعد الخاصّة بفتح الحسابات الصادرة عن مؤسسة النقد العربي السعودي.
٨. الطلب من العميل إعطاء معلومات عن أية حسابات مصرفية موجودة أو علاقات مع بنوك محليّة أخرى والتي يجب أن تتم متابعتها في حال الاشتباه بالعميل.
٩. بذل الجهود والعناية الواجبة في حال كانت هناك شكوك بشأن نزاهة أو صحة البيانات حول هوية العميل التي جرى الحصول عليها سابقاً، وفي هذه الحالة يتم التحقق من جديد من هويّة العميل وإعادة تقييم العلاقة.
١٠. عدم قبول أيّة عمليات من العملاء العابرين، باستثناء العمليات المنصوص عليها في تلك القواعد وبما يتوافق مع ما جاء بالقواعد الخاصّة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.
١١. عدم قبول أية حسابات جديدة أو علاقات أعمال أو عمليات ويجب تجميد أيّ حساب

should be accepted, and any freezing any existing account, business relationship or transaction when:

a. Identity of the customer cannot be verified;
b. Identity of the beneficial owner is not known; and/ or
c. Failure to obtain information on the purpose and nature of the relevant business.

موجود أو علاقة أعمال أو عمليات في حالة:

أ. عدم التمكن من التحقق من هويّة العميل.
ب. هويّة المستفيد الحقيقي غير معروفة ؛ و/أو
ج. الفشل في الحصول على معلومات بشأن الغرض وطبيعة الأعمال ذات العلاقة.

4.4 Customer Due Diligence (CDD)

٤,٤ العناية الواجبة للعملاء (CDD)

Application of due diligence means the effort made by banks and money exchangers to monitor financial transactions of customers and beneficiaries owner, ensure they understand them, and verify all business of customers, data required for opening bank accounts or establishing a banking relationship, and ensure their authenticity and clarity.

Instructions require banks and money exchangers operating in the Kingdom to apply basic due diligence measures on all permanent and casual customers and beneficiaries owner. Such measures shall be continuous and consistent with the risk level of business and transactions of customers as follows:

1. Following up activities of financial transactions and their consistency with the purpose provided upon opening of the account.
2. Due diligence is required upon establishing a business relationship, execution of casual transactions over the single or aggregated disclosed limits or being suspected of their connection with money laundering or terrorist financing, regardless of exemptions or limits specified for amounts of transactions, or if there are doubts about the accuracy or adequacy of previously obtained customer identification data.
3. Verifying any person (natural or legal) acting on behalf of the customer and ensuring validity of such action.
4. Identifying persons (natural or legal) who have control on the customer.
5. Increasing level of due diligence with respect of those customers business relationships that are determined to be of higher risk. This may be the result of the customer's business activity, ownership structure, volume or types of potential or actual transactions, including those transactions involving higher risk countries or defined by the applicable law or instructions as posing higher risk, such as correspondent banking relationships and PEPs.
6. Simple CDD measures and arrangements are not acceptable whenever there are suspicious transactions of money laundering or terrorist financing
7. The CDD requirements may be reduced with respect to low risk relationships, such as:
    a. Companies listed in the Capital Market which are subject to regulatory disclosure requirements.
    b. Other banks or financial institutions (domestic or foreign) working within the AML/CTF system in consistency with the FATF Recommendations.
    c. Individuals whose main source of funds is a salary, pension or social assistance from identified and appropriate sources and where transactions are commensurate with the source of funds.
    d. Transactions involving small amounts or particular types of transactions.

Thus, when designing and implementing controls related to due diligence to manage and mitigate the identified risks, according to the risk-based approach, banks and money exchangers should follow the following steps:

يقصد بتطبيق إجراءات العناية الواجبة هنا قيام البنوك ومحلات الصرافة بمراقبة التعاملات المالية للعملاء والمستفيدين الحقيقين لهم والتأكد من فهمها والتحقق من جميع الأعمال التي يزاولونها وكذلك من بيانات فتح الحساب أو إنشاء العلاقة المصرفية والإطمئنان بأنها موثوقة وواضحة.

وتقتضي التعليمات أن تقوم البنوك ومحلات الصرافة العاملة في المملكة بتطبيق إجراءات العناية الواجبة الأساسية على جميع العملاء الدائمين والعرضيين وبما يشمل المستفيدين الحقيقين وأن تكون تلك الإجراءات مستمرة ومتوائمة مع درجة المخاطر المرتبطة بالأعمال والعمليات التي يجريها العملاء وذلك على النحو التالي:

١. متابعة نشاط التعاملات المالية وتوائمها مع ما تم تقديمة من معلومات من العملاء حين فتح الحساب.
٢. يتطلب تنفيذ إجراءات العناية الواجبة حين إنشاء علاقة العمل وعند إجراء عمليات عارضة تفوق الحدود التي تم الافصاح عنها للمرة الواحدة أو مجمعة مع بعضها وكذلك حينما تكون هنالك حالة أشتباه بارتباطها في حدوث عملية غسل أموال أو تمويل إرهاب بغض النظر عن الإعفاءات أو الحدود المعينة لمبالغ العمليات، أو في حال وجود شكوك بشأن دقة أو كفاية البيانات التي تم الحصول عليها مسبقاً حين تحديد هوية العملاء.
٣. التحقق من ما إذا كان أي شخص (طبيعي أو إعتباري) يتصرف نيابة عن العميل والتأكد من قانونية ذلك.
٤. تحديد الأشخاص (الطبيعيين والأعتباريين) الذي لهم ملكية أو سيطرة على العميل.
٥. ينبغي تعزيز إجراء العناية الواجبة في حال العملاء وعلاقات العمل مرتفعة المخاطر، وقد يكون ذلك نتيجة نشاط العميل التجاري، أوهيكل الملكيّة، أو حجم أو أنواع العمليات المتوقّعة أو الفعليّة بما في ذلك تلك العمليات التي تشمل دولاً مصنفة بأنها ذات مخاطر عالية أو العمليات التي يتم تحديدها بموجب النظام او التعليمات المطبقة على أنها تشكّل مصدر خطر عالٍ كعلاقات البنوك المراسلة والأشخاص المعرفين سياسياً.
٦. لا تقبل إجراءات وتدابير العناية الواجبة البسيطة في حال الشك في وقوع عمليات غسل أموال أو تمويل إرهاب.
٧. إمكانية تخفيف متطلبات العناية الواجبة على العلاقات التي يتم تصنيفها ضمن الفئات ذات المخاطر المنخفضة، ومنها على سبيل المثال :
    أ. الشركات المدرجة في سوق الاوراق المالية والتي تخضع لمتطّلبات الإفصاح التنظيميّة.
    ب. البنوك أو المؤسسات الماليّة الأخرى (المحلّية أو الأجنبية) والتي تعمل ضمن نظام مكافحة غسل الأموال أو تمويل الإرهاب بما يتوافق مع توصيات مجموعة العمل المالي (فاتف).
    ج. الأفراد الذين يمثّل مصدر دخلهم الرئيسيّ الراتب، أو رواتب التقاعد أو الإعانات الاجتماعيّة من مصادر معروفة ومناسبة وحيث يتناسب مستوى العمليات مع مصدر الأموال.
    د. العمليات ذات المبالغ الصغيرة أو أنواع محددة من العمليات.

لذا فانه عند اعداد وتنفيذ ظوابط للإدارة حول العناية الواجبة والحد من المخاطر المحددة بحسب الأسلوب المرتكز على المخاطر يجب على البنوك ومحلات الصرافة اتباع الخطوات التالية :

1. Managing and mitigating the identified risks by developing measures to verify the customer's identity; collect additional information about the customer and monitor the customer's transactions.
2. Establishing control measures for:
   a. Introducing a customer identification program, actions of which vary appropriately with the customer's risks in the area of money laundering and terrorist financing.
   b. Requiring the quality of evidence, documents, technologies, and third-party guarantees to be of a specific standard.
   c. Obtaining additional information on the customer. Such information should be appropriate to the customer's assessed money laundering and terrorist financing risks.
   d. Monitoring customer's transactions and activities.
3. Establishing a customer identification program that is graduated to reflect risks, involving:
   a. A basic database, held in which all data on customers.
   b. Basic verification requirements for all customers.
   c. More extensive due diligence on acceptance of higher risk customers.
   d. Specific basic measures for identity verification of low risk customers and products.
   e. Monitoring the customer's activities and transactions based on the risk assessed.
4. Investigation into the customer's source of funds and wealth for higher-risk customers.
5. Developing monitoring guidelines for high risk customers versus low risk customers.

١. إدارة المخاطر المعروفة والحد منها بحيث يطوّر البنك أو محل الصرافة الإجراءات للتحقق من هويّة العميل وجمع معلومات إضافية عنه ومراقبة عملياته.

٢. وضع إجراءات مراقبة من أجل:

أ. تأسيس برنامج لتحديد هويّة العميل تتنوّع إجراءاته بما يتلائم مع مخاطر العميل فيما يتعلق بغسل الأموال وتمويل الإرهاب.

ب. أن تكون نوعيّة الدلائل (الاثباتات)، والمستندات واالتقنيات وضمانات الطرف الثالث ذات معيار محدّد.

ج. الحصول على معلومات إضافيّة عن العميل، حيث تكون متناسبة مع المخاطر المحددة له بالنسبة لغسل الأموال وتمويل الإرهاب.

د. مراقبة عمليات وأنشطة العميل.

٣. وضع برنامج لتحديد هويّة العميل مقسّم إلى مراحل ليعكس المخاطر ويشمل:

أ. قاعدة معلومات أساسية تحفظ جميع ما يتعلّق بالعملاء.

ب. متطلّبات تحقُق أساسية لجميع العملاء.

ج. إجراءات عناية واجبة أكثر شمولاً لقبول العملاء ذوي المخاطر العالية.

د. إجراءات أساسية محددة للتحقق من الهويّة للعملاء والمنتجات ذوي المخاطر المنخفضة.

هـ. مراقبة نشاط ومعاملات العميل وفقاً لفئة المخاطر التي ينتمي إليها.

٤. معرفة مصدر أموال العميل وثروته بالنسبة إلى العملاء الذين تم تصنيفهم من ذوي المخاطر العالية.

٥. وضع إرشادات لمراقبة العملاء ذوي المخاطر العالية مقابل أولئك ذوي المخاطر المنخفضة.

4.4. 1 Beneficiaries owner (Natural & Legal)

Banks and money exchangers should verify the beneficiaries owner of all accounts and relationships and should conduct due diligence on all final beneficiaries owner in accordance with the following:

1. Natural Persons

When the account or relationship is in the name of an individual, the bank or money exchanger should determine whether the account is used in the interest of the client in whose name it was recorded and for the purpose for which it was opened. If doubt exists, the bank should establish the capacity in which and on whose behalf the customer is acting. Identity of the beneficiaries owner, should be established to the bank's or money exchanger's satisfaction by reference to official identity documents. Banks and money exchangers should also ensure that any person claims to act on behalf of the customer, is so authorized, and identify and verify the identity of that person.

2. Legal Persons / Companies

Where the customer is a legal person/ company or establishment, the bank or money exchanger should understand the ownership structure of the establishment or the company sufficiently to determine the provider of funds, principal owners of the shares and those who ultimately own or have control over the assets such as the directors, based on the memorandum of association of the establishment/company and those with the power to give direction to the directors of the company in accordance with the company's articles of association.

With regards to a joint stock company, the bank or money exchanger should establish the identity of all shareholders or

١,٤,٤ المستفيدون الحقيقيون (الطبيعيون والاعتباريون)

يجب أن تقوم البنوك ومحلات الصرافة بالتحقق من المستفيدين الحقيقيين من الحسابات أو العلاقات والقيام بإجراءات العناية الواجبة اتجاه جميع المستفيدين النهائين وذلك وفقاً لما يلي:

١. الأشخاص الطبيعيون

عندما يكون الحساب أو العلاقة باسم فرد يتعيّن على البنك ومحل الصرافه التأكد من أن الحساب يستخدم لمصلحة الفرد الذي سجل بأسمة شخصياً وللغرض الذي فتح من أجلة (تحديد ما إذا كان العميل يتصرّف لمصلحته شخصياً) . وفي حال وجود شك بان العميل يتصرف لمصلحة اخرين فإنه يجب على البنك ومحل الصرافة أن يحدد الصفة التي يتصرف بها العميل أو بالنيابة عنه. وتحدد هوية المستفيد الحقيقي على نحو يرضي البنك أو محل الصرافة استناداً إلى مستندات الهويّة الرسميّة. كما يتعيّن على البنوك ومؤسسات الصرافة أن يضمنوا بان أيّ شخص يزعم التصرّف بالنيابة عن العميل هو مخوّل وأن يحدّدوا ويتحققوا من هويّة ذلك الشخص.

٢. الأشخاص الاعتباريون / الشركات

حيث يكون العميل شخصاً اعتبارياً/مؤسسة أو شركة، يتعيّن على البنك أو محل الصرافة أن يفهم هيكل ملكية المؤسسة أو الشركة بما يكفي لتحديد مقدم الأموال، والمالكين الرئيسيين للأسهم وأولئك الذين يملكون بشكل أساسي أو يتمتعون بالسيطرة على الأصول، أي كالمدراء أستناداً إلى عقد المؤسسة أو الشركة أو أولئك الذين يتمتعون بالصلاحية والسلطة لإعطاء التوجيهات إلى مدراء الشركة.

وفيما يتعلق بالشركة المساهمة، فإنه يجب على البنك أو محل الصرافة تحديد هويّة جميع المساهمين أو المستفيدين الحقيقين الذين يملكون نسبة ٥ % وأكثر من أسهم الشركة ويجب أن تحصل البنوك ومحلات الصرافة على دليل مثبّت بوثائق للكيان القانوني ووجوده بالإضافة إلى هويّة أصحاب الحق بمن فيهم الأشخاص الطبيعيين الذين يملكون الكيان أو يتحكمون به

beneficiaries owner who own 5% and more of the company's shares. Banks and money exchangers should obtain documentary evidence of the legal entity and existence along with the identity cards of stakeholders including the actual natural persons owning or controlling the entity in accordance with the Rules for Opening Bank Account and General Rules for their operation issued by SAMA.

In all the above cases, if a customer states that he/she is acting on his/her own, then a declaration to this effect, whether as a separate document or as a part of the account opening agreement, should be obtained from the customer, as follows:

a. For new customers: at the time of opening an account, establishing a relationship or conducting a significant transaction;
b. For existing customers: whenever there is a suspicion that the account, relationship or transaction is being used for a different or illegal purpose, thus requiring more information from the customer during the mandatory continuous updation of customer information, as per the Rules Governing the Opening of Bank Accounts by SAMA.

وفقاً لقواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها الصادرة من مؤسسة النقد العربي السعودي.

وفي جميع الحالات أعلاه، في حال ذكر المالك بانه/ها يتصرّف عن نفسه/ها، عندئذ يجب الحصول من العميل على إقرار بهذا الخصوص، سواء كمستند منفصل أو كجزء من اتفاقيّة فتح الحساب، وذلك على النحو التالي:

أ. للعملاء الجدد : في وقت فتح حساب و/او أنشاء علاقة أو حين إجراء معاملة مهمّة .
ب. للعملاء الموجودين :متى كان هناك شكّ بان الحساب، أو العلاقة أو المعاملة قد استخدمت لغرض مختلف أو غير شرعيّ، عندئذ يقتضي الأمر طلب معلومات إضافيّة من العميل وذلك من خلال متطلب التحديث المستمر الإلزامي لمعلومات العميل، وفقاً لقواعد فتح الحسابات الصادرة من مؤسسة النقد العربي السعودي.

4.4.2 Customer & Transaction Profiling

Banks and money exchangers should have a process in place to capture sufficient information about customers, and their anticipated use of their products and services, that will allow to develop a customer profile of expected activity to provide a basis for recognizing unusual and higher risk activities and transactions, which may indicate money laundering or terrorist financing. The information should be obtained at the establishment of a relationship or opening of an account and prepared for all types of relationships, including accounts and credit cards.

The extent and nature of the information details depend on the different types of customers (individual, corporation, etc.) and the different levels of risk resulting from the customer's relationship with the bank or money exchanger. Higher risk relationships, accounts and transactions will require greater scrutiny than lower risk ones.

The information should be kept up-to-date and monitoring of activity and transactions should be undertaken throughout the course of the relationship to ensure that the activity or transaction being conducted is consistent with the bank's or money exchanger's knowledge of the customer. Customer Profiles and Transaction Profiles should be reviewed and updated continuously whenever there is a suspicion of illegal transactions or activities.

1. Customer Profile

A customer profile is a means of collecting detailed information on a customer or an account/ relationship. Depending on the type of the customer, profiling will include basic information such as owners' names (including beneficial owners), partners, shareholders (except for minor shareholders of a joint stock company, holding less than 5%), authorized signers, power of attorney holders, etc.; customers' addresses including phone numbers, postal and street/ location address, e-mail, fax, etc.; purpose and the intended nature of business relationship, information of the business activities, financial information, capital amount, source of funds, source of wealth, branches, countries and products dealing in, etc. At the discretion of the bank or money exchanger, this could be an automated process. Customer identification information and documents should be Remain continuously at customer profile.

٢,٤,٤ ملفات معلومات العملاء والعمليات

يجب أن تضع البنوك ومحلات الصرافة الإجراءات الكفيلة لجمع معلومات كافية عن العملاء وعن استخدامهم المتوقع لمنتجاتهم وخدماتهم، مما يسمح بوضع تصور عن نشاط العميل المتوقع والذي يشكل الأساس لمعرفة النشاطات والعمليات غير المعتادة وذات المخاطر العالية والتي قد تشير إلى عملية غسل أموال أو تمويل إرهاب. ويجب الحصول على المعلومات عند تأسيس العلاقة أو فتح الحساب وإعدادها لجميع أنواع العلاقات، بما في ذلك الحسابات وبطاقات الائتمان.

ويتوقف مدى تفاصيل المعلومات وطبيعتها على التصنيفات المختلفة للعملاء (الأفراد، والشركات، إلخ) والمستويات المختلفة للمخاطر الناتجة عن علاقة العميل مع البنك أو محل الصرافة وتتطلب العلاقات والحسابات والعمليات ذات المخاطر العالية تدقيقاً أكبر من تلك ذات المخاطر المنخفضة.

كما يجب أن يتم تحديث المعلومات باستمرار مع مراقبة النشاطات والعمليات طوال فترة التعامل لضمان أن النشاط أو العملية قد أجريت بما يتوافق مع ما يعرفة البنك أو محل الصرافة عن العميل. ويجب مراجعة المعلومات عن العميل وعن العمليات وتحديثها بصورة مستمرة في حالة الاشتباه بوجود عمليات أو أنشطة غير مشروعة.

١. ملف معلومات العملاء

ملف معلومات العميل يعني بجمع المعلومات المفصلة عن العميل أو الحساب أو العلاقة، وتختلف بناءً على تصنيف العميل بحيث يشمل الملف المعلومات الأساسية مثل أسماء المالكين (بمن فيهم المستفيدين الحقيقيين) والشركاء والمساهمين (باستثناء المساهمين الصغار في الشركات المساهمة، والذين يملكون نسبة تقل عن ٥%)، والمفوضين بالتوقيع وأصحاب الوكالات ..الخ؛ و كذلك عناوين العملاء بما في ذلك أرقام الهاتف والعنوان البريدي والسكني والبريد الإلكتروني والفاكس.. الخ ؛ بالاضافة لغرض وطبيعة علاقة العمل والمعلومات عن أنشطة الأعمال والمعلومات المالية ومبلغ رأس المال ومصدر الأموال ومصدر الثروة والفروع والبلدان والمنتجات.. الخ. ووفقاً لتقدير البنك أو محل الصرافة يمكن أن يتحقق ذلك بطريقة آلية. وأنه يجب الحفاظ على جميع المستندات والوثائق المتعلقة بتحديد الهوية في ملف العميل بصفة مستمرة.

2. Transaction Profile

A transaction profile should be prepared to capture the number of transactions expected to be used by a customer, and the value of transactions for an average month, for each product and service. Banks and money exchangers should develop a system using specialized software to provide automatic preparation of transaction profiles and detect unusual patterns of transactions and trends that may indicate suspicious activities that are not consistent with initial assessments or expectations. All efforts should be made to establish the source of funds to the bank's or money exchanger's satisfaction and the customer and transaction profiling methodology should assist in establishing source of funds.

Transaction profile is not required for employed/ payroll, pension and fixed-income individual accounts or relationships, whose source of funds and usage of account can be determined, provided the account or relationship is used for the intended purpose. However, for accounts and relationships used for business purpose and for high-risk accounts, an appropriate transaction profile based on risk assessment, should be prepared to include all types of products and services expected to be used by the customer in the account, during the period of a month, the number of expected transactions, and their estimated monetary value, especially for high-risk products/ services such as cash, transfers, etc. The transaction profile should be reviewed and updated continuously to establish continued consistency between the profile and the actual transactions. Major inconsistencies should be investigated.

Banks and money exchangers may prepare a transaction profile on the basis of generic expected activity and transactions for certain types of products and services, however, for more complex products or services a tailored transaction profile will be necessary.

٢. ملف معلومات العمليات

يتم إعداد ملف معلومات العمليات لتحديد عدد العمليات المتوقّع تنفيذها من قبل العميل، ومتوسط مبلغ العمليات الشهري لكلّ منتج وخدمة. وعلى البنوك ومحلات الصرافة أن يطوّروا نظاماً يستخدم برامج متخصصة لتوفير عملية إعداد آلية لمعلومات العمليات مع اكتشاف الأساليب غير الاعتيادية للعمليات والأنماط التي قد تشير إلى أنشطة مشتبه بها والتي لا تنسجم مع عمليّات التقييم والتوقعات الأولية. ويجب أن تبذل إجراءات العناية الواجبة لتحديد مصدر الأموال على نحو مقبول للبنك أو محل الصرافة، كما يجب أن تساعد منهجية إعداد معلومات العميل والعمليات في تحديد مصدر الأموال.

لا يتطلب إعداد ملف معلومات عن العمليات لحسابات الرواتب، ورواتب التقاعد والحسابات الفرديّة أو العلاقات ذات الدخل الثابت والتي يمكن تحديد مصدر أموالها ووجهة استخدام الحساب شرط أن يُستخدم الحساب أو العلاقة للغرض المطلوب. وبالنسبة إلى الحسابات والعلاقات المستخدمة لأغراض الأعمال وللحسابات ذات المخاطر العالية فانه يجب إعداد معلومات مناسبة عن العمليات بناءً على تقييم المخاطر لتشمل جميع أنواع المنتجات والخدمات المتوقع أن يستخدمها العميل من خلال الحساب شهرياً، وعدد العمليات المتوقّعة، وتقدير قيمتها النقديّة، خصوصاً للمنتجات والخدمات ذات المخاطر العالية مثل النقد، وعمليّات التحويل المالي إلخ. ويجب أن تراجع معلومات العمليات وتحدّث بشكل مستمر لتحديد التوافق بين المعلومات والعمليات الفعليّة .كما يجب التحقيق في حالة الاختلافات الكبيرة بين العمليات المتوقعة والفعلية.

ويمكن أن تقوم البنوك ومحلات الصرافة بإعداد معلومات للعمليات على أساس النشاط والعمليات المتوقّعة الشاملة لبعض أنواع المنتجات والخدمات ، ولكن من الضروري عليها إعداد معلومات عن العمليات المرتبطة بالمنتجات أو الخدمات الأكثر تعقيداً.

4.4.3 Name Checking of Designated Persons

Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards compating terrorist financing. The UN, through its Security Council Resolutions (UNSCR 1267 of 1999 and successor resolutions), issues a listing of "designated persons", that are subject to certain sanction measures. Based on Saudi competent authorities' instructions, SAMA also notifies banks and money exchangers the names of "designated persons" and requires banks and money exchangers to implement the Saudi laws and the UN resolutions in this regard, including freezing of assets of individuals and entities who have been categorized as designated persons by UN or SAMA.

The following measures should be implemented by all banks and money exchangers:

1. Put in place an effective process to check all their customers' names (individuals, entities, beneficial owners, etc.) against the names that have been categorized as "designated persons" by SAMA and the UN, prior to opening account, establishing a relationship or conducting a transaction, especially for transfers in which case both the remitter's and the beneficiary's names should be checked.
2. In case a customer has been identified as being a "designated person", immediately freeze the account, relationship or the transaction and notify SAFIU and SAMA, giving full details of the account or transaction. The account or transaction should continue to be frozen

٣,٤,٤ التحقق من أسماء الأشخاص المدرجين على قوائم الأمم المتحدة او من قبل السلطات المحلية المختصة.

تلتزم المملكة العربيّة السعوديّة بجميع قرارات مجلس الأمن التابع للامم المتحدة ذات الصلة والخاصة بمكافحة تمويل الإرهاب .وتقوم الأمم المتّحدة ومن خلال قرارات مجلس الأمن (قرار مجلس الأمن رقم ١٢٦٧ للعام ١٩٩٩م والقرارات اللاحقة)، بإصدار قائمة "بالأشخاص المدرجين" الخاضعين لبعض الإجراءات العقابية. كما تقوم السلطات السعوديّة المختصّة، بإصدار تعليمات مماثلة ويتم تعميمها للبنوك ومحلات الصرافة عبر مؤسسة النقد العربي السعودي ويطلب من البنوك ومحلات الصرافة تنفيذ التعليمات الواردة بشأنها، بما في ذلك تجميد الأصول المالية للأفراد والكيانات المصنفين ضمن هذه التعليمات.

يجب أن تنفذ جميع البنوك ومحلات الصرافة التدابير التالية:

١. وضع إجراءات فعّالة للتحقق من جميع أسماء العملاء (الأفراد، والكيانات، والمستفيدين الحقيقيين، إلخ) مقابل الأسماء التي صُنّفت "كأشخاص مدرجين" من قبل السلطات المحلية والأمم المتّحدة قبل فتح الحساب, أو تأسيس العلاقة أو إجراء العملية، خصوصاً بالنسبة إلى عمليّات تحويل الأموال، وفي هذه الحالة يجب التحقق من أسماء كلّ من المحوّل والمستفيد.
٢. في حال ملاحظة وجود عميل مدرج في قوائم الامم المتحدة او التعليمات المحلية"، يتم فوراً تجميد الحساب، أوالعلاقة أو العملية وتبليغ وحدة التحريات الماليّة السعودية ومؤسسة النقد العربي السعودي، وإعطاء التفاصيل الكاملة عن الحساب أو العملية. ويستمرّ تجميد الحساب أو العملية إلى أن تعطي مؤسسة النقد العربي السعودي التوجيهات إلى البنك أو محل الصرافة.

until SAMA provides its direction to the bank or money exchanger.
3. For the purpose of continuous monitoring and suspicious should be reported to SAMA as per SAMA instructions.
4. Banks and money exchangers should also obtain the UN sanctions list from the following website: http://www.un.org/sc/committees/1267/consolist.shtml
5. Ensure to continuously check the UN List and keep it updated in their records.
6. Observe sanctions lists issued by other countries, check all transactions and transfers against these lists, to avoid potential legal conflicts with the banks' or money exchangers' customers or with banks or financial institutions in other countries, and to prevent the customers' transactions or transfers from being blocked.
7. In case an asset (account, relationship, transaction, etc.) has to be unfrozen because the designated person has been de-listed (removed from the sanctions list) by the UNSC, notify SAMA for approval to release the frozen assets of the customer. For names previously frozen at SAMA's instructions, SAMA will provide the bank or money exchanger with instructions to release the frozen assets.

٣. الاحتفاظ بقائمة محدّثة في قاعدة البيانات الخاصة بالكيانات والأشخاص المدرجين على هذه القوائم وذلك لأغراض المتابعة والقيام بإبلاغ مؤسسة النقد العربي السعودي بذلك حسب ما نصت التعليمات.

٤. القيام بتحديث بيانات المدرجين على قوائم الأمم المتحدة من خلال رجوع البنوك ومحلات الصرافة إلى قائمة العقوبات من موقع الأمم المتّحدة على شبكة الإنترنت على العنوان التالي: http://www.un.org/sc/committees/1267/consolist.shtml.

٥. التأكّد من المتابعة المستمرة لقائمة الأمم المتّحدة وإبقائها محدّثة في السجلات.

٦. مراقبة قوائم العقوبات الصادرة والمتوفرة عن الدول الأخرى والتحقق من جميع العمليات والتحويلات ومقارنتها مع هذه القوائم لتفادي أية اشكاليات قانونية محتملة قد تواجة البنك أو محل الصرافة من عملائه أو من قبل البنوك والمؤسسات المالية او أي جهات اخرى محلية كانت او دولية ، وكذلك لتجنب تجميد عمليات أو تحويلات العملاء.

٧. في حال توجّب رفع التجميد عن الأصول (حساب، علاقة، عملية، إلخ) كون الشخص المدرج على أو قوائم الأمم المتحدة او التعليمات المحلية قد تم رفع اسمه من القائمة (رفع عن قائمة العقوبات) من قبل مجلس الأمن فإنه يجب من البنوك ومحلات الصرافة إخطار مؤسسة النقد العربي السعودي للموافقة على رفع تجميد الأصول للعميل، وبالنسبة إلى الأسماء التي تم تجميد علاقاتها سابقاً بناءً على تعليمات مؤسسة النقد العربي السعودي سوف تقوم المؤسسة بإحاطة البنك أو محل الصرافة بالتعليمات المتعلقة برفع التجميد عن هذه الأصول.

4.5 Customer Risk Assessment

٤,٥ تقييم مخاطر العميل

Every relationship, account or transaction should be risk assessed from a money laundering and terrorist financing perspective. The complexity of the risk assessment process should be determined according to factors established by the business risk assessment.

The basis for the customer risk assessment should include factors such as:

1. High-risk jurisdictions/ countries, as defined by UN or the list of non-applying or inadequately applying countries of FATF's Recommendations, as explained in **Rule 5.2**;
2. High-risk businesses or customers, as explained in **Rule 4.6**;
3. High-risk products and services the customer may be dealing in, as explained in **Rule 5.1**;
4. The delivery method, such as the way the relationship is set up (directly/ face-to-face or indirectly) or the manner the products/ services are delivered to customers (e.g., internet, phone banking, etc.);
5. Other risk variables should also be considered when risk assessing a customer, as explained in **Rule 5.3**.

Customers to whom one of the above high-risk categories applies should be rated as high risk. However, the rating could be changed to a lower risk, provided the customer profiling is considered satisfactory and the rating change is justified and approved by a senior management. Such accounts classified as high risk should be subject to enhanced due diligence, closer monitoring and their risk statuses reviewed and updated continuously.

يجب أن تقيّم البنوك ومحلات الصرافة كلّ علاقة، أو حساب أو عملية من جهة مخاطر غسل الأموال وتمويل الإرهاب ويختلف مدى تعقيد عمليّة تقييم المخاطر بحسب العوامل الموضوعة في إجرّاءات تقييم مخاطر الأعمال ، وإن الأساس الذي ترتكز عليه عملية تقييم مخاطر العميل يجب أن تشمل على عدة عوامل منها على سبيل المثال مايلي :

١. الدول والمناطق المصنفة بأنها ذات مخاطر عالية، كما هي معرّفة من قبل الأمم المتّحدة أو مايصدر عن مجموعة العمل المالي (فاتف) بشان الدول التي لاتطبق أو لاتطبق بشكل كافي توصيات المجموعة كما هو موضح في القاعدة ٢,٥.

٢. الأعمال أو العملاء المصنفين بأنهم ذوي مخاطر عالية، كما هو موضح في القاعدة ٦,٤.

٣. المنتجات والخدمات المصنفة بأنها ذات مخاطر عالية التي يتعامل بها العميل، كما هي موضحة في القاعدة ١,٥.

٤. طريقة تقديم الخدمة، مثل طريقة تأسيس العلاقة (مباشرة، وجهًا لوجه أو بشكل غير مباشر) أو الطريقة التي تقدّم بها المنتجات والخدمات إلى العملاء (أي الإنترنت، والخدمات البنكيّة عبر الهاتف، إلخ) ؛

٥. متغيّرات المخاطر الأخرى التي يجب أن تؤخذ في الاعتبار عند تقييم مخاطر العميل، كما هو موضح في القاعدة ٣,٥.

ويجب أن يصنف العملاء الذين تنطبق عليهم إحدى الفئات أعلاه ضمن العملاء ذوي المخاطر العالية. ولكن قد يتغيّر التصنيف إلى فئة مخاطر أقل شرط أن تعتبر معلومات العميل مقبولة مع أخذ موافقة الإدارة العليا على التغيير في التصنيف وتبرير ذلك. ويجب بذل إجراءات العناية الواجبة على الحسابات المصنّفة بأنها ذات مخاطر عالية مع مراقبتها عن كثب ومراجعة وضع المخاطر لها وتحديثها بصفة مستمرة.

4.6 Customer Risks

٦,٤ مخاطر العميل

Customer risks are those that a particular customer or a category of customers may create due to their activities or behavior. Determining the potential money laundering or terrorist financing risks, to the extent that such risk can be identified, posed by a customer, or category of customers, is critical to the development of an overall risk-based framework. Based on its own criteria, a bank or money exchanger should determine whether a particular customer

ان مخاطر العميل هي التي قد تنشأ بسبب عميل محدّد أو فئة من العملاء بسبب أنشطتهم أو سلوكهم. وتعد عملية تحديد المخاطر المحتملة لغسل الأموال أو تمويل الإرهاب إلى المدى الذي يمكن فيه تحديد هذا الخطر الناتج عن عميل أو فئة من العملاء أساسية لتطوير إطار العمل العام على أساس المخاطر. ويحدد البنك أو محل الصرافة وفقاً للمقياس الخاص به ما إذا كان عميل محدّد يُسبب خطراً عالياً مع تحديد الأثر المحتمل لأيّة عوامل تقلل من هذه

poses a higher risk and the potential impact of any mitigating factors on that assessment. Banks and Money Exchagers shall classify all their customers based on risk . Application of risk variables may mitigate or aggravate the risk assessment.

The types of customers or relationships, and the potential risks they may pose, are described below:

الخطورة. وعلى البنوك وشركات الصرافة أن تقوم بتصنيف جميع عملائها وفقاً للمخاطر. علماً إن استخدام متغيرات المخاطر قد يخفف أو يُفاقم تقييم المخاطر.

وفيما يلي وصف لأنواع العملاء أو العلاقات والمخاطر المحتملة التي قد تنشاء عنها:

4.6.1 Individual Personal Accounts

These are accounts of individuals who open personal accounts for non-commercial and personal use. This category includes mainly employed/ payroll, fixed-income, pensioners, and self-employed individuals. Such personal accounts normally constitute a mass consumer business for many banks and generally do not involve close relationship management by a specific relationship manager. The sheer number of these accounts and the scale of transactions, usually small tickets, make the processes of monitoring demanding for banks.

While the AML risks for employed/ payroll individuals, pensioners and fixed income may be regarded as low, due to the fact that their sources of income can reasonably be established and are generally of smaller value, banks should be alert and exercise more due diligence for individuals who are self-employed. For these customers, it is difficult to reasonably determine their sources of income due to lack of any formal/ official supporting documents. In addition, self-employed individuals are relatively of higher risk due to their free-lancing activities. They may act as agents, on behalf of others, in real estate or other activities and receive a commission in return. However, they sometimes use their accounts as a transitory depository for their customers' funds, relating to a deal, pending final disposal. This poses additional AML risks for these accounts.

The following rules should apply as minimum standards for accounts of individual customers:

1. Employed/ Payroll, Pensioners & Fixed Income Individuals

These are individuals who are employed/ on payroll, on pension or with a regular fixed income and whose main source of income is derived from salary, pension, social benefits and the like, from an identified and appropriate source and whose transactions commensurate with the funds. Such customers are considered as low-risk and the following basic information is sufficient to constitute customer profile:

1. Obtaining proper and valid identification of the customer as stated in SAMA Account Opening Rules.
2. Ensuring customer's identification shows ID number, name, nationality and date/ place of birth.
3. Ensuring customer is not a PEP; otherwise extra due diligence is required as per Rule **4.5.4**.
4. Obtaining address and telephone/ mobile number. Also fax number and/ or e-mail address, if available.
5. Account is used for the purpose intended and not for commercial purpose; otherwise it should be treated as commercial account and additional information on the business activity obtained.
6. Taking reasonable measures to determine source of funds/ income; for example, using any one of the following means:
   a. Employment identification card for government, public and private sectors employees;
   b. Payroll slip, pension slip (for pensioners), electronic or paper salary certificate, or letter from employer;
   c. Copy of statement of another bank if salary is

١,٦,٤ الحسابات الشخصيّة الفردية

وهي فئة حسابات الأفراد الذين يقومون بفتح الحسابات الشخصيّة للاستخدام الخاص وليس للاستخدام التجاري وتشمل هذه الفئة حسابات الرواتب، والدخل الثابت, والمتقاعدين، والأفراد الذين يعملون لحسابهم. وتشكّل هذه الحسابات الفرديّة عادة أعمالاً كبيرة لقطاعات الأفراد في بنوك عديدة ولا تشمل عادة إدارة مباشرة أو وثيقة من قبل مدير علاقات محدد. وبسبب العدد الكبير لهذه الحسابات وحجم العمليات والتي تكون عادة بمبالغ صغيرة، تجعل من عمليّات المراقبة أمراً واجباً على البنوك.

ففي حين يمكن اعتبار مخاطر غسل الأموال للأفراد أصحاب حسابات الرواتب، والمتقاعدين وذوي الدخل الثابت منخفضة وذلك يعود لكون أن مصادر الدخل يمكن تحديدها بشكل معقول وهي عادة ذات قيمة صغيرة الا انه يجب أن تتنبه البنوك وتبذل إجراءات عناية واجبة بصورة أكبر بالنسبة إلى الأفراد الذين يعملون لحسابهم. وكذلك بالنسبة إلى هؤلاء العملاء الذين يصعب أن يُحدد بشكل معقول مصدر الدخل بسبب النقص في وجود المستندات الرسميّة والثبوتية. إضافة إلى ذلك يصنف الأفراد الذين يعملون لحسابهم انهم من ذوي المخاطر العالية بالنسبة إلى أنشطتهم المتعددة بحيث قد يعملون بصفة وكلاء بالنيابة عن آخرين في الأنشطة العقاريّة أو الأنشطة الأخرى ويحصلون على عمولة مقابل ذلك, ولكنّهم يستخدمون أحياناً حساباتهم للإيداع المؤقت لأموال عملائهم المتعلّقة بصفقة معينة إلى حين إتمامها. ويشكّل هذا الأمر خطورة إضافيّة بالنسبة لمخاطر مكافحة غسل الأموال لهذه الحسابات.

وتنطبق القواعد التالية كمعايير أساسية لحسابات العملاء الأفراد :

١. الأفراد أصحاب الرواتب، والمتقاعدين وذوي الدخل الثابت

وهم الأفراد أصحاب الرواتب، أو المتقاعدون أو ذو الدخل الثابت العادي والذي يأتي مصدر دخلهم الرئيسي من الراتب، والإعانات الإجتماعيّة وما إلى ذلك، ومن مصدر محدّد ومقبول والذين تتفق عملياتهم مع مصدر هذه الأموال ويمكن أعتبار هؤلاء العملاء ضمن الفئات ذات المخاطر المنخفضة بحيث تعد المعلومات الأساسيّة التالية كافية لتشكّل معلومات العميل:

١. الحصول على هويّة سارية المفعول ومناسبة للعميل كما هو محدد ضمن القواعد الخاصّة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.
٢. التأكد من ان هوية العميل تشتمل على رقم بطاقة الهويّة، والاسم، والجنسية وتاريخ/مكان الولادة.
٣. التأكد من أن العميل ليس شخصاً معرّفاً سياسياً؛ وفي حالة كونه كذلك يجب بذل إجراءات العناية الواجبة وفقاً القاعدة ٤,٥,٤.
٤. الحصول على العنوان ورقم الهاتف الثابت ورقم الهاتف الجوال، وأيضاً رقم الفاكس و/أوعنوان البريد الإلكتروني في حال كان متوفراً.
٥. التأكد من ان الحساب مستخدم للغرض المطلوب وليس لغرض تجاري؛ وخلافاً لذلك فانه يجب أن يُعامل كحساب تجاري بحيث يتم الحصول على معلومات إضافية حول النشاط التجاري.
٦. اتخاذ الإجراءات المناسبة لتحديد مصدر الأموال / الدخل والتي يمكن الحصول عليها من خلال أيّ من الوسائل التالية على سبيل المثال:
   أ. بطاقة العمل لموظفي الحكومة والقطاعين العام والخاص.
   ب. إشعار الراتب، وإشعار راتب التقاعد (للمتقاعدين)، وشهادة الراتب الإلكترونيّة أو الورقية أو خطاب من المنشأة.
   ج. نسخة من كشف حساب العميل في بنك آخر في حال حُوّل الراتب إلى ذلك البنك.
   د. لا يتوجب الحصول على معلومات إضافية في حال حُوّل الراتب مباشرة إلى البنك

transferred to that bank;
d. If salary is directly transferred to the same bank (individually or through payroll system) no need of further evidence;
e. Salary transferred through SARIE, indicating thereon as payroll/ salary;
f. Customer's self-declaration indicating his/her employer's name, salary/income and position; or
g. Any other reasonable means satisfactory to the bank and money exchanger;
h. However, in case of doubt, an official documentary confirmation of the customer's salary/ income should be obtained.

7. Conducting extra due diligence if a bank or money exchangers becomes aware that another bank or money exchanger has refused to deal with a particular customer on AML/ CTF grounds.

2. Self-Employed Individuals (Free Dealers, Agents, etc.)

For self-employed, in addition to above requirements, a self-declaration signed by the customer confirming his/her income, source of funds and business activity should be obtained. In case of doubt, enhanced due diligence should be made to determine the source of funds, and the type of activity the customer is engaged in, as these individuals are relatively of higher risk due to their free-lancing activities.

3. High Net Worth Individuals

For High Net Worth Individuals, who are considered as high-risk due to the size and nature of their activities and transactions, in addition to above, an enhanced due diligence is required and a detailed customer and transaction profiles should be prepared to also include the customer's source of funds and source of wealth, and anticipated account activity.

In all the above cases, where any doubt or suspicion arises as to the identity, address or source of income/ funds or any other information of a customer during the course of the relationship, the bank or money exchanger should re-verify all the information by reasonable means and reassess the relationship.

4.6.2 Private Banking Customers

Private Banking is the term used for preferential banking services provided to high net-worth customers by a bank. Private Banking normally caters for very wealthy, powerful and influential individuals, including PEPs. These customers are assigned a private banker or relationship manager to act as a liaison between the customer and the bank, and to facilitate the customer's use of a wide range of financial services and products that usually involve complex transactions and large sums of money, including investment services, trust vehicles and wealth management. These clients demand a high level of confidentiality. As a result, Private Banking is exposed to greater money laundering vulnerability and terrorist financing and banks should apply enhanced due diligence to such operations.

Banks should have clear customer acceptance policies for handling Private Banking customers, recognizing the money laundering and terrorist financing risks inherent in this category of accounts. They shall categorize of private account customers under high risk customers and conduct contiuous due delignece procedures. Banks should endeavor to accept only those clients whose source of wealth and funds can reasonably be established to be legitimate. The following rules should apply as a minimum:

1. Establish the identity of the clients and all the beneficial

نفسه (بشكل فرديّ أو عبر نظام الرواتب).
هـ. في حالات تحويل الراتب عبر نظام سريع يجب تعريفه كحساب رواتب.
و. إقرار شخصي من العميل يُشير إلى اسم صاحب العمل، والراتب/ الدخل والمنصب.
ز. أيّة وسيلة أخرى مناسبة ومقبولة من قبل البنك أومحل الصرافة.
ح. وفي حالة الشك يجب الحصول على تأكيد رسمي مكتوب عن راتب / دخل العميل.

٧. بذل إجراءات إضافية للعناية الواجبة في حال معرفة البنك أو محل الصرافة بان بنكاً أو محل صرافة آخر قد رفض التعامل مع عميل محدّد لسبب يتعلق بمكافحة غسل الأموال أو تمويل الإرهاب.

٢. الأفراد الذين يعملون لحسابهم (التجّار، الوكلاء الذين يعملون بشكل حرّ، إلخ)

بالإضافة إلى المتطلّبات أعلاه وبالنسبة إلى الأفراد الذين يعملون لحسابهم يجب الحصول على إقرار شخصي موقّع من العميل يؤكّد دخله، ومصدر الأموال والنشاط التجاري. وفي حالة الشك يجب بذل إجراءات العناية الواجبة المعززة لتحديد مصدر الأموال ونوع النشاط الذي يقوم به العميل، إذ ان هؤلاء الأفراد مدرجون نسبياً ضمن الفئات المصنفة بأنها ذات مخاطر عاليه بسبب أنشطتهم الحرة.

٣. الأفراد ذوي الثروات الكبيرة

يصنف الأفراد ذوي الثروات الكبيرة ضمن الفئات ذات المخاطر العالية بسبب حجم وطبيعة أنشطتهم وعملياتهم، وبالإضافة إلى ما ذكر أعلاه فان بذل إجراءات العناية الواجبة مطلوب بحيث يجب إعداد معلومات مفصّلة عن العميل وعملياته لتشمل أيضاً مصدر أموال العميل ومصدر ثروته ونشاط حسابه المتوقّع.

في جميع الحالات أعلاه، فإنه يلزم في حال الشك أو الاشتباه بهويّة العميل أو عنوانه أو مصدر دخله/أمواله أو أيّة معلومات أخرى عنه خلال فترة التعامل أن يتم إعادة التحقق من جديد من جميع المعلومات بواسطة وسائل مناسبة وأن يعاد تقييم العلاقة من جديد.

٢,٦,٤ عملاء الحسابات الخاصة

يقصد بالخدمات البنكية الخاصة الخدمات البنكية المتميزة التي يقدّمها البنك إلى العملاء الذين يتمتعون بثروات عالية. وبشكل عام تخدم هذه البنوك الأفراد الاثرياء من ذوي النفوذ والسلطة، بمن فيهم الأشخاص المعرفين سياسياً. ويعيّن البنك لهؤلاء الأشخاص موظفاً خاصاً أو مديراً للعلاقة ليؤمّن الصلة بين العميل والبنك ويسهّل استخدام العميل لمجموعة واسعة من الخدمات والمنتجات المالية التي عادة ما تتضمن عمليات معقدة ومبالغ كبيرة من المال بما في ذلك خدمات الإستثمار وخدمات الأمناء وإدارة الثروات, ويطلب مثل هؤلاء العملاء مستوىً عالياً من السرّية وبالتالي تكون الخدمات البنكية الخاصة أكثر عرضة من غيرها لأنشطة غسل الأموال ويجب على البنوك أن تخضع هذه العمليات لإجراءات معززة من العناية الواجبة.

كما يجب على البنوك أن تتبع سياسيات واضحة لقبول العملاء من أجل التعامل مع عملاء الخدمات البنكية الخاصة مع تحديد مخاطر غسل الأموال وتمويل الإرهاب التي تنطوي عليها هذه الفئة من الحسابات. وعليها أن تصنف عملاء الحسابات الخاصة ضمن العملاء ذو المخاطر العالية وبذل إجراءات العناية الواجبة المستمرة وأن تحرص فقط على قبول العملاء الذين تكون مصادر دخلهم و ثروتهم وأموالهم مشروعة على نحو مؤكّد وكحدّ أدنى من الضروري تطبيق القواعد التالية:

١. تحديد هوية العملاء وجميع المستفيدين الحقيقيين.
٢. الحصول على أوراق ثبوتية مناسبة وسارية المفعول وفقاً للقواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.

owners.
2. Obtain proper and valid identification documents as per SAMA Account Opening Rules.
3. If there are any intermediaries involved, extra due diligence should be required to cover the intermediary as well.
4. The profiling process for a Private Banking account should include obtaining and recording the following minimum information:
   a. Purpose and reasons for opening the account.
   b. Anticipated account activity.
   c. Documentation of Source of wealth (description of customer's commercial/ economic activities which have generated the net worth) and estimated net worth of the customer.
   d. Source of funds (description of the origin and the means of transfer for monies that are expected for the account opening and subsequent large transfers).
   e. References or other sources to corroborate reputation, where available.
5. Bank officers handling the account should personally meet the prospect.
6. Anonymous, fictitious name, coded or numbered accounts should not be allowed.
7. All account opening should be subject to senior management approvals in addition to the relationship manager.
8. If the Private Banking customer is also a PEP, then the requirements for PEP should apply, as per Rule **4.6.4** above.
9. All Private Banking accounts should be subject to close monitoring by a senior officer, covering unusual or suspicious activities.
10. Large cash transactions should be scrutinized more closely, in particular those of complicated nature or lacking a clear economic purpose undertaken during the period of the relationship. Enhanced due diligence procedures should be complied with. In case there are doubts of money laundering and terriost financing, FIU shall be reported thereof.

٣. في حال إشراك أيّ من الوسطاء فانه يتطلب تعزيز إجراءات العناية الواجبة في التحقق من هوية العملاء لتشمل الوسيط أيضاً
٤. يجب أن تشمل عملية إعداد المعلومات المتعلقة بالحسابات الخاصة المفتوحة في البنوك الحصول على الحدّ الأدنى من المعلومات التالية وتسجيلها:
   أ. الغرض من فتح الحساب ودوافع ذلك.
   ب. النشاط المتوقع للحساب.
   ج. توثيق مصدر الثروة (وصف الأنشطة التجارية والإقتصادية التي يمارسها العميل والتي أدّت إلى تكوين ثروته) وتقدير قيمة ثروة العميل.
   د. الدخل و مصدر الأموال (وصف المصدر وطرق تحويل الأموال المتوقعة لفتح الحساب والتحويلات الضخمة بعد ذلك)
   هـ. المراجع أو المصادر الأخرى لتعزيز السمعة حيثما تتوفر.
٥. يجب مقابلة العميل شخصياً من قبل موظفي البنك المسؤولين عن الحساب.
٦. عدم السماح بالأسماء المجهولة والوهمية أو الحسابات السرية المرّمزة أو المرّقمة.
٧. يجب إخضاع كافة عمليات فتح الحسابات لموافقة الإدارة العليا ومدير العلاقة.
٨. تنطبق المقتضيات ذات الصلة وفقاً للقاعدة **٤,٦,٤** أعلاه في حال كان عميل الحسابات الخاصة شخص معرّف سياسياً.
٩. يجب إخضاع كافة الحسابات المصنفة ضمن الحسابات الخاصة للمراقبة عن كثب من قبل أحد كبار الموظفين على نحو يغطي الأنشطة غير العادية أو المشتبه بها.
١٠. يجب تشديد الرقابة على جميع العمليات وبالأخص العمليات النقدية الكبيرة والعمليات ذات الطبيعة المعقدة أو ليس لها غرض اقتصادي واضح التي تتم طوال فترة العلاقة مع الأخذ في الاعتبار ضرورة التقييد بمتطلبات إجراءات العناية الواجبة المشددة، والإبلاغ عند وجود شك بعمليات غسل الأموال أو تمويل إرهاب لوحدة التحريات المالية.

4.6.3 Commercial Entities' Accounts

These are accounts opened by legal entities for the purpose of conducting commercial activities. Commercial entities include small enterprises such as sole proprietorships and establishments to large companies and corporations. Banks should maintain a customer profile for each commercial relationship, which should cover business and financial related information, source of funds, purpose of account, deposits and banking needs. The extent of details and nature of the information to be requested will vary in relation to the size, structure, risk and type of commercial activities of the business entities, as described below.

1. Small Business Entities

Small businesses are defined as those commercial entities with lower turnover of transactions (e.g., less than SAR one million per annum). These entities range from sole traders/ proprietorships, small establishments and small family concerns to partnerships, professional firms and small private companies.

2. Corporations & Large Business Entities

These are incorporated legal bodies such as corporations, public companies, private companies, partnerships, etc. large businesses are defined as those with significant turnover (e.g., SAR one million per annum and above), whether they are sole traders/ proprietorships, small establishments, small family businesses, partnerships, professional firms or small

٣,٦,٤ حسابات المنشآت التجاريّة

هي حسابات فتحتها منشآت نظامية لغرض إجراء الأنشطة التجاريّة. وتشمل جميع المنشآت التجاريّة من الشركات الصغيرة مثل المؤسسات الفردية والمؤسسات التجارية إلى الشركات الكبيرة. ويجب أن تحتفظ البنوك بمعلومات العميل لكلّ علاقة تجاريّة تشمل معلومات تتعلّق بالأعمال والأموال، ومصدر الأموال، والغرض من الحساب، والإيداعات والاحتياجات البنكيّة. وتختلف التفاصيل وطبيعة المعلومات التي تُطلب بناءً على الحجم، وهيكل المنشأة، والمخاطر ونوع الأنشطة التجاريّة، وذلك وفقاً للتالي.

١. المنشآت الصغيرة

تعرّف المنشآت الصغيرة على أنها تلك المؤسسات التجارية ذات المبيعات والعمليات الصغيرة نسبياً (أقل من مليون ريال سعودي في السنة). وقد تكون هذه المنشآت من التجّار أو المؤسسات الفردية، والمؤسسات الصغيرة والمؤسسات العائلية الصغيرة أو الشركات، والمؤسسات المهنيّة والشركات الخاصّة الصغيرة.

٢. الشركات و المنشآت التجارية الكبيرة

وهي هيئات نظامية مؤسسة مثل الشركات العامة والخاصة والمؤسسات، إلخ.وتعرّف المؤسسات الكبيرة على أنها ذات المبيعات والعمليات الكبيرة (مليون ريال سعودي في السنة وأكثر)، سواء كان تجّاراً أو مؤسسات فردية، أو مؤسسات صغيرة، أو مؤسسات عائليّة

private companies.

3. General Requirements

For all commercial entities, the principal guidance is to look behind the entity to identify those who have control over the business and entity's assets. As a commercial entity can be used as a front to provide cover for money laundering activities, especially cash-intensive businesses, banks should ensure they obtain adequate information about the entity's business/ trading activities and the expected use of the bank's products and services.

Banks should obtain the following information for all commercial entities at the time of opening account/ relationship for applying the customer due diligence in accordance with the risk assessment of the customer:

1. Valid and original identification documents as required in the SAMA Account Opening Rules.
2. Large business entities and corporations: The financial structure and nature of the business entity and its annual financial statements.
3. Small business entities: An assessment of the business entity's financial statements, turnover and revenue/ income.
4. Names of beneficial owners, partners, managers, powers-of-attorney, authorized signatories, shareholders (except for minor shareholders of joint stock companies, owning less than 5%), etc., as applicable.
5. Description of customer's line of business and business activities.
6. Types and nature of products and services the entity may be dealing in.
7. List of significant suppliers, customers and their geographical locations, as applicable.
8. Description of geographical coverage where the business entity carries out its activities, as applicable.
9. List and locations of branches and outlets, if any.
10. Purpose and intended nature of the business relationship/ account. The account should be used for the purpose it is opened.
11. For *large business entities and corporations*, bank employees should pay site visits to acquaint themselves with the nature of business activities. All customer visits should be properly documented and the records maintained.
12. For *small business entities*, where feasible/ practical, bank employees may pay site visits to acquaint themselves with the nature of business activities, and the customer visits documented and records maintained.
13. Individual accounts used for commercial purposes should be treated as small business entities in terms of profiling.
14. Banks should seek information on the customer's relationship with other banks and seek information from these banks if suspicions arise about their dealings with the customer. Extra due diligence is needed, if the bank has reason to believe that other bank(s) rejected this relationship.
15. Banks should collect direct or indirect information about the business entity from any known or available sources.
16. Banks should ascertain the accuracy of the information provided by the business entity when opening an account, e.g., ascertaining the business address, etc.
17. Banks should use their best efforts, through customer profiling and transaction profiling, to ascertain the sources of all deposits, paying additional attention to large cash deposits.
18. These entities' accounts shall be operated by Saudi citizens. Entities may not grant a power of attorney to Non-Saudis.

صغيرة، أو شركات، أو شركات مهنيّة أو شركات خاصة صغيرة.

٣. المتطلّبات العامّة

إن القاعدة الرئيسية بالنسبة إلى جميع المنشآت التجاريّة هي النظر ما وراء المنشأة لتحديد هويّة الذين يسيطرون على أعمال وأصول المنشأة ويتعيّن على البنوك أن تضمن بأنها تحصل على معلومات كافية حول أعمال المنشأة وأنشطتها التجارية والاستخدام المتوقّع لمنتجات البنك وخدماته حيث أن المنشأة التجارية يمكن أن تُستخدم كواجهة لتوفير التغطية لأنشطة غسل الأموال، وخصوصاً من خلال المشاريع التي تدرّ أموالاً كبيرة ، ويجب أن تحصل البنوك على المعلومات التالية لجميع المنشآت التجاريّة عند فتح الحساب أو تأسيس العلاقة من أجل تطبيق إجراءات العناية الواجبة وفقاً لتقييم مخاطر العميل :

١. مستندات صحيحة وأصلية لتحديد الهوية كما هو مطلوب في القواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.
٢. المنشآت والشركات الكبيرة : الهيكل المالي وطبيعة كيان الأعمال والبيانات الماليّة السنويّة.
٣. المنشآت الصغيرة : تقييم البيانات المالية والمبيعات والإيرادات والدخل.
٤. أسماء المستفيدين الحقيقيين، والشركاء، والمدراء، والوكلاء، والمفوضين بالتوقيع، والمساهمين (باستثناء المساهمين الثانويين في الشركات المساهمة والذين يملكون ما يقلّ عن ٥%) ..إلخ
٥. وصف نوع أعمال العميل وأنشطته التجاريّة.
٦. أنواع وطبيعة المنتجات والخدمات التي قد تتعامل بها المنشأة.
٧. قائمة المورّدين والعملاء الرئيسيين ومواقعهم الجغرافية.
٨. وصف التغطية الجغرافيّة حيث تقوم المنشأة التجاريّة بأنشطتها.
٩. قائمة ومواقع الفروع ومنافذ البيع في حال وجودها.
١٠. الغرض والطبيعة المطلوبة للعلاقة التجاريّة / الحساب. وأن يستخدم الحساب للغرض الذي فتح من أجلة.
١١. يجب أن يقوم موظّفو البنك بزيارات ميدانية ليطلعوا على طبيعة الأنشطة التجاريّة بالنسبة إلى المنشآت التجارية الكبيرة والشركات ويجب أن تكون جميع زيارات العملاء موثّقة بشكل صحيح مع الاحتفاظ بالسجلات.
١٢. يستطيع موظّفو البنك أن يقوموا بزيارات ليطلعوا على طبيعة الأنشطة التجاريّة *بالنسبة* إلى المنشآت التجاريّة *الصغيرة* وحيث يكون ممكناً أوعملياً مع توثيق زيارات العملاء والاحتفاظ بالسجلات.
١٣. يجب أن تعامل الحسابات الفرديّة المستخدمة لأغراض تجارية كحسابات المنشآت التجاريّة الصغيرة فيما يتعلق بالمعلومات المطلوبة عنها.
١٤. يجب على البنوك الحصول على معلومات عن علاقة العميل بالبنوك الأخرى مع طلب المعلومات من هذه البنوك في حال ظهر اشتباه حول تعاملاتها مع العملاء ، كما يجب بذل إجراءات العناية الواجبة المشددة في حال اشتباه البنك برفض بنك اخر إجراء مثل هذه العلاقة مع العميل.
١٥. يجب أن تجمع البنوك المعلومات المباشرة وغير المباشرة عن المنشأة التجاريّة من أيّة مصادر معروفة أو متوفرّة.
١٦. يجب أن تتحقّق البنوك من دقة المعلومات المقدّمة من المنشأة التجاريّة عند فتح الحساب، مثل التأكّد من العنوان التجاريّ، إلخ.
١٧. يجب أن تبذل البنوك قصارى جهدها، من خلال إعداد معلومات العميل والعمليات للتحقق من مصادر جميع الإيداعات. مع توجيه اهتمام إضافي للإيداعات النقديّة الكبيرة.
١٨. كما يجب أن تدار حسابات هذه المنشأت التجارية من قبل مواطنين سعوديين ولا يحق التفويض بوكالة لغير السعودي.

4.6.4 Politically Recognized Persons

Individuals who are or have been occupying or are expected to occupy in the future leadership positions, for example heads of state or of government, senior public sectors, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, or employees of regional and international organizations. In addition, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or less important individuals in the foregoing categories.

The political influence and power of PEPs could give rise to abuse of the positions to illegally amass wealth, the proceeds of which are often transferred and concealed under the names of relatives or close associates. Banks and money exchangers should apply the following standards, as a minimum:

1. Comply with all the SAMA Account Opening Rules relating to opening accounts for individuals.
2. Have policies in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing & new customers as well as the beneficial owners.
3. To put in place appropriate risk management systems to determine whether a potential customer, existing customer or the beneficial owner is a politically exposed person.
4. Determine the source of funds, source of wealth and beneficial owners for all PEPs.
5. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Banks and money exchangers should be required to obtain senior management approval to continue the business relationship.
6. Categorize all such accounts and relationships as High Risk for enhanced due diligence, and should require approval of a General Manager, Managing Director, or CEO
7. Where Banks and money exchangers are in a business relationship with PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.
8. Accounts of PEPs and related individuals should be reviewed continuously and must be approved by General Manager, Managing Director, or CEO for retaining the relationship/ account.

٤,٦,٤ الأشخاص المعرّفون سياسياً

وهم الأفراد الذين يتولون أو كانوا يتولون أو من المتوقع أن يتولون في المستقبل مناصب قيادية عامّة، على سبيل المثال رؤساء الدول أو رؤساء الحكومات، أو كبار موظفي قطاعات الحكومة والقضاء والقطاع العسكري، أو كبار المديرين التنفيذيين للمؤسسات المملوكة للدولة، أو كبار مسؤولي الأحزاب السياسية، أو موظفي المنظمات الإقليمية والدولية. كما ان علاقات الأعمال مع أفراد عائلة الأشخاص المعرفين سياسيّاً أو الأشخاص المرتبطين بهم قد تنطوي على مخاطر سمعة مماثلة لمخاطر السمعة التي يتعرض لها الأشخاص المعرفين سياسياً بحدّ ذاتهم. ولا يشمل التعريف الأفراد ذوي المراتب الوسطى أو الأفراد الأقل شأناً في الفئات السابقة الذكر.

قد يؤدي التأثير السياسي وسلطة الأشخاص المعرفين سياسياً إلى استخدام سلطاتهم للإثراء غير المشروع، وغالباً ما تُنقل عائدات هذه الثروات تحت أسماء أقارب أو أشخاص مقرّبين بغرض حجبها. وعلى البنوك ومحلات الصرافة تطبيق المعايير التالية كحد أدنى:

١. الالتزام التام بكافة القواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي بخصوص فتح حسابات للأفراد.
٢. وضع سياسات لتحديد هويّة وتصنيف الأشخاص المعرفين سياسياً والأفراد المرتبطين بهم بغرض تعزيز الرقابة, كما أن تحديد هويّة الأشخاص المعرفين سياسياً يجب أن يشمل العملاء الحاليين والمستقبليين وكذلك المستفيدين الحقيقيين.
٣. وضع نظم مناسبة لإدارة المخاطر لتحديد ما إذا كان العميل المستقبلي، أو العميل الحالي أو المستفيد الحقيقي من الأشخاص المعرفين سياسياً.
٤. تحديد مصدر الأموال ومصدر الثروة والمستفيدين الحقيقيين لجميع الأشخاص المعرّفين سياسياً.
٥. عند قبول أحد العملاء واكتشف بعد ذلك أن العميل أو المستفيد الحقيقي من الأشخاص المعرفين سياسياً ، ينبغي الحصول على موافقة الإدارة العليا على مواصلة علاقة العمل معه.
٦. تصنيف جميع هذه الحسابات والعلاقات بانها ذات مخاطر عالية بغرض توفير إجراءات العناية الواجبة المعززة ويقتضي ذلك الحصول على موافقة المدير العام أو العضو المنتدب أو الرئيس التنفيذي لفتح هذه الحسابات.
٧. في حالة وجود علاقات عمل مع أي شخص معرف سياسياً، ينبغي القيام بالمتابعة المستمرة المشددة لعلاقة العمل معه.
٨. يجب مراجعة حسابات الأشخاص المعرّفين سياسياً والأفراد المرتبطين بهم بشكل مستمر والحصول على موافقة المدير العام أو العضو المنتدب أو الرئيس التنفيذي من أجل استمرار العلاقة أو الحساب.

4.6.5 Walk-In Customers

A walk-in or occasional customer is one who conducts a transaction with a bank or money exchanger but does not maintain an account or any type of relationship with the bank or money exchanger. These include citizens, residents and visitors on a temporary visa/ residence. As banks and money exchangers do not have adequate background information about these individuals, banks or money exchangers may be at risk if they conduct financial transactions for them. Therefore, banks and money exchangers should not accept any transactions from walk-in customers unless they fall under the following categories:

1. Citizen or Resident Not Holding accounts: Banks and money exchangers are allowed to accept settlement of bills of services and public utilities (electricity, water, telephone) and payments to state authorities and government dues (traffic, passports, etc.). They may

٥,٦,٤ العملاء العارضون (العابرون)

العميل العارض او العابر هو الذي يقوم بعملية من خلال بنك أو محل صرافة دون أن يكون لديه أيّ حساب أو أيّ نوع من العلاقات مع البنك أو محل الصرافة. وتشمل هذه الفئة المواطنين والمقيمين وكذلك الزوّار الذين يحملون تأشيرة/إقامة مؤقتة. وقد تتعرض البنوك أو محلات الصرافة للخطر في حال إجراء العمليات الماليّة لهؤلاء العملاء بسبب عدم توفر المعلومات الكافية عنهم. لذا فانه يحظر على البنوك ومحلات الصرافة قبول أيّة عمليات من العملاء العابرين ما لم يتم تصنيفهم ضمن الفئات التالية :

١. الشخص (المواطن أو المقيم) الذي لا يملك حسابات : يُسمح للبنوك ومحلات الصرافة قبول تسديد فواتير الخدمات العامّة (الكهرباء، والماء والهاتف) ومستحقات الجهات الحكوميّة وتسديد الرسوم الحكوميّة (المرور، والجوازات، إلخ) ، وتبديل العملات النقدية شريطة ألا يتجاوز مبلغ الأستبدال للمرة الواحدة (٥,٠٠٠) ريال سعودي أو ما يعادله وبإجمالي لا يتجاوز مبلغ (٥٠,٠٠٠) ريال سعودي أو ما يعادله خلال العام الواحد ، وأن يتم إستيفاء معلومات الهوية المدنية للمواطنين وجواز السفر للوافدين وتدوين ذلك

exchange currencies no exceeding (SAR 5000) per a transaction of its equivalent, with a total of no more than (SAR 50,000) during one year, provided the identfcation of information for citizen and passport information of expatriate should be obtained and a currency exchange form should be filled out thereof. Banks and money exchangers shall establish an electronic reference using the custormer's identfcation number.

2. Visitors on a temporary visa/residence (Foreign Pilgrims, Tourists, Businessmen & Diplomats): Banks and money exchangers are allowed to accept settlement of bills of any services and public utilities, payments to state authorities and government dues, and encashment of travelers checks. currency exchange and receiving remittances up to (SAR 5000) per transaction and not exceeding the equivalent of (SAR 50,000) in total within the validity of the visa. A copy of the passport should be obtained including the pages showing the entry and visa stamps. Genuinity of the copy should be verified by the customer and the bank. Banks and money exchangers shall establish an electronic reference using the custormer's passport number during this time.
3. For the allowed receiving remittances, a copy of the passport should be obtained including the page evidencing the visa. Full compliance with all the instructions issued concerning money transfers regulation, other details such as home country address, contact in Saudi Arabia and signature should be obtained.
4. In case of suspicion, the bank or money exchanger should report the transaction to FIU enclosing copies of the identfcation or passport and the transaction, and customer details.

في نموذج إستبدال العملة. والاحتفاظ برقم الهوية او رقم الجواز كمرجع آلي للعمليات المنفذة.

٢. الزوّار بتأشيرة دخول/ إقامة مؤقتة ، والزوّار (الحجّاج الأجانب، والسوّاح، ورجال الأعمال والدبلوماسيون) : يُسمح للبنوك ومحلات الصرافة قبول تسديد فواتير الخدمات العامّة (الكهرباء، والماء والهاتف) ومستحقات الجهات الحكوميّة وتسديد الرسوم الحكوميّة، وصرف الشيكات السياحيّة، وتبديل العملات النقدية ، وقبول التحويلات المالية شريطة ألا يتجاوز مبلغ العملية الواحدة سواء الأستبدال او التحويل مبلغ (٥,٠٠٠) ريال سعودي أو ما يعادله وبإجمالي لا يتجاوز مبلغ (٥٠,٠٠٠) ريال سعودي أو ما يعادله ضمن فترة صلاحية التأشيرة وأن يتم استيفاء معلومات جواز السفر والحصول على صورة منه مشتملة على ختم الدخول والتأشيرة ورقمها ويصادق على مطابقتها للاصل من قبل كل من العميل وموظف البنك، وعلى البنك ومحل الصرافة الاحتفاظ برقم الجواز خلال هذه الفترة كمرجع آلي للعمليات المنفذة.

٣. عند قبول التحويلات المالية يجب الحصول على نسخة عن جواز السفر بما في ذلك الصفحة التي تظهر تأشيرة الدخول وذلك عند القيام بالعمليات المسموح بها. ويجب أن تراعى متطابات التحويل المالي الاخرى بما في ذلك توفر التفاصيل الأخرى مثل العنوان في البلد الأم، ورقم شخص أو جهة الاتّصال في المملكة العربيّة السعوديّة والتوقيع.

٤. في حال وجود شبهة يجب أن يبلّغ البنك أو محل الصرافة عن العملية لوحدة التحريات الماليّة ويرفق بها نسخة عن الهوية او جواز السفر والعملية وتفاصيل عن العميل.

4.6.6 Charity Organizations & Non-Profit Entities

A charity organization or non-profit entity refers to a legal entity or organization that primarily engages in raising/ collecting donations and/ or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of benevolent deeds.

Banks and money exchangers should have in place policies, procedures and controls to comply with SAMA Account Opening Rules requirements regarding the handling of accounts and transactions for charity organizations and non-profit entities. When dealing with accounts, relationship or transactions of any charity organizations or non-profit entities, banks and money exchangers should observe the following:

1. Not to open account or set up a relationship for any charity organization or non-profit entity (local or international) unless it meets statutory requirements related to this type of accounts that provided in the Rules Governing the Opening of Bank Accounts & General Operational Guidelines and obtains the official registration by the relevant government ministry or authority, specifying the purpose and activity.
2. To strictly comply with the SAMA Account Opening Rules relating to specific requirements and restrictions when dealing with charity organization accounts.
3. Not to open accounts in the names of chairmen or managers of charities for managing charity funds.
4. To classify charity organization accounts as High Risk and exercise extra and continuous due diligence.
5. Not to accept any transfers or payments (incoming or outgoing) of any donations or contributions into or out of Saudi Arabia except permitted entities. in accordance with the rules for opening bank accounts and the general operational rules. This is regardless of whether the funds

٦،٦،٤ الجمعيات والمنظمات الخيرية والجهات غير الهادفة للربح

إن المنظمات الخيرية أو الجهات غير الهادفة للربح هي عبارة عن منشأة أو منظمات قانونية تعمل بشكل رئيسي في جمع التبرعات و/أو صرف الأموال لأهداف محددة خيرية، أو دينية، أو ثقافية، أو تربوية، أو إجتماعية أو من أجل تنفيذ أنواع أخرى من الأعمال التطوعية.

لذا يجب على البنوك ومحلات الصرافة أن يتبعوا سياسات وإجراءات وضوابط مشددة للتقيد بأحكام القواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي لا سيما فيما يتعلق بإدارة الحسابات والعمليات الخاصة بالجمعيات والمنظمات الخيرية والجهات غير الهادفة للربح، ويجب على البنوك ومحلات الصرافة أثناء التعامل مع الحسابات أو العلاقات أو العمليات الخاصة بأي من الجمعيات والمنظمات الخيرية أو الجهات غير الهادفة للربح التقيّد بما يلي:

١. عدم فتح أي حساب أو إقامة أي علاقة لأي جمعية منظمة خيرية أو جهه غير هادفة للربح (سواء محلية أو دولية) إلا بعد استيفاء المتطلبات النظامية الخاصة بهذه الفئة من الحسابات المنصوص عليها في قواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها والحصول على السجل الرسمي أو الترخيص من قبل الوزارة أو الجهة الحكومية المختصة والذي يحدّد فيه الغرض من المنظمة ونشاطها.

٢. التقيّد التام بالقواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي وخاصة بالأحكام والقيود المحددة عند التعامل مع حسابات الجمعيات والمنظمات الخيرية.

٣. عدم فتح الحسابات باسم رؤساء أو مدراء الجمعيات والمنظمات الخيرية لإدارة الأموال الخيرية.

٤. تصنيف حسابات الجمعيات المنظمات الخيرية في خانة المخاطر العالية وبذل إجراءات العناية الواجبة المستمرة عند التحقق من هوية العملاء.

٥. عدم قبول أي تحويلات أو مدفوعات (الواردة أو الصادرة) لأي من التبرعات أو المساهمات التي تدخل إلى المملكة أو تخرج منها، عدا الجهات المسموح لها بذلك وفقا

originate from natural persons, legal entities, organizations and multi-national organizations, independent or public charities.
6. Not to enter into any transaction, knowing that the funds or property involved are owned or controlled by criminals or criminal organizations, or that a transaction is linked to, or likely to be used in criminal activity, and should report such case to FIU.
7. To freeze any transaction and immediately report the matter to FIU, in case of reasonable grounds to suspect that that an individual or entity is, by any means, directly or indirectly, providing or collecting funds in the knowledge that such funds will be used for illegal purposes,
8. To design their fund transfer systems (for incoming and outgoing transfers) to be capable of detecting customer names against designated persons of UN or SAMA, prior to processing the transaction for the purpose taking appropriate action.
9. Not to allow to transferring funds in favor of any charity organizations outside the Kingdom of Saudi Arabia other than permitted entities. in accordance with the rules for opening bank accounts and the general operational rules
10. Full compliance with all the instructions issued concerning money transfers regulation, ensuring the application of the rules of cable transfers (see paragraph 5.1.2).

للقواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي. وذلك بغض النظر عن مصدر الأموال سواء كانت من الأشخاص الطبيعيين أو المنشآت والمنظمات القانونية أو المنظمات المتعددة الجنسيات أو الجمعيات الخيرية المستقلة أو العامة.

٦. عدم الدخول في أي عملية قد تكون الأموال أو الممتلكات المتضمنة فيها مملوكة أو مدارة من قبل مجرمين أو تنظيمات إجرامية أو أي عملية مرتبطة بنشاط إجرامي أو قد تستخدم في مثل هذا النشاط ويجب إبلاغ وحدة التحريات المالية عن مثل هذه الحالات.

٧. تجميد أي عملية وإبلاغ وحدة التحريات المالية فوراً عن الحالة حين توفر الأسس المعقولة للإشتباه بان أحد الأفراد أو المنشآت يقوم بطريقة أو بأخرى بشكل مباشر أو غير مباشر بتوفير الأموال أو جمعها وانها ستسخدم لأغراض غير مشروعة.

٨. تصميم الأنظمة الألية الخاصة بها لتحويل الأموال (الواردة والصادرة) بحيث تكون لها القدرة على اكتشاف أسماء العملاء ومقارنتها مع قوائم الأشخاص المدرجين من قبل الأمم المتحدة أو مؤسسة النقد قبل تنفيذ العملية من أجل اتخاذ الإجراء المناسب.

٩. عدم السماح بتحويل الأموال لصالح أي جمعيات ومنظمات خيرية او جهات غير هادفة للربح خارج المملكة العربية السعودية عدا الجهات المسموح لها بذلك وفقا للقواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.

١٠. التقييد التام بكافة التعليمات الصادرة بشان تنظيم التحويلات المالية والتاكد من تطبيق القواعد الخاصة بالتحويلات البرقية انظر فقرة (٢,١,٥).

4.6.7 Trustees, Nominees & Intermediaries Accounts

٤،٦،٧ حسابات الأمناء والموكلين والوسطاء

1. Trustee & Nominee Accounts

These accounts are normally used to provide an extra layer of security to protect the confidentiality of legitimate customers. However, these structures can also be misused to circumvent customer identification procedures for the purpose of money laundering. Therefore, it is essential that the true relationship is understood. Banks should have in place procedures to ensure the following:

1. Establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee or nominee.
2. If the customer is acting on behalf of another person, ensure that he/she has the authorization to do so, and identify and verify the identity of the beneficiaries' owner.
3. Where the customer is a trustee, understand the structure of the trust sufficiently to determine the provider of funds, those who have control over the funds (trustees) and any persons or entities who have the power to remove the trustees.
4. Make a reasonable judgment as to the need for further due diligence and obtain appropriate evidence of formation and existence along with identity of the settlers/ grantors, trustees or persons exercising effective control over the trust and the principal beneficiaries.
5. Exercise special care in initiating business transactions with companies that have ordinary shareholders; obtain satisfactory evidence of the identity of beneficiaries owner of all such companies; and monitor the identity of actual beneficiaries owner.

2. Intermediaries 'clients Accounts

These are accounts opened by professional intermediaries (such as lawyers, , independent financial advisors, etc.) who act as professional asset managers on behalf of other clients

١. حسابات الأمناء والموكلين

توفر هذه الحسابات عادة مستوى أعلى لأمن وحماية سرية العلاقات المصرفية المشروعة. ولكن قد تُستغل هذه الترتيبات وتستخدم على نحو مخالف لطبيعتها للتهرب من إجراءات التعرّف على هوية العميل وبغرض القيام بعمليات غسل الأموال. ولذلك فمن الضروري فهم العلاقة الحقيقية. إذ يجب على البنوك وضع الإجراءات التي تضمن ما يلي:

١. تحديد ما إذا كان العميل يستعمل إسم عميل آخر يقوم بدور "الواجهة" له أو يتصرّف بالنيابة عن شخص آخر كالأمين أو ممثل الشخص.

٢. تحديد ما إذا كان العميل يتصرّف بالنيابة عن شخص آخر حيث يجب التأكّد من انه مفوّض بالتصرّف على ذلك النحو كما يجب تحديد هوية المستفيد الحقيقي والتحقق منها.

٣. حين يكون العميل أميناً، يجب فهم طبيعة ترتيبات الأمانة بشكل مرضٍ لتحديد الجهة التي تقدّم الأموال والجهات التي تسيطر على الأموال (الأمناء) وكذلك أي شخص أو منشأة يملك/ تملك السلطة الكافية لإقالة الأمناء.

٤. ينبغي إتخاذ القرار بشأن الحاجة إلى زيادة إجراءات العناية الواجبة والحصول على الأدلة المناسبة حول تفاصيل ترتيبات الأمانة ووجودها وكذلك حول هوية منفذي التسوية والأمناء أو الأشخاص الذين يسيطرون فعلياً على ترتيبات الأمانة والمستفيدين الأساسيين.

٥. ينبغي ممارسة عناية خاصة عند البدء بالمعاملات التجارية مع شركات لديها مساهمين اسميين حيث يتعين الحصول على إثباتات مرضية حول هوية المستفيدين الحقيقيين لكل هذه الشركات مع وضع إجراءات كافية لمراقبة هوية المستفيدين الحقيقيين الفعليين.

٢. حسابات العملاء الوسطاء

هي الحسابات التي يفتحها الوسطاء المهنيون (مثل المحامين ، والمستشارين الماليين المستقلّين، إلخ...) والذين يعملون كمدراء محترفين للأصول بالنيابة عن عملاء آخرين (الأفراد أو الشركات). ويمكن أن تكون هذه الحسابات "مجمّعة" تدار من قبل وسطاء مهنيين بالنيابة

(individuals or corporations). These accounts could be pooled accounts managed by professional intermediaries on behalf of entities such as, pension funds, or managed by lawyers or that represent funds held on deposit or in escrow for a range of clients.

These types of accounts are potentially vulnerable to the money laundering subsequent to the placement phase. Specific vulnerable activities include:

1. Intentional or unwitting facilitation of a customer's money laundering scheme and the activities of rogue employees who undertake illegal activities.
2. Wash sales or other fictitious trading schemes to transfer money.
3. Transfer of value between parties through the sale of shares in small, illiquid issues at artificially arranged prices, without regard to fair market value.

Due to risks accompanying these accounts, banks should have procedures in place and ensure the following:

1. The broker is registered and legal.
2. Perform reinforced due diligence on the intermediary itself and the account should be classified as High Risk.
3. Verify and be satisfied with the broker's reputation and integrity.
4. Establish that the broker has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring of its customers and beneficiaries owner, which is satisfactory to the bank.
5. Establish that the broker has in place written policies, procedures and internal controls to address and the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the broker in money laundering and terrorist financing schemes.
6. When a bank has knowledge or reason to believe that a client account opened by a professional broker is on behalf of a single client, that client must be identified.
7. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficiaries owner, all beneficiaries owner of the account held by the intermediary must be identified.
8. Where the funds are co-mingled, the bank should look through to the beneficial owners, unless the bank can establish that the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as that of the bank.
9. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.
10. In the absence of the above requirements, then the bank should not permit the intermediary to open an account.

عن جهات معينة مثل صناديق التقاعد، أو التي تدار من قبل محاميين أوالتي تمثل الأموال المحتفظ بها في حساب وديعة أو حساب أمانة لمجموعة من العملاء.

وتعتبر هذه الأنواع من الحسابات معرضة لمخاطر غسل الأموال وخصوصاً في مرحلة "التغطية". وتتمثل نقاط الضعف في الأنشطة التالية:

١. التسهيل المتعمد أو غير المتعمد لمخطط العميل الهادف إلى غسل الأموال والأنشطة غير القانونية التي يمارسها الموظفون المحتالون.
٢. عمليات البيع الصورية أو مشاريع التجارة الوهمية الأخرى لتحويل الأموال.
٣. نقل الأموال بين الأطراف المعنية من خلال بيع الأسهم بإصدارات صغيرة وغير سائلة وبأسعار زائفة ومرتبة، بغض النظر عن القيمة العادلة في السوق.

ولما يصاحب هذه الحسابات من مخاطر فإنه يجب أن تضع البنوك إجراءات للتأكد مما يلي:

١. أن الوسيط مسجل وقانوني.
٢. بذل إجراءات العناية الواجبة المعززة في التحقق من هوية الوسيط وتصنيف الحساب في خانة المخاطر العالية.
٣. التحقق من سمعة الوسيط ونزاهته والقبول بها.
٤. أن الوسيط يمارس إجراءات العناية الواجبة بصورة ملائمة وموثقة، بما في ذلك مباديء "اعرف عميلك" ومتطلبات تحديد هوية العملاء، ومراقبة أنشطة عملائه والمستفيدين الحقيقيين على نحو مقبول بالنسبة للبنك.
٥. أن الوسيط لديه سياسات وإجراءات وضوابط داخلية للتعامل مع مخاطر قد تنشأ من استخدام أعماله كوسيلة للقيام بأنشطة غير قانونية، بما في ذلك وضع ضوابط للإدارة تمنع الوسيط من التورط في مخططات غسل الأموال وتمويل الإرهاب.
٦. إذا علم البنك أو كان لديه سبب يجعله يعتقد بأن حساب العميل الذي تم فتحه من قبل وسيط مهني بالنيابة عن عميل آخر، فإنه يجب عليه تحديد هوية هذا العميل.
٧. عندما لا تكون أموال الوسيط مختلطة في البنك، بل توجد "حسابات فرعية" يمكن نسبها لكلّ مستفيد حقيقي فإنه يجب على البنك التعرف على هوية كل المستفيدين الحقيقيين من الحساب الذي يملكه الوسيط.
٨. عندما تكون الأموال مختلطة فإنه يجب على البنك أن يتفحص المستفيدين الحقيقيين ما لم يثبت أن الوسيط خاضع لنفس التشريعات التنظيمية والإجراءات الرقابية المتعلقة بغسل الأموال وبشكل خاص لنفس معايير العناية الواجبة فيما يتعلق بقاعدة عملائه كتلك التي يطبقها البنك.
٩. يجب على البنوك قبول هذا النوع من الحسابات بشرط أن تكون قادرة على التأكد من أن الوسيط قد مارس إجراءات العناية الواجبة الملائمة وأن لديه النظم والضوابط اللازمة لتحديد ملكية المستفيدين المعنيين للأصول في الحسابات المجمّعة.
١٠. في حال عدم وجود المتطلبات السابقة، على البنك أن لا يسمح للوسيط بفتح الحساب لديه.

4.6.8 Insurance Companies Accounts

These are accounts opened by insurance companies who offer insurance products directly to their customers or through agents. The insurance sector is potentially at risk and can provide the opportunity for misuse, knowingly or unknowingly, for money laundering and financing of terrorism.

As insurance companies deal with their own customers, banks should exercise extra due diligence on these accounts, and, in addition to SAMA's Insurance Companies Accounts Opening Rules requirements, banks should have procedures

٨،٦،٤ حسابات شركات التأمين

هي الحسابات المفتوحة من قبل شركات التأمين التي تقدم منتجات –التأمين إلى عملائها إمّا بصورة مباشرة أو بواسطة الوكلاء. ويعتبر قطاع التأمين عرضة للمخاطر وقد يصبح قابلاً للاستغلال عن علم أو عن غير علم لأغراض غسل الأموال وتمويل الإرهاب .

وبما أن لشركات التأمين عملائهم الخاصين, فإنه يجب على البنوك زيادة إجراءات العناية الواجبة على مثل هذه الحسابات وبالإضافة إلى التقيّد بأحكام القواعد الخاصة بفتح حسابات شركات التأمين والصادرة عن مؤسسة النقد العربي السعودي ويجب على البنوك وضع

and controls in place to implement the following:

1. Dealing only with registered and regulated insurance companies.
2. Performing extra due diligence on the insurance companies and classifying the accounts as High Risk.
3. Verifying and being satisfied with the insurance company's reputation and integrity.
4. Establishing that the insurance company has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring for its customers, that is satisfactory to the bank.
5. Establishing that the insurance company has in place written policies, procedures and internal controls to address the risks of its business being used as a vehicle for illegal activities, including the establishment of management controls to prevent the involvement of the insurance company in money laundering and terrorist financing schemes.
6. In the absence of the above requirements, then the bank should not permit the insurance company to open an account.

الإجراءات والضوابط لتنفيذ ما يلي:

١. حصر التعامل مع شركات التأمين المسجلة والنظامية.
٢. زيادة إجراءات العناية الواجبة لحسابات شركات التأمين وتصنيفها على انها ذات مخاطر عالية.
٣. التحقق من سمعة شركة التأمين ونزاهتها والقبول بها.
٤. التحقق من أن شركة التأمين تمارس إجراءات العناية الواجبة بصورة ملائمة وموثقة، بما في ذلك مباديء "اعرف عميلك" ومتطلبات تحديد هوية العملاء، ومراقبة أنشطة عملائها والمستفيدين الحقيقيين على نحو مقبول بالنسبة للبنك.
٥. التحقق من أن شركة التأمين لديها سياسات وإجراءات وضوابط داخلية للتعامل مع مخاطر قد تنشأ من استخدام أعمالها كوسيلة للقيام بأنشطة غير قانونية، بما في ذلك وضع ضوابط للإدارة تمنع شركة التأمين من التورط في مخططات غسل الأموال وتمويل الإرهاب.
٦. في حال عدم وجود المتطلبات السابقة، على البنك أن لا يسمح لشركة التأمين بفتح حساب لديه.

4.6.9 Introduced & Referred Businesses

It is customary for banks to rely on the procedures undertaken by other banks or introducers (person, entity or a professional intermediary) when business is being referred. In doing so, banks risk placing reliance on the due diligence procedures that they expect the introducers to have performed . Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures, or that are unwilling to share copies of due diligence documentation.

1. Introduced Business

Banks that use introducers should carefully assess whether the introducers are reputable and are exercising the necessary due diligence in accordance with the acceptable KYC standards. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:

The customer due diligence procedures of the introducer should be stronger than those which the bank would have conducted itself for the customer. The banks should also ensure that the required due diligence includes that of the introducer.

1. The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.
2. The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.
3. nkBas should reach agreement with the introducer that it will be permitted, upon its request, to obtain and carefully review all relevant identification data and other documentation pertaining to the customer and the introducer.
4. The decision to open the account should not be solely based on the introducer's reputation; rather all KYC process should take place for the introducer as well as the account owner.
5. This type of accounts should be classified as High Risk, and reinforced due diligence should be performed on accounts related to those entities.

٤،٦،٩ <u>الأعمال المقدمة والمحالة من جهات أخرى</u>

من الشائع لدى البنوك أن تعتمد على الإجراءات التي اتخذتها بنوك أخرى أو جهات التعريف (سواء كانت شخص ، أو منشأة أو وسيط مهني) عند إحالة الأعمال إليها. وفي حال قيامها بذلك تتحمل البنوك مخاطر الاعتماد على إجراءات العناية الواجبة والتي تتوقع أن جهات التعريف قامت بإجرائها. وبغض النظر عن السمعة الطيبة التي تتمتع بها تلك الجهات لا تستبعد المسؤولية النهائية للبنك المتلقي في معرفة عملائه والوقوف على أنشطتهم التجارية وعلى وجه الخصوص فإنه يجب على البنوك عدم الاعتماد على جهات التعريف التي تخضع لمعايير أضعف من تلك التي تخضع لها إجراءات "اعرف عميلك" المعتمدة لدى البنك أو الجهات التي لا تبدي أستعداداً لتقديم نسخ من مستندات العناية الواجبة.

١. **<u>الأعمال المقدمة</u>**

ينبغي على البنوك التي تستخدم جهات التعريف أن تقوم بإجراء تقييّم دقيق عن هذه الجهات وأنها تمارس إجراءات العناية الواجبة اللازمة طبقاً للمعايير المقبولة لمعرفة العملاء علماً أن المسؤولية النهائية في معرفة العملاء تقع دائماً على عاتق البنك. وعليه فإنه للتأكّد من إمكانية الإعتماد على جهة التعريف يتعين على البنوك أن تستخدم المعايير التالية:

يجب أن تكون إجراءات العناية الواجبة المعمول بها من قبل جهة التعريف أشد من تلك التي كان البنك سوف يطبقها بالنسبة لنفس العميل. كما يجدر بالبنوك التأكد من إن إجراءات العناية الواجبة المطلوبة تشمل تلك المتبعة من جهة التعريف.

١. يجب على البنك أن يتأكد من إمكانية الاعتماد على النظم التي تستخدمها جهة التعريف للتحقق من هوية العميل.
٢. يجب على البنك أن يتوصل إلى اتفاق مع جهة التعريف بحيث يُسمح له بالتحقق من إجراءات العناية الواجبة التي تطبقها جهة التعريف في أي مرحلة.
٣. يجب على البنك أن يتوصل إلى اتفاق مع جهة التعريف يسمح له الحصول عند طلبه على كافة بيانات التعرّف على الهوية ومراجعتها بعناية، فضلاً عن المستندات الأخرى المتعلقة بجهة التعريف والعميل.
٤. يجب أن لا يعتمد قرار فتح الحساب فقط على سمعة جهة التعريف بل يجب أن تتم عملية معرفة العميل على كلّ من جهة التعريف وصاحب الحساب.
٥. يجب تصنيف هذه النوعية من الحسابات بأنها عالية المخاطر، وتحتاج الى إجراء العناية الواجبة المعززة للحسابات التابعة لتلك الجهات.
٦. يجب المتابعة بشأن المستجدات للعلاقات المصرفية المحالة بشكل مستمر.

6. Referred banking relationships developments must be followed up on a continuous basis.

2. Referred Business

This means a relationship referred by one branch to another, within one bank or externally from other banks inside or outside the country. In such cases, the branch/bank accepting the relationship should conduct normal KYC process. Due diligence should include full verification of the customer's identification and information, including beneficiaries owner, comprising the following steps:

1. Banks must take all reasonable steps to identify suspicious transactions. This should require banks to have a reasonable understanding of the normal nature of the customer's business, and having a reasonable understanding of the commercial basis of the transaction to be undertaken or service to be provided.
2. Where a foreign branch, subsidiary or associate refers business to a bank in Saudi Arabia, in addition to the above procedures, the bank should seek the full business rationale for the referral, and determine whether it complies with Saudi Arabian laws and regulations.
3. If the referred branch determines that it has insufficient information to enable it to accept the referral, the business must be declined and the referring branch, subsidiary or associate notified.

٢. <u>الاعمال المحالة</u>

يقصد بها إحالة علاقة مصرفية من فرع إلى آخر ضمن البنك الواحد ، أو من قبل بنوك اخرى داخلية او خارجية. وفي هذه الحال يقوم الفرع /البنك الذي قبل العلاقة بتطبيق الإجراءات المعتادة لمعرفة العميل ويجب أن تؤدي إجراءات العناية الواجبة هذه إلى التحقق الكامل من بيانات الهوية والمعلومات الخاصة بالعميل بما في ذلك المستفيدين الحقيقيين عبر المراحل التالية:

١. يجب على البنوك اتخاذ الخطوات اللازمة للتعرّف على العمليات المشتبه بها, لذلك عليها أن تفهم جيداً طبيعة عمل العميل والغرض التجاري للعملية المنفّذة أو الخدمة المقدّمة.
٢. في حال قام فرع خارجي، أو شركة تابعة أو مرتبطة بإحالة أعمال ما إلى أحد البنوك في المملكة العربية السعودية، يجب على البنك أن يبحث عن المبرر التجاري للإحالة ويحدّد مدى تقيّد تلك الجهة وبالأنظمة والتعليمات المحلية.
٣. إذا كان الفرع الذي أحيلت إليه الأعمال لا يملك المعلومات الكافية التي تمكّنه من قبول الإحالة، فعليه رفضها وإخطار الفرع الذي أحالها أو الشركة التابعة أو المرتبطة بذلك.

4.6.10 Correspondent Banking Relationships

Correspondent banking is the provision of banking services by one bank (correspondent bank) to another bank (respondent bank) by means of a correspondent account. Through the correspondent account, respondent banks can conduct transactions for themselves and for their customers in jurisdiction where they have no physical presence. These services include cash management, international wire transfers of funds, check collection, and foreign exchange services, which usually involve large amounts and numerous transactions.

Correspondent banking, by its nature, creates an indirect relationship whereby the correspondent bank carries out financial transactions for the respondent bank on behalf of its customers (individuals or entities) without having enough information about the customers or by relying on the information and KYC due diligence provided by the respondent bank. This anomaly, coupled with the fact that the respondent bank may have inadequate AML/CTF standards, poses additional risks in this relationship.

Therefore, banks and money exchangers who maintain correspondent banking relationships should take strict measures to prevent the use of their correspondent accounts for money laundering, terrorist financing and other illegal purposes. Prior to opening any account, banks should fully understand and appropriately document full details of the respondent bank's management and nature of the business. In addition to requirements relating to correspondent banks relationship as stipulated in SAMA Account Opening Rules, the following requirements should apply as minimum standards for opening and maintaining correspondent bank accounts:

1. Banks should not open a correspondent account for or deal with a Shell Bank.
2. Correspondent bank accounts shall not be opened before the approval of the compliance officer in addition to that of the chief executive officer/director.
3. Banks should immediately inform SAMA of opening correspondent bank account in Saudi Riyal.

١٠،٦،٤ علاقات البنوك المراسلة

علاقات البنوك المراسلة هي تقديم الخدمات البنكية من قبل أحد البنوك (البنك المراسل) إلى بنك آخر (البنك المتلقي) من خلال حساب مراسل فبواسطة هذا الحساب تتمكن البنوك المتلقية من إجراء العمليات لها ولعملائها في الدول التي لا يكون لها تواجد فعلي. وتشمل خدمات المراسلة إدارة النقد، والتحويلات البرقية الدولية للأموال، وتحصيل الشيكات والخدمات المرتبطة بالعملات الأجنبية والتي غالباً ما تتضمن مبالغ طائلة من الأموال وعمليات عديدة.

وبحكم طبيعتها تؤدي علاقات المراسلة البنكية إلى إنشاء علاقة غير مباشرة بحيث ينفّذ فيها البنك المراسل عمليات مالية لصالح البنك المتلقي وبالنيابة عن عملائه (سواء الأفراد أو المنشآت) من دون توفر المعلومات الكافية عن العملاء أو من خلال الاعتماد على المعلومات وإجراءات العناية الواجبة التي يقوم بها البنك المتلقي. وأن هذا الاستثناء مع عدم التأكّد من ملاءمة المعايير التي وضعها البنك المتلقي لمكافحة غسل الأموال وتمويل الإرهاب يعرّضان علاقة المراسلة البنكية إلى مخاطر إضافية.

وعليه فإنه يجب على البنوك ومحلات الصرافة الذين يقيمون علاقات المراسلة البنكية أن يتخذوا إجراءات مركزة لمنع استخدام الحسابات المراسلة لديهم لأغراض غسل الأموال وتمويل الإرهاب أو أغراض أخرى غير نظامية .وقبل فتح أي حساب من الحسابات فإنه يجب على البنوك أن تقوم بجمع معلومات كافية حول البنوك المتلقية مع التفاصيل المتعلقة بإدارة البنك المتلقي وطبيعة أعماله وتوثيق ذلك. وبالإضافة إلى المتطلبات الخاصة بحسابات البنوك المراسلة كما هو منصوص عليه في القواعد الخاصة بفتح الحسابات الصادرة عن مؤسسة النقد العربي السعودي فانه يجب تطبيق المتطلبات التالية كحدّ أدنى لفتح حسابات البنوك المراسلة والمحافظة عليها:

١. لا يجوز للبنوك أن تفتح حساباً للمراسلة لصالح البنوك الصورية ولا أن تتعامل معها.
٢. لا تفتح حسابات البنوك المراسلة إلا بعد الحصول على موافقة مدير إدارة الالتزام بالإضافة إلى موافقة الإدارة العليا (الرئيس التنفيذي/المدير العام) .
٣. يجب على البنوك إحاطة مؤسسة النقد حال فتح حسابات للبنوك المراسلة بالريال السعودي.
٤. يجب منع الأطراف الثالثة من تشغيل حسابات البنوك المراسلة
٥. تمنع الودائع النقدية المحلية. ولا يجوز القبول بهذا الإتفاق المعروف باسم "حسابات

4. Third parties are prohibited from operating correspondent bank accounts, .
5. local cash deposits should not be allowed. This arrangement, known as "Payable-Through Accounts" should not be accepted.
6. The correspondent bank should not be under sanctions by the UN or Saudi Arabia.
7. Banks should also determine from any available information (e.g., internet) whether the correspondent bank has been subject to any money laundering or terrorist financing investigations or regulatory action.
8. Banks should obtain certification of AML/CTF compliance for all correspondent relationships, which should include the following information:
   a. The location, major business activities, and management.
   b. That they are under jurisdiction of their central bank or a similar monitory authority and are committed to the FATF recommendations.
   c. That they are governed by and committed to AML/CTF and KYC policies and procedures.
   d. That they have procedures in place for reporting suspicious transactions.
   e. That they are not dealing with any Shell Bank.
   f. Any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing.
   g. The certification should be either renewed or confirmed by the correspondent bank every three years.
9. Banks and money exchangers should apply satisfactory due diligence on a continuous basis regarding the banking correspondence relationships, document the responsibilities of AML/CTF, which are the correspondent and receiving banks responsibilities and apply due diligence regarding all banking correspondence relationships, including correspondence relationships that already exist.

الدفع المراسلة".

٦. أن لا يكون البنك المراسل مدرجاً ضمن قوائم العقوبات أو الحظر المحلية أو الصادرة عن الأمم المتحدة.

٧. يجب على البنوك بالإستناد إلى أي مصادر معلوماتية متوفرة ومنها على سبيل المثال (شبكة الإنترنت) التحقق من مدى خضوع البنك المراسل لأي تحقيقات في مجال غسل الأموال أو تمويل الإرهاب أو لأي إجراءات قانونية اخرى.

٨. يجب على البنوك الحصول على شهادة تأكيد الالتزام بقواعد مكافحة غسل الأموال وتمويل الإرهاب لكافة علاقات البنوك المراسلة ومنها المعلومات التالية:

أ- موقع الأعمال وأنشطتها الرئيسية وإدارتها.

ب- خضوع البنوك المراسلة لسلطة البنك المركزي أو لهيئة رقابية مماثلة والتزامها بتوصيات مجموعة العمل المالي.

ج- خضوع البنوك المراسلة لسياسات وإجراءات مكافحة غسل الأموال وتمويل الإرهاب ومعرفة العميل والإلتزام بها.

د- وجود إجراءات للإبلاغ عن العمليات المشتبه بها.

هـ- عدم التعامل مع أي بنك صوري.

و- الحصول على أي معلومات أخرى ذات صلة تضمن أن البنك المراسل يولي موضوع مكافحة غسل الأموال وتمويل الإرهاب عناية كافية.

ز- يجب على البنك المراسل تجديد الشهادة أو تحديثها كلّ ثلاث سنوات.

٩. يجب على البنوك ومحلات الصرافة تطبيق إجراءات كافية للعناية الواجبة بشكل مستمر تجاه علاقات المراسلة المصرفية وتوثيق مسئوليات مكافحة غسل الأموال وتمويل الإرهاب التي تقع على عاتق البنك المراسل والبنك المستقبل وتطبيق إجراءات العناية الواجبة تجاه كافة العلاقات المراسلة المصرفية بما في ذلك علاقات المراسلة القائمة بالفعل.

4.7 Operations Monitoring

4.7.1 Monitoring Process

Monitoring process of operations means pursuance actions of all operations conducted by all permanent or casual customers to deduct any unusual operations. Banking Control Law, money exchanging regulating decision and article 6 of the Saudi AML Law require all financial institutions to take actions to monitor operations and have in place internal precautionary and supervisory measures to detect and foil any of the offences stated herein, and comply with all instructions issued by the concerned supervisory authorities in this area.

The size of the bank or money exchanger, the AML/CTF risks it faces, number and volume of transactions and the type of activity under scrutiny will impact the degree and nature of monitoring. In applying a risk-based approach to monitoring, banks and money exchangers must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the perceived risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. The principal aim of monitoring in a risk-based system is to respond to institution-wide issues based on each bank's or money exchanger's analysis of its major risks. As a general rule, banks and money exchangers should however ensure that all customer transactions are being monitored.

٧،٤ مراقبة العمليات

١،٧،٤ عملية المراقبة

يقصد بعملية مراقبة العمليات إجراءات متابعة لجميع العمليات التي يجريها كافة العملاء الدائمين أو العرضيين بهدف الكشف عن أي عمليات غير طبيعية، ويلزم نظام مراقبة البنوك وقرار تنظيم مهنة الصرافة ونظام مكافحة غسل الأموال في المادة السادسة منه كافة المؤسسات المالية بوضع إجراءات لمراقبة العمليات وإتخاذ تدابير داخلية إحترازية ورقابية لرصد وإحباط أي من المخالفات المنصوص عليها في النظام والتقيّد بكافة التعليمات الصادرة عن السلطات الرقابية المعنية في هذا المجال.

وتؤثّر العوامل المختلفة مثل حجم البنك أو محل الصرافة والمخاطر التي يتعرض لها في مجال مكافحة غسل الأموال وتمويل الإرهاب وعدد العمليات وحجمها ونوع النشاط الخاضع للرقابة على درجة المراقبة وطبيعتها. وعند تطبيق الأسلوب المرتكز على المخاطر في مجال المراقبة، فإنه يجب على البنوك ومحلات الصرافة أن تعرف أن العمليات والحسابات أو العملاء لن يخضعوا لنفس مستوى إجراءات الرقابة حيث تختلف درجة الرقابة بحسب المخاطر المرتبطة بالعميل وبالمنتجات أو الخدمات التي يستعملها وبموقعه وموقع عملياته. ويبقى الهدف الأساسي من المراقبة بحسب درجة المخاطر هو التعامل مع المخاطر الرئيسية المفروضة على البنك أو محل الصرافة بحسب ما يحددها بناء على عمليات التحليل إلا أن القاعدة العامة تقتضي بأن تتأكد البنوك ومحلات الصرافة من إخضاع كافة العمليات التي يجريها العملاء للمراقبة اللازمة.

Risk-based approach monitoring allows banks and money exchangers to create financial thresholds below which an activity review procedures will be mitigated, and clarify justifications on which these thresholds are based. Thresholds used for this purpose should be reviewed on a continuous basis to assess capability of the risk levels established. Banks and money exchangers should also assess the adequacy of any systems and processes.

Banks and money exchangers should pay special attention, control all operations and use an electronic monitoring system to facilitate the monitoring process through deducting unusual changes and internal alerts and reports identifying unusual transactions or activity for further examination. The appropriateness and sophistication of automated monitoring system will depend on the relevance of the parameters to the nature of business undertaken by each bank or money exchanger.

Certain types of transactions or group of events should alert banks and money exchangers to the possibility that the customer is conducting suspicious activities. For example:

1. Unusual patterns of transactions that do not have apparent or visible economic, lawful or commercial purpose;
2. Events that involve complex transactions;
3. Unusual large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer;
4. Very high account turnover, inconsistent with the size of the balance;
5. Transactions connected with entities or individuals, who are the subject of the local or UN sanctions;
6. Business relationship or transactions with entities or individuals from or in countries which do not sufficiently apply the FATF Recommendations or have weak AML/CTF systems.
7. A customer who provides false or misleading information, refuses to provide relevant information, or refuses to provide his/her identity or whose identity cannot be verified.
8. Requests for information received from domestic and international correspondent banks in regard to inquiries about the operations and activities of some customers.
9. Requests for disclosure of customer balances and accounts and inquiries received from the local supervisory and regulatory authorities.
10. Requests for seizure and operation prohibition received from local authorities, international organizations and lists of other countries.

All the above may indicate the existence of money laundering or terrorist financing transactions through the account. The background and purpose of such transactions should be examined as far as possible and documented in writing. Those results should be provided upon request by the supervisory authority and be retained at least for 10 years, and suspicious transactions should be reported in writing to FIU.

When applying risk-based monitoring approach for money laundering and terrorist financing, the following points should be taken into consideration:

1. No transaction shall be excluded from monitoring.
2. Transaction amount shall not be a factor of risk determination.
3. Focus is given on particular high-risk businesses and accounts.

ومن خلال معيار تحديد المخاطر، يصبح بإمكان البنوك ومحلات الصرافة وضع حدود مالية تمكنه من تخفيف إجراءات مراجعة أي نشاط يقع دون مستواها مع إيضاح المبررات التي بناءً عليها تم وضع هذه الحدود ، ويجب القيام بالمراجعة المستمرة لهذه الحدود المالية وتقدير إمكانية الاستمرار بها في ظل مستويات المخاطر المختلفة. كما يجب على البنوك ومحلات الصرافة إجراء عمليات التقييم المستمر للتأكد من ملائمة الأنظمة والعمليات.

كذلك يجب على البنوك ومحلات الصرافة إيلاء عناية خاصة ومراقبة جميع العمليات واستعمال نظم آلية لتسهيل عملية المراقبة من خلال كشف المتغيرات غير الطبيعية والإنذارات والبلاغات الداخلية التي تحدّد العمليات أو الأنشطة غير العادية والمطلوب إخضاعها لمراقبة إضافية. ويعتمد مدى تعقيد ومناسبة النظام على ملائمته لمعايير وطبيعة الأعمال التي ينفّذها كل بنك أومحل صرافة.

ان من شأن بعض أنواع العمليات أو مجموعة من الأحداث أن تنبه البنوك ومحلات الصرافة عن إمكانية ممارسة العميل لأنشطة مشتبه بها والتي من بينها على سبيل المثال مايلي:

١. الأنماط غير العادية للعمليات التي لا تحقق هدفاً إقتصادياً أو قانونياً أو تجارياً واضحاً أو ظاهراً.
٢. الأحداث التي تتضمن عمليات معقّدة.
٣. مبالغ كبيرة غير إعتيادية من الودائع النقدية والتي لا تتماشى مع العمليات الطبيعية والمتوقعة للعميل.
٤. العائدات العالية جداً على الحسابات على نحو لا يتلاءم مع حجم الرصيد.
٥. العمليات المتصلة بالمنشآت أو الأفراد الخاضعين لعقوبات محلية أو مفروضة من الأمم المتحدة.
٦. علاقات الأعمال أو العمليات مع المنشآت أو الأفراد من/في الدول التي لا تطبق على نحو كامل توصيات مجموعة العمل المالي أو تعاني من ضعف في أنظمتها الخاصة بمكافحة غسل الأموال وتمويل الإرهاب.
٧. العميل الذي يقدم معلومات خاطئة أو مضللة، أو يرفض تقديم المعلومات المطلوبة أو الإفصاح عن هويته أو العميل الذي لا يمكن التحقق من هويته.
٨. طلبات الاستعلام الواردة من البنوك المراسلة الداخلية والخارجية بشان الاستفسار عن عمليات وانشطة بعض العملاء.
٩. طلبات الكشف عن ارصدة وحسابات العملاء والاستفسارات الواردة من السلطات الاشرافية والرقابية المحلية.
١٠. طلبات الحجز والحظر على التعامل الواردة من السلطات المحلية والمنظمات الدولية وما يدرج ضمن قوائم الدول الاخرى.

ويمكن لمجمل العناصر المذكورة اعلاه أن تشير إلى وجود شبه بعمليات غسل للأموال أو تمويل الإرهاب عبر الحساب البنكي. لذلك يجب فحص خلفية هذه العمليات والغاية منها قدر المستطاع وتوثيق ما تم التوصل اليه كتابياً وإتاحة تلك النتائج عند طلبها من قبل السلطة الإشرافية والاحتفاظ بها لمدة عشر سنوات على الأقل, والإبلاغ عن حالات الإشتباه خطياً إلى وحدة التحريات المالية.

كما يجب أخذ النقاط التالية في الإعتبار عند تطبيق أسلوب الرقابة المرتكز على المخاطر في مكافحة غسل الأموال أو تمويل الإرهاب وذلك على النحو التالي:

١. أن لاتستثنى أي عملية من الرقابة.
٢. ان لا تشكّل قيمة العملية عاملاً لتحديد الخطر.
٣. التركيز على الأعمال والحسابات ذات عالية المخاطر.
٤. التركيز على بعض الأفراد والمنظمات والدول المحددة.
٥. يجب على البنوك ومحلات الصرافة قبل تطبيق الأسلوب المرتكز على المخاطر أن تحدد مجموعة أكثر شمولية من المؤشرات المعتمدة والمرتبطة بأساليب وتقنيات غسل الأموال أو تمويل الإرهاب. ويمكن تحويل هذه المؤشرات إلى إستراتيجيات لتقييم خطر غسل الأموال أو تمويل الإرهاب وتصميم الضوابط للتخفيف من هذه المخاطر.

4. Focus is given for particular individuals, organizations and countries.
5. Before applying risk-based approach, banks and money exchangers should identify a more comprehensive set of indicators of the method and techniques used for money laundering and terrorist financing, which can then be turned into strategies to assess money laundering and terrorist financing risk and devise controls to mitigate such risk.

4.7.2 Financial Investigation Process

Banks and money exchangers should have a process in place for the financial investigation and analysis of unusual customer activity or transactions, which should include the expected frequency, size, volume and origin/ destination of customer funds whether specific to an individual customer, or for a generic customer, type or product type; and the presence of risk factors specific to the bank's or money exchanger's nature of the activity and customer base.

The investigation and analysis of the unusual and higher risk activity and transactions should be conducted by an independent reviewer, and should include the following:

1. Reviewing the identified activity/ transaction in light of the customer risk assessment and the customer due diligence information that it holds;
2. Making further enquiries to obtain additional information required to enable a determination as to whether the activity/ transaction has a rational explanation;
3. Considering the activity/ transaction in the context of any other relationships connected with the customer by referring to the relevant customer due diligence information and making enquiries to reach for appropriate conclusions;
4. Updating customer due diligence information to record the results of the enquiries made;
5. Not to alert the customer that his transactions are under review, monitoring etc.
6. Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and additional customer due diligence information obtained;
7. Considering whether further improvements of the monitoring process is required (staff training, enhancing the monitoring system parameters, strengthening controls for more vulnerable products/ services);
8. Applying increased levels of monitoring to particular relationships;
9. Where the activity or transaction does not have a rational explanation, considering whether the circumstances require a suspicious activity report to be submitted to the bank's or money exchanger's Money Laundering Control Unit (MLCU) or designated Compliance Officer.
10. In case a bank or money exchanger, through its monitoring and investigation process, finds that an activity or transaction of a customer is suspicious, further due diligence should be conducted including re-verifying the customer's information, obtaining additional information, and re-assessing the relationship.

4.7.3 Transaction Monitoring Reinforcement

Monitoring high-risk transactions conducted throughout the relationship period should be strengthened and enhanced, taking in consideration the importance of compliance with requirements of identity verification procedures, due diligence procedures and transactions monitor despite their nature & amount.

٤،٧،٢ عملية التتبع المالي (التحقق)

يجب على البنوك ومحلات الصرافة وضع آلية للتتبع (التحقق) والتحليل المالي للأنشطة أو العمليات غير العادية التي يقوم بها العملاء، بحيث تتضمن عدد مرات تكرار وحجم ومصدر أو وجهة أموال العملاء المتوقعة، سواء كانت تخص عميلاً واحداً أو مجموعة من العملاء أو لنوع من المنتجات، فضلاً عن وجود عوامل المخاطر الخاصة بطبيعة نشاط البنك أو محل الصرافة وبقاعدة عملائه.

كما يجب أن تتم إجراءات التتبع والتحليل في النشاط والعمليات غير المعتادة وذات المخاطر العالية من قبل مراجع مستقلّ بحيث تتضمن ما يلي:

١. مراجعة النشاط/العملية في ضوء تقييم مخاطر العميل ومعلومات العناية الواجبة الخاصة به.
٢. طلب الحصول على معلومات إضافية والتي تسمح بإيجاد تفسير منطقي للنشاط/العملية.
٣. الأخذ في الاعتبار وضع النشاط/العملية في سياق أي علاقات أخرى مرتبطة بالعميل من خلال الرجوع إلى معلومات العناية الواجبة الخاصة بالعميل وعمل الإستفسارات للوصول إلى نتائج مناسبة.
٤. تحديث معلومات العناية الواجبة لتسجيل نتائج الإستفسارات التي تمت في هذا الخصوص.
٥. عدم تنبيه العميل أن معاملاته قيد المراجعة أو المراقبة ونحو ذلك.
٦. مراجعة مدى ملاءمة تقييم مخاطر العميل في ضوء النشاط غير الاعتيادي الذي قام به العميل والمعلومات الإضافية التي تم التوصل إليها من خلال العناية الواجبة لهذا العميل.
٧. التحسين المستمر لعملية المراقبة (كتدريب الموظفين، وتحسين معايير نظام المراقبة، وتعزيز الضوابط للمنتجات/الخدمات الأكثر عرضة للمخاطر).
٨. زيادة مستويات الرقابة على بعض العلاقات المحددة.
٩. في حال عدم وجود تفسير منطقي للنشاط أو العملية، يجب دراسة الظروف المحيطة لمعرفة مدى الحاجة إلى إعداد تقرير عن العملية المشتبه بها لتقديمه إلى وحدة مراقبة غسل الأموال أو إلى مسؤول الالتزام لدى البنك أو محل الصرافة.
١٠. في حال إكتشف البنك أو محل الصرافة، عبر عملية المراقبة والتتبع، ان نشاط العميل أو العملية التي يجريها يثير/تثير الشبهات، عليه يجب تعزيز إجراءات العناية الواجبة، بما في ذلك إعادة التحقق من المعلومات التي قدّمها العميل، والحصول على معلومات إضافية وإعادة تقييم العلاقة معه.

٤،٧،٣ تعزيز مراقبة العمليات

يجب تشديد وتعزيز الرقابة على جميع العمليات ذات المخاطر العالية التي تتم طوال فترة العلاقة، مع الأخذ في الاعتبار ضرورة التقييد بمتطلبات إجراءات التحقق من هوية العملاء وإجراءات العناية الواجبة ومراقبة العمليات بغض النظر عن طبيعتها وقيمتها.

4.8 Suspicious Transaction

4.8.1 Reporting Suspicious Transactions

The reporting of suspicious transaction or activity is critical to the competent authorities' ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. The Saudi AML Law and its implementation regulation and SAMA Rules require banks and money exchangers to file Suspicious Transaction Report (STR) once a suspicion has been formed.

The AML Law and its implementation regulation shall be applicable to banks, money exchangers and their employees. Employees whose suspicions are aroused, but who then deliberately fail to make further inquiries, wishing to remain ignorant or demonstrate "willful blindness", may be considered under the Saudi AML Law to have the requisite knowledge. However, the Saudi AML Law relieve the bank or money exchanger, management and employees from any liability that may be caused by performing the duties provided for or by violating the provisions of confidentiality, unless it is established that they have acted in bad faith to hurt the involved person.

Thus, banks and money exchangers reporting policy should mandate employees to do the following:

1. If an employee suspects that a money laundering transaction is taking place, he/she should immediately report it to the bank's or money exchanger's internal MLCU or designated Compliance Officer. (Refer to **Rule 4.7.4** for details).
2. Attempts of suspicious transactions, which have been identified as suspicious but were foiled before occurrence, must be reported.
3. Banks and money exchangers should make available, to the appropriate authorities all documents, statements and related transactions.
4. All documents, reports and information relating to internally investigated cases not reported to the authorities for lack of suspicion, should be maintained by the bank and money exchanger for record purposes in accordance with records documentation referred to in Article 4.11.
5. It is a criminal offence for bank or money exchanger employees to tip off or assist any customer or individual that they know or suspect of having been involvement in any money laundering or terrorist financing activities. If an employee thinks that a transaction may be related to a criminal activity, this must be immediately reported to the bank's or money exchanger's MLCU/ Compliance Officer.
6. The notifying bank or money exchanger and its employees are free of any blame or charge in respect of any AML/CTF notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

٨،٤ العمليات المشتبه بها

١،٨،٤ الإبلاغ عن العمليات المشتبه بها

يعد التبليغ عن عملية أو نشاط مشتبه به عنصراً هاماً لتعزيز قدرة السلطات المختصة على استخدام المعلومات المالية في مكافحة غسل الأموال وتمويل الإرهاب والجرائم المالية الأخرى ، لذا فإنه من الواجب على البنوك ومحلات الصرافة أن يلتزموا بالتبليغ عن العمليات المشتبه بها وذلك بموجب نظام مكافحة غسل الأموال ولائحته التنفيذية وقواعد مؤسسة النقد

وتسري أحكام نظام مكافحة غسل الأموال ولائحته التنفيذية على البنوك ومحلات الصرافة والموظفين لديهم. وبحسب أحكام نظام مكافحة غسل الأموال يجوز اعتبار الموظفين الذين تعمدوا الإخفاق في التبليغ بالرغم من اشتباههم بعملية غسل الأموال رغبة منهم في غضّ النظر أو القيام بـ"الإغفال المتعمد"، بحكم العالمين بعملية غسل الأموال. وفي الوقت نفسة فإن نظام مكافحة غسل الأموال ولائحته التنفيذية تعفيان البنك أو محل الصرافة، وإدارتهم وموظفيهم من أي مسؤولية قد تنشأ من تنفيذ الواجبات المنصوص عليها في النظام أو حين الخروج عن أي قيد مفروض لضمان سرية المعلومات ما لم يثبت أن ما قاموا به قد تم بسوء نية بقصد الإضرار بصاحب العملية.

لذا يجب أن تلزِم سياسة الإبلاغ المعتمدة من قبل البنوك ومحلات الصرافة الموظفين بالقيام بالمهام التالية:

١. يجب على كل موظف في حالة اكتشافة او اشتباهة بعملية غسل اموال أو تمويل إرهاب أن يبلغ وحدة المراقبة الداخلية لغسل الأموال أو مسؤول الالتزام في البنك أو محل الصرافة (لمزيد من التفاصيل، راجع **القاعدة ٤،٨،٤**)
٢. يجب الإبلاغ عن محاولات القيام بالعمليات المشتبه بها التي تمّ رصدها لكنها منعت قبل حدوثها.
٣. يجب على البنوك ومحلات الصرافة أن يضعوا كافة الوثائق والبيانات والعمليات ذات الصلة بالعملية المبلغ عنها في متناول السلطات المختصة.
٤. يجب على البنك ومحل الصرافة المحافظة على كافة المستندات والتقارير والمعلومات المتصلة بالحالات التي جرى التحقيق فيها داخلياً وإن لم يتم الإبلاغ عنها للسلطات لعدم الاشتباه بها وذلك لأغراض التسجيل. وفقاً لمتطلبات حفظ السجلات المشار إليها في الفقرة ١١،٤.
٥. يعتبر قيام الموظفين في البنك أو محل الصرافة بالتلميح أو تنبيه أو مساعدة أي عميل أو فرد وهم يدركون أو يشتبهون في ضلوعه في أي أنشطة لغسل الأموال أو تمويل الإرهاب بمثابة جريمة جنائية. وإذا ظنّ الموظف أن العملية قد تكون مرتبطة بنشاط إجرامي عليه أن يبلغ عنها على الفور لوحدة مراقبة غسل الأموال أو مسؤول الالتزام في البنك أو محل الصرافة.
٦. يُعفي البنك أو محل الصرافة أو الموظف المبلغ من أية مسؤولية نتيجة تبليغه للجهة المختصة عن شبهة غسل أموال أو تمويل إرهاب سواء ثبتت صحة الاشتباه بها أو لم تثبت، طالما أن التبليغ قد تم بحسن نية.

4.8.2 Reporting Requirements

According to the AML Law, financial institutions including banks and money exchangers are required to report all transactions suspected to relate to money laundering or terrorist financing, including any attempts to conduct such transactions, to FIU. The Law also requires banks and money exchangers to submit a detailed report including all available information and supporting documentation on the parties involved, and provide it to the FIU. In order to achieve the requirements above, the following should be observed:

i. Reporting should be in accordance with the form approved by the FIU and the form of the provided by SAMA, and should contains the following:

1. Names of suspected individuals/ entities, their identifies, addresses and phone numbers.
2. Statement with respect to the suspected transaction/s, the involved parties, how it was discovered and present condition/ status.
3. The exact amount of the suspected transaction/s and related banking accounts.
4. Reasons of suspicion upon which the bank or money exchanger staff had depended/ based on.

ii. Banks and money exchangers should provide the technical report on reported cases to the FIU within 10 days from the reporting date, including the following:

1. Ensure completion of all the data and filling in of all fields in the reporting form regarding suspected transactions, including any attempted transactions, related to money laundering, indicating the name of the branch and the region, where the suspected account is domiciled;
2. Submit the original suspicion report, statement of account of 6 months, attachments of account (opening account documents) and technical report on studying the reported account to the FIU.

iii. Take the following actions after reporting:

1. keep records, copies of the report and notification, the technical record and its attachment to be used as a reference in future.
2. Follow-up the reported customer activity. In case the suspected activities persist and no feedback is received from the FIU within two months of the date of notification, the notification should be reconfirmed by reporting the same to the FIU.
3. Follow-up the report to the FIU concerning a feedback on all reports after six months from the date of reporting.

٢,٨,٤ متطلبات الإبلاغ

يقتضي نظام مكافحة غسل الأموال أن تقوم المؤسسات المالية بما فيها البنوك ومحلات الصرافة بإبلاغ وحدة التحريات المالية عن جميع العمليات المشتبه بأن لها علاقة بغسل الأموال أو تمويل الإرهاب بما في ذلك أي محاولات متعلقة بإجراء مثل هذه العمليات، كما يقتضي النظام أن تقوم البنوك ومحلات الصرافة بإعداد تقرير مفصل عن هذه العمليات يتضمن جميع البيانات والمعلومات المتوافرة لديها عن تلك العمليات والأطراف ذات الصلة، وتزويد وحدة التحريات المالية بها. ولتحقيق ما أشير إليه أعلاه بشأن الإبلاغ والتقرير الفني يراعى التالي:

أ- يكون الإبلاغ وفق النموذج المعتمد من وحدة التحريات المالية والمبلغ بشأنه من مؤسسة النقد العربي السعودي على أن يحتوي على مايلي:

١. أسماء الأفراد/المنشآت المشتبه بهم/بها، وهويتهم وعناوينهم وأرقام هواتفهم.
٢. بيان عن العملية/العمليات المشتبه بها والأطراف المشتركة بها وطريقة اكتشافها وحالتها/وضعها الراهن.
٣. المبلغ الصحيح للعملية/العمليات المشتبه بها والحسابات البنكية المرتبطة بها.
٤. أسباب الإشتباه التي اعتمد عليها/استعملها موظفو البنك أو محل الصرافة.

ب- تقدم البنوك ومحلات الصرافة التقرير الفني عن حالات الإبلاغ لوحدة التحريات المالية خلال عشرة أيام من تاريخ التبليغ على أن يتضمن الآتي:

١. التأكد من استكمال كافة البيانات وتعبئة كافة الخانات في نموذج الإبلاغ فيما يتعلق بالعمليات المشتبه بها المرتبطة بغسل الأموال، من خلال ذكر إسم الفرع والمنطقة حيث تم فتح الحساب المشتبه به.
٢. إرسال أصل البلاغ مع كشف الحساب لمدة ستة أشهر ومرفقات الحساب (مستندات فتح الحساب) وتقرير فني عن دراسة الحساب محل البلاغ إلى وحدة التحريات المالية.

ج- ان تتخذ البنوك ومحلات الصرافة الاجراءات التالية ما بعد مرحلة الابلاغ:

١. الإحتفاظ بسجلات ونسخ من البلاغ والتقرير الفني وملحقاته في البنك أو محل الصرافة للاستفادة منها كمرجع في المستقبل.
٢. متابعة نشاط العميل محل البلاغ وفي حال استمرار نشاطاته المشتبه بها وعدم ورود تغذية عكسية من وحدة التحريات المالية خلال فترة شهرين من تاريخ الابلاغ القيام باجراء تعزيز بلاغ للوحدة بشانها.
٣. متابعة الطلب من وحدة التحريات المالية بشان الحصول على تغذية عكسية عن جميع البلاغات بعد مضيء ستة اشهر من تاريخ الابلاغ.

4.8.3 Tipping Off

Banks and money exchangers and their directors, officers and employees should not disclose the fact that a customer is being or has been investigated or reported for a suspicious transaction. Banks and money exchangers should exercise extreme caution when performing additional customer due diligence (CDD) because of suspicious transaction, so as not to unintentionally tip off the customer. In case the bank or money exchanger feels the performance of CCD may tip off the customer, it could then decide to discontinue the CDD but to file a suspicious activity report to FIU.

The Saudi AML Law and Bylaws prohibit financial institutions and their employees from alerting customers or other related parties about suspicions of their activities or about their notification to the authorities. The Saudi AML Law, notification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi

٣,٨,٤ التلميح وتنبيه العملاء

لا يجوز للبنوك ومحلات الصرافة ومدرائهم ومسؤوليهم وموظفيهم الإفصاح عن خضوع أحد العملاء للتحقيق أو للتبليغ من جرّاء عملية مشتبه بها. ويجب على البنوك ومحلات الصرافة توخي الحذر أثناء تعزيز إجراءات العناية الواجبة للعميل بناءً على الاشتباه به كي لا يتمّ التلميح بذلك إلى العميل بشكل غير متعمّد. وفي حال رأى البنك او محل الصرافة أن عمل إجراءات العناية الواجبة سيؤدي إلى تنبيه العميل حينئذ يستطيع إيقاف هذا الإجراء ورفع بلاغ اشتباه بشانه إلى وحدة التحريات المالية .

يحظّر نظام مكافحة غسل الأموال ولائحته التنفيذية على المؤسسات المالية وموظفيها تحذير العملاء أو الأطراف الأخرى المرتبطة بهم بالشبهات التي تحوم حول أنشطتهم أو بالإبلاغ عنها إلى السلطات, وبالوقت نفسه ينص نظام مكافحة غسل الأموال على أن إبلاغ السلطات بالحالات المشتبه بها في مجال غسل الأموال وتمويل الإرهاب لا يتعارض مع توفير السرية المصرفية أو سرية العميل بموجب الانظمة والتعليمات المصرفية السعودية.

banking laws and regulations.

4.8.4 Money Laundering Control Unit (MLCU)

Banks and money exchangers must establish an independent and dedicated function to handle money laundering and terrorist financing control and reporting activities. For banks and money exchangers, with five branches and less this function can be handled by the designated Compliance Officer for the bank or money exchanger. For banks and money exchangers with more than five branches, an independent and dedicated Money Laundering Control Unit should be established with adequate staff. In both the above situations, the designation of the MLCU staff or Compliance Officer to handle the money laundering and terrorist financing control function, should be a Saudi, of senior management position within the bank or money exchanger, knowledgeable of the compliance function and reporting directly to the General Manager or Managing Director of the bank or money exchanger.

The officer-in-charge of the money laundering control function, as an individual or a unit, should have sufficient authority, independence, accountability and resources, and he/she should be granted timely access to customer information (such as identification data, due diligence information, transaction records and other relevant data) to enable him/her to discharge his/her functions effectively.

MLCU, or designated Compliance Officer, will have the following functions and responsibilities:

1. Monitoring of all transactions for the purpose of detecting activities that may involve money laundering and terrorist financing activities.
2. Receiving suspicious transactions relating to money laundering and terrorist finance from branches, transfer centers and various internal departments of the bank or money exchanger, and taking necessary actions for collection of information about it, analysis of the data collected, and making necessary decision for taking appropriate action, which should be documented in writing.
3. Reporting suspicious transactions to the Saudi Financial Intelligence Unit (SAFIU), when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspected case.
4. Developing electronic programs for controlling and detecting unusual operations as well as large cash transactions and complex operations which have no legal or economic purpose and other operations that may have a connection with activities of money laundering and terrorism financing, and updating the indicators that reflect existence of suspicious money laundering and terrorism financing acts in a manner consistent with the development and diversity of the techniques adopted in committing financial crimes
5. Submission of proposals targeting development of internal policies, plans, procedures and controls along with methods for facilitating application of the same. Approval of a state-of-the art automated system in the area of anti-money laundering.
6. Ensuring that staff, in branches and other departments, comply with the instructions and procedures pertaining to accounts monitoring; and ensuring that employees understand the importance of such procedures and instructions as well as the importance of the adopted procedures for suspicious activities and reporting requirements.
7. Supporting of Compliance Department in its task of verifying that the established rules, regulations and

٤,٨,٤ وحدة مراقبة غسل الأموال

يجب على البنوك ومحلات الصرافة إنشاء وحدة مستقلة ومتخصصة لمراقبة عمليات غسل الأموال وتمويل الإرهاب والتبليغ عنها. ويمكن أن يتولّى مسؤول الالتزام هذه الوظيفة في البنوك ومحلات الصرافة التي لديها خمسة فروع أو أقل. أمّا في البنوك ومحلات الصرافة التي لديها أكثر من خمسة فروع فيجب إنشاء وحدة مستقلّة ومتخصصة لمراقبة غسل الأموال وتزويدها بالموظفين المناسبين وفي كلا الحالتين يتم تعيين الموظفين أو مسؤول الالتزام في هذه الوحدة لتولي مهام مراقبة غسل الأموال وتمويل الإرهاب من بين المواطنين السعوديين الذين يتبوؤن منصباً إدارياً عالي في البنك أو محل الصرافة، على أن يكونوا ملمين بوظيفة الالتزام ويتبعون مباشرة إلى المدير العام أو المدير التنفيذي للبنك أو محل الصرافة.

كذلك يجب أن يتمتع المسؤول عن وظيفة مراقبة غسل الأموال، سواء كفرد أو كوحدة بالسلطة الكافية والإستقلالية والمسؤولية والموارد الضرورية, وأن يتمكّن من الاطلاع والوصول في الوقت المناسب إلى المعلومات الخاصة بالعميل (مثل بيانات تحديد الهوية، ومعلومات العناية الواجبة، وسجلات العمليات وسائر البيانات ذات الصلة) ليقوم بتأدية مهامه على أكمل وجه.

وستكون مهام ومسؤوليات وحدة مراقبة غسل الأموال أو مسؤول التزام في البنك أو لدى محل الصرافة كالتالي:

١. مراقبة جميع العمليات من أجل رصد الأنشطة التي قد تتضمن عمليات غسل للأموال أوتمويل للإرهاب.
٢. تلقي البلاغات عن العمليات المشتبه بها المتعلقة بغسل الأموال أوتمويل الإرهاب من الفروع ومراكز التحويل والإدارات الداخلية المختلفة في البنك أو لدى محل الصرافة واتخاذ الإجراءات اللازمة بجمع المعلومات عنها وتحليلها واتخاذ القرار اللازم لتنفيذ الإجراء المناسب وتوثيقه كتابياً.
٣. القيام بعملية الإبلاغ عن العمليات المشتبة بها إلى وحدة التحريات المالية السعودية فور تحديد الاشتباه، وذلك وفقاً لإجراءات التبليغ المتبعة مع إعداد تقرير فني مفصّل عن الحالة المشتبه بها خلال المدة المحددة.
٤. تطوير برامج آلية لمراقبة واكتشاف العمليات غير الاعتيادية وكذلك العمليات النقدية الضخمة والعمليات المعقدة والتي ليس لها غرض قانوني او اقتصادي وغيرها من العمليات التي قد يكون لها ارتباط بأنشطة غسل الأموال وتمويل الارهاب وتحديث المؤشرات التي تظهر وجود أعمال مشتبه بها كعمليات غسل للأموال وتمويل الارهاب على نحو يواكب تطور وتنوع التقنيات المعتمدة في ارتكاب الجرائم المالية.
٥. تقديم المقترحات الهادفة إلى تطوير السياسات والخطط والإجراءات والضوابط الداخلية ووضع المناهج لتسهيل تطبيق هذه المقترحات والموافقة على إنشاء نظام آلي حديث في مجال مكافحة غسل الأموال.
٦. التأكّد من أن الموظفين في الفروع والإدارات الأخرى يتقيّدون بالتعليمات والإجراءات المتعلقة بمراقبة الحسابات وانهم يدركون أهمية التعليمات والإجراءات المعتمدة لمكافحة الأنشطة المشتبه بها وتلبية متطلبات الإبلاغ.
٧. دعم إدارة الالتزام في التحقق من تطبيق القواعد والتنظيمات والمتطلبات الموضوعة بشكل فعّال وفقاً لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب.
٨. إنتقاء الموظفين المؤهلين لشغل المناصب في الوحدة وتطوير مواد التدريب والاستمرار في تدريبهم لتزويدهم بآخر المعلومات حول أنشطة غسل الأموال وتمويل الإرهاب بغرض تحسين معرفتهم في تحديد هذه الأنشطة وأنماطها وطبيعتها وكيفية تفاديها ومعالجتها.
٩. إعداد وتقديم التقارير الدورية عن الأنشطة التي تمارسها وحدة مراقبة غسل الأموال/مسؤول الالتزام المعين لمكافحة أنشطة غسل الأموال وتمويل الإرهاب وعن الوضع العام للبنك أو محل الصرافة وإداراته وفروعه المختلفة، كما يجب دعم هذه

requirements are effectively applied in compliance with AML/CTF requirements.
8. Selection of qualified staff to fill the positions in the unit and the development of ongoing training materials to provide them with latest information on money laundering and terrorist financing activities, with the aim of enhancing their knowledge to identify such activities, trends and nature of activities, and how these can avoided and dealt with.
9. Preparation and submission of periodic reports regarding the activities conducted by MLCU/ designated Compliance Officer for money laundering and terrorist financing activities as well as the general status of the bank or money exchanger and its various departments and branches vis-à-vis this matter which need to be supported by statistical data for those activities, and recommendations made for their development/ improvements.
10. Responding to all SAMA's circulars and requests relating to customer accounts statements and blocking, and preparation of the required information in the proper form and timeframe.
11. Maintaining a database comprising all data relating to money laundering and terrorist financing matters in the bank or money exchanger, such as the suspicious cases reported, blocked accounts, etc. and updating of all the old cases in the database.
12. Making appropriate continuous supervisory visits to the banks' various sectors and departments, including branches and money transfer centers.
13. Participation in the Financial Crimes and Money Laundering Committee.
14. Participation in the process of educating and training all the bank staff categories and all customers segments.

التقارير بالبيانات الإحصائية عن تلك الأنشطة وبالتوصيات الصادرة لتطويرها وتحسينها.

١٠. الالتزام التام بكافة التعاميم والطلبات الصادرة عن مؤسسة النقد بشأن كشوفات حسابات العملاء وتجميدها وإعداد المعلومات المطلوبة بالطريقة الملائمة وضمن الإطار الزمني المناسب.

١١. الاحتفاظ بقاعدة بيانات تتضمن كافة البيانات المتعلقة بمسائل غسل الأموال وتمويل الإرهاب في البنك أو محل الصرافة كالحالات المشتبه بها التي تمّ الإبلاغ عنها والحسابات المجمّدة، إلخ... فضلاً عن تحديث كافة الحالات السابقة في قاعدة البيانات.

١٢. القيام بإجراء زيارات رقابية مستمرة لمختلف قطاعات وإدارات البنك بما في ذلك الفروع ومراكز التحويل.

١٣. المشاركة في أعمال اللجنة المصرفية لمكافحة الجرائم المالية وغسل الأموال.

١٤. المشاركة بعملية التوعية والتدريب لمختلف الفئات الوظيفية في البنك وكافة شرائح العملاء.

4.9 Internal Control

٩,٤ الرقابة الداخلية

4.9.1 Internal Control Procedures

Under the Saudi AML Law, The Banking Control Law.
Decision of the Minister of Finance & National Economy on Regulating Money Changing Business, financial institutions are required to establish internal control procedures and prevent themselves from being used for purposes of money laundering and terrorist financing.

To apply an effective approach, the internal control procedures of the banks or money exchangers must be imbedded within their systems, programs and procedures to cover the issue of money laundering and terrorist financing. Senior management is ultimately responsible for ensuring that a bank or money exchanger maintains an effective internal control structure, including suspicious activity monitoring and reporting. The strength of senior management leadership and compliance with AML/CTF are an important aspect of the application of the procedure. Senior management must create a culture of compliance, ensuring that all employees adhere to the bank's or money exchanger's policies, procedures and processes designed to limit and control risks.

In addition to other compliance internal controls, the nature and extent of AML/CTF controls will depend upon a number of factors, including:

1. Nature, scale and complexity of a bank's or money exchanger's business.
2. Diversity of a bank's or money exchanger's operations, including geographical diversity.
3. Bank's or money exchanger's customer, product and

١,٩,٤ إجراءات الرقابة الداخلية

يلزم نظام مكافحة غسل الأموال ونظام مراقبة البنوك وتنظيم أعمال مهنة الصرافة المؤسسات المالية بوضع إجراءات للرقابة الداخلية والمحافظة على منع استخدامها لأغراض غسل الأموال وتمويل الإرهاب.

ومن أجل تطبيق أسلوب فعّال فإنه يجب أن يتم إدراج إجراءات الرقابة الداخلية الخاصة بمجال مكافحة غسل الاموال وتمويل الارهاب بالبنوك أو محلات الصرافة ضمن سياسات وخطط وإجراءات خاصة بالبنك او محل الصرافة ليشمل موضوع غسل الأموال وتمويل الإرهاب، كما أن من الواجب على الإدارة العليا أن يكون لها المسؤولية الابتدائية والنهائية للتأكّد من أن البنك أو محل الصرافة لديه نظام عمل فعال للرقابة الداخلية بما في ذلك مراقبة النشاطات المشتبه بها والإبلاغ عنها. وتعتبر قوة قيادة الإدارة العليا والتزامها بمكافحة غسل الأموال وتمويل الإرهاب مظهراً مهماً من مظاهر تطبيق هذا الإجراء. ويجب على الإدارة العليا أن تنشيء وتنشر ثقافة الالتزام بمجال مكافحة غسل الاموال وتمويل الارهاب بصفة خاصة لتضمن تقيّد جميع الموظفين بالسياسات والإجراءات والعمليات التي وضعها البنك أو محل الصرافة للحدّ من المخاطر ومراقبتها.

وإلى جانب الضوابط الداخلية الأخرى للالتزام، ترتبط طبيعة ومدى الضوابط الخاصة بمكافحة غسل الأموال وتمويل الارهاب بعدد من العوامل ومنها:

١. طبيعة ودرجة ومدى تعقيد أعمال البنك أو محل الصرافة.
٢. تنوّع عمليات البنك أو محل الصرافة، بما في ذلك التنوّع الجغرافي.
٣. عميل البنك أو محل الصرافة والمعلومات عن منتجاته ونشاطه وقنوات تقديم الخدمة المستخدمة.

activity profile and distribution channels used.
4. Volume and size of the transactions.
5. Degree of risk associated with each area of the bank's or money exchanger's operation.
6. Extent to which the bank or money exchanger is dealing directly with the customer or through third parties.

Therefore the framework of internal control procedures of banks or money exchangers should:

1. Provide increased focus on a bank's or money exchanger's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
2. Provide for regular review of the risk assessment and management processes, taking into account the environment within which the bank or money exchanger operates and the activity in the market place.
3. Provide for an AML/CTF compliance function and designate an individual at management level responsible for managing the compliance function.
4. Ensure that adequate controls are in place before new products are offered.
5. Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
6. Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CTF compliance and provide for timely updates in response to changes in regulations.
7. Implement risk-based customer due diligence policies, procedures and processes.
8. Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
9. Enable timely identification of reportable transactions and ensure accurate filing of required reports.
10. Include AML/CTF compliance in job descriptions and performance evaluations of appropriate personnel.
11. Provide for appropriate continuous training to be given to all relevant staff.

٤. حجم العمليات ومقدارها.
٥. درجة المخاطر المرتبطة بكافة مجالات عمليات البنك أو محل الصرافة.
٦. كيفية تعامل البنك أو محل الصرافة مع العميل بشكل مباشر أو عبر أطراف ثالثة.

ولذلك فإنه يجب أن يكون إطار عمل إجراءات الرقابة الداخلية في البنوك ومحلات الصرافة على النحو التالي:

١. زيادة التركيز على عمليات البنك أو محل الصرافة (المنتجات، الخدمات، العملاء والمواقع الجغرافية) الأكثر عرضة من غيرها للإستغلال من قبل غاسلي الأموال والمجرمين الآخرين.
٢. الإدارة والمراجعة المنتظمة لعمليات تقييم المخاطر مع الأخذ بعين الإعتبار البيئة التي يعمل فيه البنك أو محل الصرافة والنشاط الحاصل في السوق.
٣. تكوين وحدة التزام خاصة لمكافحة غسل الأموال وتمويل الإرهاب وتعيين موظف على مستوى إداري رفيع للقيام بهذه الوظيفة.
٤. التأكد من وضع الضوابط الملائمة قبل تقديم منتجات جديدة.
٥. إعلام الإدارة العليا بمبادرات الالتزام والنواقص المكتشفة في الالتزام، والإجراءات التصحيحية المتخذة والتقارير المرفوعة عن النشاطات المشتبه بها.
٦. التركيز على تلبية كافة المتطلبات النظامية للاحتفاظ بالسجلات والتبليغ وتوصيات الالتزام بمكافحة غسل الأموال وتمويل الإرهاب والقيام بالتحديثات للإستجابة للتغييرات على التنظيمات في وقت مناسب.
٧. اعتماد الأسلوب المرتكز على المخاطر عند عمل إجراءات العناية الواجبة للسياسات والإجراءات والعمليات.
٨. وضع ضوابط مناسبة للتعامل مع العملاء والعمليات والمنتجات المصنفة ضمن الفئات ذات المخاطر العالية وذلك حسب الضرورة مثل وضع حدود للعمليات أو الحصول على موافقات الإدارة.
٩. تسهيل تحديد العمليات التي يمكن التبليغ عنها في الوقت الصحيح وضمان رفع التقارير المطلوبة على النحو المناسب.
١٠. يجب أن يشمل وصف الوظائف وتقييمات الأداء على الالتزام بمكافحة غسل الأموال وتمويل الإرهاب.
١١. توفير التدريب الملائم المستمر لكافة الموظفين المعنيين.

4.9.2 Assessment of Internal Controls

Banks and money exchangers should establish means of independently and periodically assessing the effectiveness of the internal controls and the adequacy of the overall AML/CTF programs. The assessment should include validating the operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based approach reflects the risk profile of the bank or money exchanger.

The internal audit department of the bank or money exchanger, which should be separate from the compliance function, should conduct independent testing to assure the adequacy of the overall compliance function. The results of the testing should be documented and communicated to senior management for appropriate action.

٤،٩،٢ تقييم إجراءات الرقابة الداخلية

يجب على البنوك ومحلات الصرافة وضع الأساليب اللازمة لتقييم فاعلية الضوابط الداخلية وملائمة برامج مكافحة غسل الأموال وتمويل الإرهاب بشكل مستقلّ ودوري. ويشمل التقييم المصادقة على عملية تقييم المخاطر وعمليات الإدارة والضوابط الداخلية ذات الصلة والتأكّد من أن الأسلوب المعتمد والمرتكز على المخاطر يعكس معلومات المخاطر التي يواجهها البنك أو محل الصرافة.

ويتعيّن على إدارة التدقيق الداخلي في البنك أو محل الصرافة، والتي يجب أن تعمل بشكل مستقل عن وظيفة الالتزام إجراء فحص مستقلّ لمدى ملاءمة وظيفة الالتزام وتوثيق نتائج الفحص وإرسالها إلى الإدارة العليا لاتخاذ الإجراء المناسب.

4.10 Staff Training & Hiring

٤،١٠ تدريب الموظفين وتعيينهم

4.10.1 Staff Training & Awareness

The AML Law and Bylaws mandate all financial institutions to develop training programs to educate their employees and enhance their understanding of Due Diligence, KYC principles, money laundering and terrorist financing risks, trends and preventive methods. As employees become familiar with such activity, they can play an effective role by taking preventive measures to reduce the occurrence and

٤،١٠،١ تدريب الموظفين ورفع مستوى الوعي لديهم

بموجب نظام مكافحة غسل الأموال ولائحته التنفيذية، يجب على المؤسسات المالية إعداد برامج تدريبية مستمرة للموظفين المختصين لتحسين معرفتهم بمباديء العناية الواجبة و معرفة العميل ولإحاطتهم بالمستجدات في مجال عمليات غسل الأموال وتمويل الإرهاب، وبما يرفع من قدراتهم في التعرف على تلك العمليات وأنماطها وكيفية التصدي لها. وتدريب الموظفين

control of money laundering and terrorist financing.

Banks and money exchangers should provide their employees with appropriate and adequate training, and ongoing awareness, with regard to money laundering and terrorist financing. A bank or money exchanger must have successful controls based on both training and awareness. This requires an institution wide effort to provide all relevant employees with at least general information on AML/CTF laws, regulations and internal policies on compliance.

Applying a risk-based approach to the various methods available for training, however, gives each bank or money exchanger, additional flexibility regarding the frequency, delivery mechanisms and focus of such training. A bank or money exchanger should review its own workforce and available resources and implement training programs that provide appropriate AML/CTF information, as follows:

1. Tailored to the appropriate staff responsibility (e.g., front-line staff, compliance staff, or customer relations staff, account opening and operations.).
2. At the appropriate level of detail (e.g., complex products, new products and services, trends).
3. At a frequency related to the risk level of the business line involved.
4. All new staff, before starting their work, should be educated in the importance of AML/CTF policies while regular and continuous refresher training should be provided to staff to ensure that they are reminded of their responsibilities and kept informed of new developments.
5. Testing to assess staff knowledge commensurate with the detail of information provided.
6. Training programs shall include various levels of staff in the bank or money exchanger including members of the Board, Directors in charge and Executive Directors.

Additionally, banks and money exchangers should make all their staff aware of their responsibilities, personal obligations, liability and penalties under the legislation, should they fail to comply with the relevant requirements, as stated in Saudi AML Law.

على هذا النشاط ليصبح باستطاعتهم القيام بدور فعّال من خلال اتخاذ التدابير الوقاية للحد من حدوثها ومكافحتها.

وبالتالي يجب على البنوك ومحلات الصرافة توفير التدريب الملائم والمناسب لموظفيهم وتوعيتهم باستمرار على أنشطة غسل الأموال وتمويل الإرهاب.كما يجب على البنك أو محل الصرافة القيام بوضع ضوابط جيدة مبنية على التدريب والتوعية، الأمر الذي يستدعي بذل جهد ضخم على مستوى المؤسسات لتزويد كافة الموظفين المعنيين على الأقل بالمعلومات العامة بالانظمة والتعليمات الخاصة بمكافحة غسل الأموال وتمويل الإرهاب وعن سياسات الالتزام الداخلية.

إلاّ أن تطبيق الأسلوب المرتكز على المخاطر على مختلف أساليب التدريب المتوفرة يمنح كلّ بنك أو محل صرافة مرونة إضافية لتكرار هذا التدريب وآليات توفيره والنقاط الواجب التركيز عليها. ويجب على البنك أو محل الصرافة مراجعة الموارد البشرية والموارد الأخرى المتوفرة له وتطبيق برامج تدريبية تؤمّن المعلومات المناسبة عن مكافحة غسل الأموال وتمويل الإرهاب، على النحو الآتي:

١. تكون البرامج مفصّلة حسب مسؤولية الموظفين المعنيين (مثلاً الموظفين المتعاملين مع العملاء بصورة مباشرة، موظفو الالتزام، أو الموظفون في قسم العلاقات مع العملاء وفتح الحسابات والعمليات).
٢. مراعاة أدّق التفاصيل (مثلاً، المنتجات المعقّدة، المنتجات والخدمات والأنماط الجديدة).
٣. يجب أن يتم تكرارها بالملائمة مع مستوى المخاطر التي يواجهها خط الأعمال.
٤. يجب تثقيف كافة الموظفين قبل مباشرتهم للعمل حول أهمية سياسات مكافحة غسل الأموال وتمويل الإرهاب بينما يجب إعادة التدريب المنتظم والمستمر للموظفين لضمان تذكيرهم بمسؤولياتهم وإطلاعهم الدائم على التطورات الجديدة
٥. إجراء الإختبارات لتقييم معرفة الموظفين بالنسبة إلى تفاصيل المعلومات التي يتم تقديمها.
٦. أن تشمل البرامج التدريبية مختلف مستويات الموظفين في البنك أو محل الصرافة بما فيهم أعضاء مجلس الإدارة والمدراء المسئولين والتنفيذيين.

بالإضافة إلى ذلك يجب على البنوك ومحلات الصرافة توعية كافة موظفيهم بالمسؤوليات الملقاة على عاتقهم وواجباتهم الشخصية والعقوبات التي قد يتعرضون لها بموجب النظام في حال أخفقوا في الالتزام بالمتطلبات ذات الصلة كما هو منصوص عليه في نظام مكافحة غسل الأموال.

4.10.2 Staff Hiring & Appointment of Senior Positions

Banks and money exchangers should put in place adequate background screening procedures to ensure high standards when hiring employees. Banks and money exchangers can develop a risk-based approach on the level of screening based on the function and responsibilities associated with a particular position.

In addition, banks and money exchangers should comply with the provisions stipulated in the SAMA Directive issued in April 2005, relating to Qualification Requirements for Appointment to Senior Positions in Banks, including notifying SAMA for each senior appointment and the annual submission of a list of senior positions.

٤،١٠،٢ تعيين الموظفين واختيارهم في مناصب رفيعة

يجب على البنوك ومحلات الصرافة وضع إجراءات مناسبة لفحص خلفية الأشخاص وتطبيق معايير عالية عند تعيين الموظفين. وبإمكانهم اعتماد أسلوب مرتكز على المخاطر بالنسبة لمستوى الفحص بناءً على المهام والمسؤوليات المرتبطة بمنصب معيّن.

كما يجب عليهم الالتزام بلأحكام المنصوص عليها في التوجيه الصادر عن مؤسسة النقد العربي السعودي في شهر أبريل ٢٠٠٥م بشأن متطلبات التعيين في مناصب الإدارة العليا في البنوك، بما في ذلك إخطار مؤسسة النقد العربي السعودي بكلّ تعيين يحصل في منصب في الإدارة العليا وتقديم لائحة سنوية بالأشخاص الذين يشغلون المناصب العليا.

4.11 Record Keeping & Retention

Banks and money exchangers must keep all records (documents, instructions, transactions, files and reports) relating to their operations in accordance with normal business practices, for ease of reference in their own use, and for use by supervisory/ regulatory and other authorities, and for internal and external auditors. The records should be adequate enough to be able to reconstruct a transaction and offer a complete audit trail of all financial transactions, in particular cash transactions and funds transfer.

١١،٤ حفظ السجلات

يجب على البنوك ومحلات الصرافة الاحتفاظ بكافة السجلات (المستندات والتعليمات والعمليات والملفات والتقارير) المتعلقة بالعمليات التي يجرونها وفقاً للممارسات المعتادة للأعمال كي تشكّل مرجعاً سهلاً لهم وللسلطات الرقابية/التنظيمية والسلطات الأخرى وكذلك للمراجعين الداخليين والخارجيين. ويجب أن تكون هذه السجلات مناسبة بما فيه الكفاية لإيجاد عملية تم تنفيذها ولتوفير تتبع وسجل كامل لكافة العمليات المالية ، لا سيما العمليات النقدية وتحويلات الأموال.

The Saudi AML Law requires financial institutions to maintain, for a minimum of ten years following the conclusion of an operation/ transaction or termination of an account/ relationship, all records and documents that explain the financial, commercial and monetary transactions, whether local or foreign, the files of account documentation, related correspondence and copies of the identification documents. Taking into consideration the local law, customer transaction records, such as agreements, checks, etc., should be retained indefinitely.

In specific cases, banks and money exchangers may be instructed by SAMA or other Saudi competent authorities, to maintain any transactions or account records beyond the minimum time period stated below. Banks and money exchangers should keep and retain these records in the form and for the period as indicated below:

1. Primary Records

Type of Record	Retention Form	Retention Period
a. Customer account opening agreements and related account documents	Original form	Permanently
b. Certified/ attested copies of customer identification documents	Originals of the certified/ attested copies	Permanently
c. All customer transaction records and instructions: i. Manual instructions (e.g., checks, transfer applications, etc.) ii. Automated instructions (e.g., internet, phone banking, ATM, incoming wire transfers, etc.)	One of the following: i. Original form ii. Electronic form	Permanently
d. Statements and details of customer accounts and balances.	Electronic form	Permanently

2. Secondary/ Non-Financial Records

Type of Record	Retention Form	Retention Period
a. Customer profiles, risk assessments and all other KYC related documents	Original and/or electronic form	Minimum 10 years
b. Investigations, suspicious activity reports, etc.	Original and/or electronic form	Minimum 10 years
c. Automated and manual reports	Original and/or electronic form	Minimum 10 years
d. Reviews, self-assessments, audit reports, etc.	Original and/or electronic form	Minimum 10 years

5. AML / CTF Other Risks

5.1 Product/ Service Risks

Product or service risks are the potential risks inherent in the

وينصّ نظام مكافحة غسل الأموال على ان المؤسسات المالية ملزمة بالإحتفاظ بكافة السجلات والوثائق التي تفسّر العمليات المالية والتجارية والنقدية، سواء المحلية أو الأجنبية وبمستندات الحسابات والمستندات ذات الصلة مع صور عن الأوراق الثبوتية، وذلك لمدة لا تقلّ عن عشر سنوات بعد انتهاء العملية أو إقفال حساب أوعلاقة مصرفية ما ، مع مراعاة النظام المحلي الذي يوجب حفظ المستندات أو الوثائق الخاصة بعمليات العملاء كالإتفاقات والشيكات وسواها لفترة غير محددة.

وفي حالات معيّنة، قد توّجه مؤسسة النقد العربي السعودي أو السلطات السعودية المختصة الأخرى تعليمات إلى البنوك ومحلات الصرافة للاحتفاظ بسجلات أيّ من العمليات أو الحسابات لفترة أطول من الحدّ الأدنى المنصوص عليه أدناه. وتحفظ البنوك ومحلات الصرافة هذه السجلات بالنموذج وللفترة المحددين أدناه:

١. السجلات الرئيسية

نوع المستند أو السجل	نموذج الحفظ	فترة الحفظ
أ. الإتفاقيات الخاصة بفتح حساب العميل ووثائق الحساب ذات الصلة	النموذج الأصلي	بشكل دائم
ب. نسخ معتمدة/ موثقة عن الأوراق الثبوتية للعميل	أصل النسخ المعتمدة / الموثقة	بشكل دائم
ج. كافة السجلات والتوجيهات الخاصة بعملية العميل: ١- التعليمات المكتوبة لتنفيذ العمليات (مثلاً، الشيكات، ونماذج الحوالات، إلخ...) ٢- التعليمات الآلية (مثلاً، الإنترنت، الخدمات البنكية على الهاتف المصرفي، الصرّاف الآلي، التحويلات البرقية الواردة، إلخ...)	أحد النماذج التالية: ١-النموذج لأصلي ٢-النموذج الإلكتروني	بشكل دائم
د. كشوفات وتفاصيل حسابات وأرصدة العميل	النموذج الكتروني	بشكل دائم

٢ السجلات والمستندات الثانوية/غير المالية

نوع السجل أو المستند	نموذج الحفظ	فترة الحفظ
أ. معلومات العميل، تقييم المخاطر وكافة المستندات الأخرى المرتبطة بمعرفة العميل	النموذج الأصلي و/أو الإلكتروني	عشر سنوات على الأقلّ
ب. التحقيقات وتقارير النشاط المشتبه به، إلخ...	النموذج الأصلي و/أو الإلكتروني	عشر سنوات على الأقلّ
ج. التقارير الآلية والورقية	النموذج الأصلي و/أو الإلكتروني	عشر سنوات على الأقلّ
د. المراجعات، التقييمات الذاتية وتقارير إدارة التدقيق الداخلي، إلخ...	النموذج الأصلي و/أو الإلكتروني	عشر سنوات على الأقلّ

٥. المخاطر الأخرى لمكافحة غسل الأموال وتمويل الإرهاب

١,٥ مخاطر المنتج/الخدمة

products or services offered by a bank or money exchanger. Banks and money exchangers should be aware of the associated risks in all the products and services they offer including the way they are delivered, especially for new or innovative products or services. Banks and money exchangers should develop appropriate risk assessment and controls. The products and services offered by banks and money exchangers, determined as posing potentially higher risks are described below.

5.1.1 Cash

Physical cash is often the ideal and most commonly used method for transfer of funds and undertaking criminal activities, including money laundering and terrorist financing, simply because the perpetrator is anonymous, untraceable, requires no intermediary, is widely accepted and provides for immediate settlement. While the provision of services to cash-generating business is a particular area of concern, however, some businesses are legitimately cash-based, especially in the retails sector, and so there will often be a high level of cash deposits associated with some of these accounts.

1. Cash Transactions

SAMA has participated for many years in the efforts to transform the Saudi economy to a bank-payment based society and has taken significant steps to discourage large cash transactions and encourage the use of banking payment systems and services, such as SARIE, SWIFT, ATM/SPAN, POS, SADAD, Internet banking, credit cards, etc. SAMA Account Opening Rules require banks and money exchangers to accept cash from customers only through an account or relationship, where a full due diligence and KYC process has been established.

Banks and money changers should urge ang encourage customers to reduce the use of cash and provide alternative banking services such as the use of electronic financial payment systems.

Banks and money exchangers should have a process in place to detect cash transactions that could be deemed as suspicious, such as:

1. Large cash deposits, not in line with the customer's type of business or occupation.
2. Numerous cash deposits of small amounts, known as structuring or smurfing, to avoid detection.
3. Cash deposits followed by a transfer (wire transfer, bank check, etc.).
4. Structured cash payments for outstanding credit card balances, with relatively large sums as payments.

2. Cross-Border Transportation of Cash

In accordance with Saudi AML Law and its implementation regulation, banks and money exchangers should comply with the requirements relating to cross-border transportation of cash coming into or going out of Saudi Arabia for their own use. The cash may be carried directly or through cash transportation firms by way of cargo, postal parcels,...etc. Banks and money exchangers or their cash transportation firms should adhere to the requirements by completing a special declaration form for any cash shipment about the money to be disclosed, in compliance with the requirements of security safety and SAMA Rules for Cash Transportation issued on 29 April 2007 to Banks and Money Exchangers.

5.1.2 Wire Transfers

يُقصد بمخاطر المنتج أو الخدمة المخاطر المحتملة الكامنة في المنتجات أو الخدمات التي يقدّمها البنك أو محل الصرافة.ويجب على البنوك ومحلات الصرافة أن تعي المخاطر المرتبطة بكافة المنتجات والخدمات التي يقدمونها، بما في ذلك طريقة تقديمها لا سيما المنتجات أو الخدمات الجديدة أو المبتكره. ويجب عليهم تطوير عمليات تقييم المخاطر والضوابط بصورة ملائمة. وفيما يلي عرض للمنتجات والخدمات التي تقدّمها البنوك و محلات الصرافة والتي تم وضعها في خانة المخاطر العالية:

١,١,٥ المال النقدي

تعتبر االاموال النقدية (الكاش) الطريقة المثلى والأكثر شيوعاً في ممارسة الأنشطة الإجرامية، بما في ذلك غسل الأموال وتمويل الإرهاب لانها بكلّ بساطة، منفذها مجهول الهوية وغير قابل للملاحقة ، ولا يتطلب تنفيذها أي طرف وسيط ، بل يلقى قبولاً واسعاً ويؤمّن تسوية فورية. وبينما يشكّل تقديم الخدمات والأعمال التي تدر المال النقدي مجالاً مثيراً للقلق غير انه توجد بعض الأعمال التي تدر المال النقدي بصورة مشروعة وخاصة في قطاع التجزئة وبالتالي ترتبط بعض هذه الحسابات بمستوىً عالٍ من الودائع النقدية.

١. العمليات النقدية

تشارك مؤسسة النقد العربي السعودي لسنوات عديدة في الجهود الرامية إلى تحويل مجتمع الإقتصاد السعودي إلى مجتمع قائم على المدفوعات البنكية بحيث اتخذت خطوات جوهرية في هذا المجال للحدّ من العمليات النقدية الضخمة وتشجيع استخدام نظم وخدمات الدفع البنكي، على غرار أنظمة سريع و سويفت و الشبكة السعودية للصراف الآلي ونقاط البيع ونظام سداد والخدمات البنكية على الإنترنت والبطاقات الإئتمانية، إلخ... وتلزم القواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي البنوك ومحلات الصرافة بعدم قبول المال النقدي من العملاء إلاّ من خلال حساب أو علاقة مصرفية ، حيث يتمّ إجراء عملية كاملة من العناية الواجبة ومعرفة العملاء.

كما ينبغي على البنوك ومحلات الصرافة العمل على حث وتشجيع العملاء على التقليل من التعامل بالنقد وتوفير الخدمات المصرفية البديلة كاستخدام نظم المدفوعات المالية اللإلتكرونية.

ويجب على البنوك ومحلات الصرافة وضع آلية لرصد العمليات النقدية التي يمكن اعتبارها بحكم المشتبه بها، ومن أمثلة ذلك:

١. الودائع النقدية الضخمة والتي لا تتوافق مع نوع الأعمال أو الوظيفة التي يمارسها العميل.
٢. الودائع النقدية العديدة بمبالغ صغيرة المعروفة بعملية التركيب لتفادي اكتشافها.
٣. الودائع النقدية والتي تتبعها عملية تحويل (تحويل برقي، شيك مصرفي، إلخ...).
٤. المدفوعات النقدية المركبة لأرصدة البطاقات الإئتمانية المستحقة والتي تشمل مبالغ ضخمة من المدفوعات.

٢. نقل المال النقدي عبر الحدود

عملاً بمقتضى نظام مكافحة غسل الأموال ولائحته التنفيذية، يجب على البنوك ومحلات الصرافة التقيّد بمتطلبات نقل الاموال النقدية الداخل إلى السعودية أو الخارج منها لاستخداماتهم الخاصة. ويمكن نقل هذا المال بطريقة مباشرة او عبر شركات نقل الاموال الخاصة سواء بالشحن أو الطرود البريدية إلخ.. ، كما يجب على البنوك ومحلات الصرافة أو الشركات المتخصصة في نقل المال النقدي التقيّد بتلك المتطلبات من خلال تعبئة نموذج الإفصاح الخاص بأي شحنة نقدية تزيد قيمتها عن حدود مبالغ الأموال الواجب الإفصاح عنها , مع التقيد بمتطلبات السلامة الأمنية و بما جاء في تعميم مؤسسة النقد بشان تنظيم عملية نقل النقد المرسل للبنوك ومحلات الصرافة بتاريخ ٢٩ أبريل ٢٠٠٧.

٢,١,٥ التحويل البرقي

يشير مصطلح التحويل البرقي (التلكس) أو تحويل الأموال إلى أيّ عملية تجري بالنيابة عن شخص محوّل (طبيعي أو اعتباري) عبر بنك أو محل صرافة وبالأساليب الإلكترونية بغرض توفير مبلغ من المال إلى شخص مستفيد يتعامل مع بنك أو محل صرافة آخر. وقد يكون الشخص المحوّل والمستفيد شخصاً واحداً أو منشأة واحدة. كذلك قد يكون التحويل عبر الدول (أي من/إلى بلد آخر) أو محلياً (داخل البلد نفسه).

وتلزم القواعد الخاصة بفتح الحسابات الصادرة عن مؤسسة النقد العربي السعودي البنوك ومحلات الصرافة بعدم قبول طلبات تنفيذ التحويلات إلاّ من العملاء الذين يملكون إتفاقية فتح حساب أو علاقة أخرى (مثلاً، خدمة التحويل المالي السريع). وعليه فإنه يجب على البنوك ومحلات الصرافة الحصول على المعلومات الملائمة عن الشخص المحوّل. كما يجب على البنوك ومحلات الصرافة إعتماد التدابير التالية عند تنفيذ التحويلات لعملائهم وذلك من أجل تحسين شفافية التحويلات البرقية لزيادة فعالية برامج مكافحة غسل الأموال وتمويل الإرهاب:

١. تعزيز اجراءات العناية الواجبة عند تنفيذ التحويلات المرتبطة بالحسابات أو الأشخاص السياسيين المعرضين للمخاطر.
٢. عدم قبول أي تحويلات واردة أو صادرة من/إلى خارج المملكة العربية السعودية لأي منظمات خيرية أو غير هادفة للربح، عدا الجهات المسموح لها بذلك وفقا للقواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي.
٣. عند تطبيق أي نظم إلكترونية جديدة لتحويل الأموال والمدفوعات فإنه يجب التأكّد من أنها صممت على أن تكون لديها قدرات تسمح بمنع واكتشاف عمليات غسل الأموال وتمويل الإرهاب. ومن ضمن أساليب الدفع الإلكتروني الجديدة، على سبيل المثال، البطاقات المسبوقة الدفع، المحافظ الالكترونية/والبطاقات ذات القيمة المخزّنة، والمدفوعات عبر الهواتف الجوالة، وخدمات الدفع على الإنترنت، إلخ...، فإنه يجب التأكّد من ان لا يتم تقديم هذه الخدمات إلاّ إلى العملاء الذين يملكون حساباً أو علاقة مصرفية أخرى مع البنك أو محل الصرافة.
٤. الالتزام بمعايير الشفافية وضمان احتواء رسائل التحويلات المالية (المرافقة للتحويل) التي تبعثها وتستلمها البنوك المنشئة والمستقبلة والبنوك المراسلة وشركات تقديم خدمات التحويل على المعلومات الكاملة عن المنشئ والمستفيد كما هو محدد ادناه.
٥. الحصول على المعلومات الكاملة والدقيقة عن منشئ الحوالة وذلك للحوالات الصادرة وأن يتم الاحتفاظ بها كاملة في رسالة الحوالة، على أن تتضمن ما يلي:

٥/١- اسم منشئ الحوالة.

٥/٢- رقم حساب / رقم عضوية منشئ الحوالة.

٥/٣- عنوان منشئ الحوالة، ويمكن استبدال العنوان في حال عدم توفره برقم الهوية الحكومية وهي الهوية الوطنية للمواطنين، ورقم الإقامة للوافدين، ورقم السجل التجاري للشركات، أو تاريخ ومحل الميلاد معاً.

٥/٤- ينبغي تحديد الغرض من التحويل بالتفصيل.

٥/٥-معلومات الهوية للطرف المستفيد من الحوالة وكحد ادنى رقم الهوية الحكومية الصادرة من بلد المستفيد .

٦. في حال الحوالات الواردة ومع اهمية مراعاة المتبع في الدول والمؤسسات المالية العاملة بها فانه يجب الحصول على المعلومات الكاملة عن منشئ الحوالة وان يتم ارفاقها كاملة مع رسالة الحوالة ، كما انه يجب الحصول على معلومات الهوية للطرف المستفيد من الحوالة عن طريق المنشئ.
٧. أخذ العناية الواجبة المستمرة تجاه العملاء المصدرين والمستقبلين للحوالات والتدقيق على العمليات المنفذة طوال فتره تلك العلاقة لضمان اكتمال وتوافق العمليات التي يتم إجرائها مع حجم نشاط العملاء بما في ذلك مصدر الدخل. علما انه تقع مهمة تطبيق

The term wire transfer or funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a bank or money exchanger by electronic means for the purpose of making an amount of money available to a beneficiary person at another bank or money exchanger. The originator and the beneficiary may be the same person/ entity. The transfer could be a cross-border transfer (to/ from a different country) or a domestic transfer (within the same country).

SAMA Account Opening Rules require banks and money exchangers to accept transfers only from customers having account or other relationship agreement (e.g., express remittance service). Therefore banks and money exchangers should always have adequate information about the originator/ remitter. To enhance the transparency of wire transfers for effective AML/CTF programs, banks and money exchangers should adopt the following measures when executing transfers for their customers:

1. Exercise Enhanced due diligence when processing transfers relating to accounts of Politicians Exposed Persons (PEPs).
2. Not to accept any incoming or outgoing transfers outside Saudi Arabia, for any charity or non-profit organizations,other than permitted entities. in accordance with the rules for opening bank accounts and the general operational rules.
3. When implementing any new electronic fund transfer and payment systems, ensure they are designed with capabilities for preventing and detecting money laundering and terrorist financing transactions. Examples of the new electronic payment methods include prepaid cards, electronic purse/stored value cards, mobile payments, internet payment services, etc. Ensure these services are offered only to customers who already have an account or other bank relationship with the bank or money exchanger.
4. Comply with standards of transparency and ensure that the letters of remittances (enclosed with the transfer),sent and received by remitting, receiving and correspondent banks and transfer services companies, include full information about the remitter and the beneficiary, as determined below.
5. Obtain full information about the remitter of outgoing remittances and keep the information in the transfer letter, which should include the following:

   2/1- Remitter's name.
   2/2- Remitter's account / membership No.
   2/3- Remitter's address, if not available, it may be replaced by government ID No. (National ID of citizens, Iqama No. of expatriates and commercial registration No. of companies) or both date and place of birth
   2/4- the purpose of transfer should be determined in details.
   2/5 Identity information of the transfer beneficiary and as a minimum the ID government identification number issued by the beneficiary's country.

6. In case of incoming transfers, taking into consideration the applicable procedures of the countries and their financial institutions operating therein, full information must be obtained about the remitter to be attached fully to the transfer letter. identity information of the beneficiary of the remittance shall be obtained from the remitter. The identity of beneficiary means the government identity card issued by the beneficiary's country.
7. Taking continuous due diligence in respect of customers

إجراءات معرفة العميل والعناية الواجبة للشخص المحوّل على عاتق البنك أو محل الصرافة المحوّل، سواء كان أجنبياً أم محلياً

٨. في حال للتحويلات البرقية غير المصحوبة بالمعلومات الكاملة عن المنشئ يجب على البنوك ومحلات الصرافة العاملة في المملكة أن تعتمد إجراءات فعالة، والتصرف حيالها على النحو الآتي:

٨/١- الحصول على المعلومات الناقصة من البنك المراسل أو من شركة تقديم خدمات التحويل وهذا ينطبق على جميع البنوك المحلية والدولية.

٨/٢- رفض تنفيذ العملية و إعادة الحوالة في حالة عدم تجاوب البنك المراسل.

٨/٣- في حال الاشتباه في هذه العملية وعدم تجاوب البنك المراسل فإن ذلك يستدعي الإبلاغ عن ذلك إلى وحدة التحريات المالية.

٨/٤- توثيق القرارات التي يتم اتخاذها كتابياً متضمنة ذكر الأسباب ، والاحتفاظ بهذه السجلات المستندية والإلكترونية لمدة ١٠ سنوات بناءً على قواعد مكافحة غسل الأموال وتمويل الإرهاب الصادرة من المؤسسة.

٨/٥- يجب أن تتضمن الحوالات الواردة اسم البنك والدولة المنشئة للحوالة واسم البنك المراسل والدولة، ويجب على البنوك المراسلة الالتزام بذلك، وفي حال حدوث تغيير في معلومات منشئ الحوالة يجب أن يخطر البنك المستفيد بذلك.

٩. في حال إرسال عدة تحويلات برقية خارجية من قبل منشئ واحد وذلك ضمن تحويل مجمع لمستفيدين في دولة أخرى ينبغي أن يتم إدراج كافة المعلومات المتعلقة بالمنشئ والمصاحبة للتحويل البرقي مع ذلك التحويل لكل تحويل برقي خارجي شرط أن يحتوي ملف التحويل المجمع (الذي يتم تجميع التحويلات البرقية الفردية فيه) على المعلومات الكاملة عن المنشئ والتي يمكن تعقبها بسهولة.

١٠. في الحالات التي تمنع فيها القيود الفنية إرسال المعلومات الكاملة عن المنشئ التي تكون مصاحبه لتحويل برقي خارجي مع تحويل برقي محلي مرتبط به (خلال الفترة اللازمة لتكييف أنظمة الدفع) يجب على المؤسسات المالية الوسيطة متلقية التحويل أن تحتفظ بسجل يتضمن كافة المعلومات التي تلقتها من المؤسسة المالية المصدرة للتحويل وذلك لمدة ١٠ سنوات بناءً على قواعد مكافحة غسل الأموال وتمويل الإرهاب الصادرة من المؤسسة، مع الأخذ في الاعتبار الالتزام بمدة لا تتجاوز (٧٢ ساعة عمل) للرد على أي استفسار يرد من البنك المراسل أو السلطات المعنية.

١١. حين تكرار حالات نقص المعلومات، وعدم تعاون البنوك المنشأة للحوالة أو البنك المراسل أو شركة تقديم خدمات التحويل ينبغي على البنوك وشركات الصرافة العاملة بالمملكة تقييم العلاقة مع هذا البنك أو الشركة والنظر في تقييد، أو حتى إنهاء العلاقة معها.

١٢. في حال الاشتباه في تعاملات أو العلاقة مع البنك المراسل أو شركة تقديم خدمات التحويل من منظور غسل الأموال أو تمويل الإرهاب، يجب الإبلاغ فوراً عن ذلك لوحدة التحريات المالية، مع توثيق هذه الحالات.

١٣. يجب أخذ الموافقة المسبقة من مؤسسة النقد في حال التعاقد مع الوكلاء أو شركات تقدم خدمة التحويلات المالية.

١٤. توفر إمكانية للبنوك ومحلات الصرافة العاملة في المملكة المتعاقدة مع شركات تقديم

exporting and import remittances and checking transactions implemented during that relationship to ensure they are complete and compatible with the size of customers activity, including the source of income. Conducting KYC/ due diligence on the remitter/ originator is the responsibility of the remitting bank or money exchanger, whether foreign or local.

8. In case of wire transfers which are not accompanied with full information of remitter, banks and money exchanger operating in the Kingdom shall adopt effective measures, and act against such transfers as follows:

5/1- obtain missing information from the correspondent bank or the company providing transfer services and this applies to all local and international banks.

5/2- reject the transaction and return the remittance in the case the correspondent bank does not respond.

5/3- In case of suspicion in such a transaction and if the correspondent bank does not respond, the case should be reported to the Financial Investigation Unit.

5/4- Document decisions made in writing, including reasons and keep hard and soft copies of records for 10 years in compliance with the rules on anti-money laundering and terrorism financing issued by SAMA.

5/5- Incoming remittance shall include name of the bank, originating country, correspondent bank and the country. Correspondent banks shall comply therewith, and in case of a change in the remitter's information, the beneficiary bank should be notified thereof.

9. In case of sending cross-border wire transfers by one remitter as part of combined transfer to beneficiaries in another country, all information related to the remitter and accompanied with wire transfer should be inserted with the transfer for each cross-border wire transfer provided that the combined transfer file (in which individual wire transfers are grouped) should have full information about the remitter that can be tracked easily.
10. In situations where technical restrictions prevent sending full information of the remitter that is accompanied with a cross-border wire transfer with local wire transfer linked to it (during the period necessary to adapt payment systems), intermediary financial institutions receiving a transfer shall keep a record containing all information received from the financial institution exporting the transfer for a period of 10 years in compliance with the rules on combating money laundering and terrorist financing issued by SAMA, taking into consideration the commitment for a period no longer than (72 working hours) to respond to any inquiries received from the correspondent bank or the relevant authorities.
11. In case of repetition of lack of information situations, and non-cooperation by transfer originator banks, a correspondent bank or transfer services company, banks and money exchanger operating in the Kingdom should evaluate the relationship with the bank or the company and consider restricting or even ending the relationship therewith.
12. In case of suspecting transactions or relationship with a correspondent bank or transfer services company from the perspective of money laundering or terrorist financing, this must be reported immediately to the FIU, and these cases shall be documented.
13. Prior approval of SAMA shall be taken in the case of

contracting with agents or companies that offer financial transfers services.

14. There should be a possibility for banks and money exchangers operating in the Kingdom and contracting with financial transfer service companies to obtain full information about the parties of financial transfers carried out by such companies on their behalf.
15. The business of the contracted companies providing a remittance service regarding transactions carried out through banks and money exchangers operating in the Kingdom shall be subject to supervision and control by the bank or money exchanger through which those companies operate.
16. During the study of the relationship with a correspondent bank or a financial transfer service company and in case of going to end the relationship with them, finding alternative correspondent banks or financial transfer service companies shall be taken into account in order to avoid stopping of the transfer service with the country in question.
17. Monitor relationships with correspondent banks and financial transfer service companies, make sure they are lawful and evaluate the relationship whether the activity of the bank / company and their controls to combat money laundering and terrorist financing and transparency standards are consistent with what have been emphasized at the beginning of the relationship. Correspondent banks and financial transfer service companies shall obtain a certificate to confirm compliance with combating money laundering and terrorist financing on a continuing basis according to the rules of combating money laundering and terrorist financing, the rules of opening bank accounts and the general operational rules issued by SAMA.
18. Compliance with confidentiality of information exchanged between correspondent banks, receiving banks and financial transfer service companies, and is used only for authorized purposes in order to maintain the terms and conditions of banking secrecy and prevent its use for any other purpose.
19. Check names of wire transfer originators and beneficiaries against lists of individuals and entities that their assets should be stopped, refused or frozen based on international lists (e.g. resolutions of the United Nations 1373 and 1267), and take actions thereon.
20. Check names of individuals, entities, banks/financial transfer service companies and originator, intermediary or beneficiary countries against international lists (e.g. UN, OFAC, INTERPOL, FATF, etc...), and take actions thereon.
21. Banks and money exchanger operating in the Kingdom shall apply effective measures in all its business based on the effective measures to ensure fulfillment of KYC and due diligence requirements and relative importance. Extra due diligence for funds transferred from or to Countries that do not apply or do not fully apply FATAF's require.
22. Monitor all transactions (incoming and outgoing transfers) to detect the types of unusual activities that do not have a clear legal or economic purpose, check the background of these transactions and their purpose to the maximum extent, and document findings reached in writing.
23. Whenever there are logical reasons to suspect that customers' money, operations and transactions represent proceeds of criminal activity or have connection or relationship with money laundering or terrorist financing, the FIU shall be informed.

خدمات التحويلات المالية من الحصول على المعلومات الكاملة عن أطراف عمليات التحويل المالي التي تجريها تلك الشركات نيابةً عنهم.

١٥. يجب أن تخضع أعمال الشركات المقدمة لخدمة التحويلات المالية المتعاقد معها والمتعلقة بالعمليات المنفذة من خلال البنوك ومحلات الصرافة العاملة في المملكة لإشراف ورقابة البنك أو محل الصرافة الذي تعمل من خلاله تلك الشركات.

١٦. أثناء دراسة العلاقة مع البنك المراسل أو شركة تقديم خدمات التحويل وفي حال التوجه إلى قطع العلاقة معها فإنه يجب مراعاة البحث عن بنوك مراسلة أو شركات تقديم خدمات تحويل بديلة لتجنب إيقاف خدمة التحويل للدولة المعنية.

١٧. مراقبة العلاقات مع البنوك المراسلة وشركات تقديم خدمات التحويل والتأكد من نظاميتها وتقييم علاقة ما إذا كان نشاط هذا البنك/الشركة وضوابطه الخاصة بمكافحة غسل الأموال وتمويل الإرهاب ومعايير الشفافية تتفق مع تلك التي تم التأكيد عليها في بداية العلاقة ، ويجب على البنوك المراسلة وشركات تقديم خدمات التحويل الحصول على شهادة تأكيد الالتزام بمكافحة غسل الأموال وتمويل الإرهاب بصورة مستمرة حسب قواعد مكافحة غسل الأموال وتمويل الإرهاب وقواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها الصادرة من المؤسسة.

١٨. الالتزام بضمان أن المعلومات التي يتم تبادلها بين البنوك المراسلة والمستقبلة وشركات تقديم خدمات التحويل لا تُستخدم إلا للأغراض المصرح بها للحفاظ على أحكام وشروط السرية المصرفية ومنع استخدامها لأي أغراض أخرى.

١٩. فحص الأسماء المنشئة للتحويلات البرقية والمستفيد منها مقابل قوائم الأفراد والجهات التي يجب إيقاف حركة أصولها أو رفضها أو تجميدها بناءً على القوائم الدولية ومن أمثلتها قرارات الأمم المتحدة (١٣٧٣ و ١٢٦٧)، واتخاذ الإجراءات اللازمة حيال ذلك.

٢٠. فحص أسماء الأفراد والكيانات والبنوك/شركات تقديم خدمات التحويل والدول – المنشئة للتحويلات أو الوسيطة في عمليات التحويل أو المستفيدة من عمليات التحويل – مقابل القوائم الدولية ومن أمثلتها (UN, OFAC,INTERPOL, FATF, etc..) واتخاذ الإجراءات اللازمة حيال ذلك.

٢١. أن تعتمد البنوك ومحلات الصرافة العاملة في المملكة في جميع تعاملاتها إجراءات فعالة لتحقق من استيفاء متطلبات التعرف على العملاء وإجراءات العناية الواجبة مبنية على معيار معدل المخاطر والأهمية النسبية. وتشديد ممارسة العناية الواجبة للأموال التي يتم تحويلها من و إلى الدول الصادر بشانها تحذيرات من قبل مجموعة العمل المالي.

٢٢. مراقبة جميع المعاملات (الحوالات الصادرة والواردة) لرصد أنماط الأنشطة غير الطبيعية التي لا يكون لها غرض اقتصادي أو قانوني واضح، وفحص خلفية تلك العمليات والغرض منها لأقصى حد ممكن، وأن تسجل كتابياً ما يتم التوصل إليه من نتائج.

٢٣. يجب عند توفر أسباب معقولة للاشتباه في أن أموال العملاء والعمليات والمعاملات تمثل متحصلات لنشاط إجرامي أو في ارتباطها أو علاقتها بعمليات غسل الأموال أو تمويل الإرهاب التبليغ عنها لوحدة التحريات المالية.

٢٤. في حال تم استلام التحويل من خارج المملكة باسم المستفيد فلا يتم دفع المبلغ إلا عن طريق حساب أو إنشاء علاقة لضمان الحصول على معلومات كاملة عن المستفيد، ويمكن أن يُفتح هذا الحساب أو أن تنشأ هذه العلاقة من قبل العميل عند استلام التحويل مع مراعاة القواعد الخاصة بفتح الحسابات وتشغيلها الصادرة عن مؤسسة

24. In case of receipt of a remittance from outside the Kingdom on behalf of a beneficiary, it shall be paid only by an account or by creating a relationship to ensure obtaining complete information about the beneficiary. A customer can open the account or establish the relationship when he receives the remittance, taking into account the rules for opening and operating accounts issued by SAMA.
25. For domestic transfers (within Saudi Arabia), ensure the remitter's name and account number is included, which should be recorded and retained in the system of remitting bank or money exchanger for prompt retrieval if requested by competent authorities. Also should be Verify the identity of the beneficiary of a local remittance (incoming) in accordance with the rules for opening bank accounts and the general operational rules.
26. It is not allowed to receive any transfer from a particular country to be passed through one of the banks operating in the Kingdom for a beneficiary in a bank located abroad in any currency other than the Saudi riyal.
27. When receiving a transfer in Saudi riyal from a particular country to be passed through one of the banks operating in the Kingdom for a beneficiary in a bank located outside the Kingdom, the purpose of remittance shall be determined in details.
28. Retain all physical and system records of all funds transfers in accordance with the prevailing record retention periods.

النقد.

٢٥. بالنسبة إلى التحويلات المحلية (داخل المملكة العربية السعودية)، فإنه يلزم التأكّد من ذكر اسم المحوّل ورقم حسابه والقيام بتسجيلهما وحفظهما في نظام البنك أو محل الصرافة المحوّل لغرض استرجاع المعلومات بسرعة في حال طلبت السلطات المختصة ذلك. كما انه يلزم التحقق من هوية المستفيد من التحويل الداخلي (الوارد) وذلك وفقاً لقواعد فتح الحسابات البنكية والقواعد العامة لتشغيلها.

٢٦. عدم السماح باستقبال أي حوالة تنشأ من بلد معين ليتم تمريرها عن طريق أحد البنوك العاملة في المملكة لمستفيد في بنك يقع خارج المملكة بأي عملة غير الريال السعودي.

٢٧. عند استقبال أي حوالة بالريال السعودي تنشأ من بلد معين ليتم تمريرها عن طريق أحد البنوك العاملة في المملكة لمستفيد في بنك يقع خارج المملكة لابد من تحديد الغرض من الحوالة بالتفصيل.

٢٨. حفظ كافة سجلات الأنظمة والسجلات المستندية لكافة التحويلات المالية وفقاً لفترات حفظ السجلات المتبعة

5.1.3 Alternative Remittances

Alternative remittance system refers to a type of financial service involving the transfer of funds or value from one geographic location to another through informal and unsupervised networks or mechanisms, which usually operate outside the regulated conventional financial sector. The very features (efficiency, anonymity and lack of paper trail, low cost, no need to prove identity, and the exchange rate) which make alternative remittance system attractive to customers with legitimate income (mainly expatriates remitting money to relatives in home countries), also make the system convenient for the transfer of illicit funds.

Therefore, due to this inherent risk, these systems have proven themselves vulnerable to misuse for money laundering and especially for terrorist financing purposes. Quite often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms, most common being “Door-to-Door”, “Hawala”, or "Hundi". In addition to the vulnerability for misuse, unauthorized or unlicensed alternative remittance services are illegal in Saudi Arabia and in violation of the Banking Control Law. Those who practice such activities are subject to legal penalties. Therefore, banks and licensed money exchangers should endeavor to assist authorities in fighting such unlawful activities.

Persons who offer these illegal services, at a certain point, channel their funds in “blocks” through the banking system by cash deposits and then remit the funds to the beneficiary by a transfer, or communication/ message. Therefore, banks and money exchangers should apply prudent measures to identify and prevent the use of customer accounts for this illegal business. While such suspicious transactions may be difficult to monitor, the application of due diligence process and relevant red flags indicators can help in identifying such transactions. As a minimum, banks and money exchangers should implement the following steps:

1. Have a mechanism in place to monitor customer

٣,١,٥ التحويلات البديلة

يشير نظام التحويل المالي البديل إلى نوع من الخدمة المالية التي تتضمن تحويل الأموال من موقع جغرافي إلى آخر عبر شبكات أو آليات غير رسمية وغير مراقبة والتي تعمل عادة خارج القطاع المالي التقليدي والمنظّم. ان خصائص هذا النظام (الكفاءة، وإخفاء الإسم، وقلّة المستندات الورقية، انخفاض التكلفة، عدم الحاجة لاثبات الهوية، سعر الصرف) مما تجعله جذاباً في عيون العملاء ذوي الدخول المشروعة (وهم بشكل رئيسي المقيمين من الأجانب الذين يحوّلون المال إلى أقربائهم في بلدهم الأم) كما تساعد أيضاً في جعله فرصة ملائمة لتحويل الأموال غير المشروعة.

وعليه، وبسبب هذا الخطورة الكامنة، اتضح أن هذه النظم ضعيفة وعرضة للإستغلال لغايات غسل الأموال وبشكل خاص لأغراض تمويل الإرهاب. وغالباً ما تكون مرتبطة بمناطق جغرافية محددة ويتم وصفها من خلال مجموعة متنوعة من المصطلحات المحددة، والتي من بينها، "التحويلات المباشرة" و"الحوالة" و"السندات الأذنية" Hundi. وبالإضافة إلى قابلية التعرّض للاستغلال من مثل القائمين لعمليات غسل الأموال وتمويل الإرهاب وتعتبر خدمات التحويل المالي البديلة غير المصرّح بها أو غير المرخصة خدمات غير نظامية في المملكة العربية السعودية ومخالفة لنظام مراقبة البنوك ويترتب على مزاوليها عقوبات نظامية ،لذا يجب أن تسعى البنوك ومحلات الصرافة المرخص لها إلى مساندة السلطات في مكافحة هذه الأنشطة غير النظامية.

إن الأشخاص الذين يقدّمون هذه الخدمات يقومون في مرحلة معيّنة، بتوجيه أموالهم بشكل مجمع عبر النظام البنكي ومن خلال الودائع النقدية، ومن ثمّ يحوّلونها إلى الشخص المستفيد بإجراء تحويل أو إتصال/رسالة. لذلك يجب على البنوك ومحلات الصرافة إتخاذ اجراءات احترازية لتحديد ومنع استخدام حسابات العملاء للقيام بمثل هذه الأعمال غير النظامية. وقد تصعب مراقبة هذه العمليات إلاّ أن تطبيق اجراءات العناية الواجبة ومؤشرات غسل الأموال وتمويل الإرهاب ذات الصلة يسهم في التعرّف على هذه العمليات. ويتعيّن على البنوك ومحلات الصرافة، على الاقل إتخاذ الخطوات التالية:

١. وضع آلية لمراقبة حسابات العملاء أو علاقاتهم البنكية لاكتشاف أنماط الأنشطة

accounts or relationships for trends of suspicious activities that could indicate dealing or providing alternative remittance service.
2. No account or relationship should be opened or retained if there is any evidence of the account or relationship being used for any type of alternative remittances (e.g., hawala, hundi). Any activities noted under this category should be reported as suspicious activities to FIU .
3. Obtain satisfactory explanation for a customer who maintains several accounts at various locations without reasonable justification.
4. Have a process in place to monitor activity of a customer who receives numerous small deposits to his/her account from various locations, which are not consistent with his/her line of business in accordance with his/her account profile on file. Such account is often used as "collection account" to accumulate funds from various groups and then sent abroad in a single transaction.
5. Track transactions whereby large cash deposits are credited into a customer account and then immediately followed by a telex transfer to another country.
6. The above trends could indicate that the customer is engaged in offering alternative remittance service illegally and, if banks and money exchangers deemed the activities to be suspicious, these should be reported to FIU.

The above-stated trends are not exhaustive and banks and money exchangers should implement more controls based on experience and understanding of their customers.

المشتبه بها والتي قد تشير إلى التعامل مع خدمات التحويلات المالية البديلة أو تقديمها.

٢. لا يجوز فتح وحفظ أي حساب أو علاقة إذا ثبت بأي طريقة أنها تستخدم لأي نوع من أنواع التحويلات المالية البديلة (مثلاً، الحوالة، الهوندي Hundi). ويجب الإبلاغ عن أي أنشطة تندرج في هذه الفئة على انها أنشطة مشتبه بها إلى وحدة التحريات المالية.

٣. الحصول على تفسير مرضٍ عن أي عميل لديه حسابات عديدة في مواقع مختلفة من دون تبرير منطقي.

٤. وضع اجراءات لمراقبة نشاط العملاء الذين يتلقون عدداً من الودائع الصغيرة في حساباتهم من جهات مختلفة على نحو لا يتفق مع نوعية أعمالهم وفقاً لمعلومات حساباتهم المذكورة في ملفاتهم وغالباً ما تستعمل هذه الحسابات كـ"حسابات تجميع" لتجميع الأموال من مجموعات مختلفة بغية تحويلها إلى الخارج في عملية واحدة.

٥. تتبع العمليات والتي يتم بموجبها إيداع مبالغ نقدية ضخمة في حساب العميل يعقبها تحويل برقي فوري إلى بلد آخر.

٦. قد تشير الأنماط أعلاه إلى أن العميل متورط في تقديم خدمة التحويلات المالية البديلة بأسلوب غير نظامي، وفي حال اشتبهت البنوك ومحلات الصرافة بهذه الأنشطة عليهم الإبلاغ عنها إلى وحدة التحريات المالية.

علما ان الأنماط المذكورة أعلاه ليست شاملة ويجدر بالبنوك ومحلات الصرافة تطبيق المزيد من الضوابط بناءً على تجاربهم وفهمهم لعملائهم.

5.1.4 Money Exchangers

Money Exchange is a regulated business in Saudi Arabia and all money exchangers are subject to the Ministerial Order # 31920 dated 16/2/1402H, which requires all money exchangers to obtain specific license from SAMA. The Ministerial Order prohibits money exchangers from accepting deposits and restricts their activities to purchase and sale of foreign currencies, travelers checks, bank drafts and making remittances inside and outside Saudi Arabia as per the license granted to them by SAMA. The Banking Control Law also prohibits non-banking entities from conducting banking business and, as per authority given, SAMA can impose penalties including revoking of license.

SAMA Account Opening Rules permit banks to open accounts for licensed money exchangers, provided that they have been registered by Ministry of Commerce and licensed by SAMA with a valid licence, specifically indicating that they are allowed to conduct such activity taking into consideration that the license allows cross-border transfers. Therefore, these entities should be categorized as High Risk for an extra customer due diligence and closer scrutiny.

٥,١,٤ محلات ومؤسسات الصرافة

يعتبر تبديل وصرف الأموال من الأعمال المنظمة في المملكة العربية السعودية وتخضع جميع محلات الصرافة للقرار الوزاري رقم ٣١٩٢٠ الصادر بتاريخ ١٤٠٢/٢/١٦هـ، والذي يلزم كافة محلات الصرافة بالحصول على ترخيص من مؤسسة النقد العربي السعودي. كما يحظر الأمر الوزاري على محلات الصرافة قبول الودائع ويحصر أنشطتهم بشراء وبيع العملات الأجنبية والشيكات السياحية والكمبيالات البنكية, والقيام بالتحويلات المالية داخل السعودية وخارجها كلاً حسب الترخيص الممنوح له من قبل مؤسسة النقد. كذلك يحظر نظام مراقبة البنوك على المنشآت غير البنكية من ممارسة الأعمال البنكية. ويمكن لمؤسسة النقد بموجب السلطة الممنوحة لها فرض أي من العقوبات المنصوص عليها في النظام والتي تراها مناسبة بما في ذلك إلغاء الترخيص.

بينما تجيز القواعد الخاصة بفتح الحسابات والصادرة عن مؤسسة النقد العربي السعودي للبنوك فتح الحسابات لمحلات الصرافة المرخص لهم شرط أن يكونوا مسجلين لدى وزارة التجارة ولديهم ترخيص ساري المفعول من قبل مؤسسة النقد العربي السعودي بحيث يسمح لهم بممارسة هذا النشاط. ، مع مراعاة ما اذا كات الترخيص يسمح بتقديم خدمة التحويل إلى خارج الحدود او انه مقتصر على ممارسة نشاط تبديل العملات (الصرافة). لذا يتوجب تصنيف تلك المنشآت ضمن فئة المنشآت ذات المخاطر العالية وتعزيز إجراءات العناية الواجبة وتشديد الرقابة عليها.

5.1.5 Electronic Banking

Electronic banking is a broad term encompassing delivery of information, products and services by electronic means (such as telephones/ mobiles, internet, automated teller machines, points of sales and automated clearing houses). Electronic banking provides opportunities for banks to offer a variety of their banking products and services in a faster, more convenient and cheaper way.

The number of banks providing banking services through electronic means is growing considerably, with increasing range of services becoming available, including account services, credit cards, transfers, bill paying services, shares trading, etc. Therefore, electronic banking is vulnerable to money laundering and terrorist financing because of its user

٥,١,٥ العمليات البنكية الإلكترونية

تشمل العمليات البنكية الإلكترونية تقديم المعلومات والمنتجات والخدمات من خلال وسائل إلكترونية (كالهاتف الثابت/الجوّال، الإنترنت، الصرّاف الآلي، نقاط البيع، وغرف المقاصة الآلية). وتوفر هذه العمليات فرصاً عديدة للبنوك لتقدّم مجموعة متنوعة من منتجاتها وخدماتها بطريقة أسرع وأرخص وأكثر راحة.

ويتزايد عدد البنوك التي تقدّم خدماتها البنكية عبر الوسائل الالكترونية بشكل ملحوظ، كما تتوسع مجموعة الخدمات المتوفرة بما في ذلك خدمات الحسابات وبطاقات الإئتمان والتحويلات وخدمات تسديد الفواتير وتداول الأسهم وغير ذلك. وبالتالي تكون العمليات البنكية الإلكترونية عرضة لغسل الأموال وتمويل الإرهاب بسبب إخفاء إسم المستخدم عند استعمال

anonymity, rapid transaction speed, and its wide geographic availability.

To prevent these risks, banks and money exchangers should be required to have policies in place and take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Such policies and measures should be compatible as a minimum with requirements of the electronic banking services rules issued by SAMA. Banks and money exchangers are not allowed to offer banking products and services through electronic banking payment methods (internet/ online banking, telephone, automated teller machine, mobile or any new electronic payment method) to customers unless they maintain a bank account or other relationship with the bank.

الخدمة وسرعة تنفيذ العمليات وانتشارها الجغرافي الواسع.

ولتفادي هذه المخاطر فإنه ينبغي على البنوك ومحلات الصرافة أن تقوم بوضع سياسات واتخاذ تدابير كافية لمنع سوء استغلال التطورات التكنولوجية في غسل الأموال أو تمويل الإرهاب. وبما يتوائم كحد أدنى مع متطلبات قواعد الخدمات المصرفية الإلكترونية الصادر عن مؤسسة النقد العربي السعودي. كما انه لا يسمح بتقديم المنتجات والخدمات البنكية الإلكترونية (العمليات البنكية على الإنترنت أو الهاتف أو الصرّاف الآلي أو الهاتف الجوّال أو أي وسيلة دفع إلكترونية جديدة) للعملاء ما لم يكن لديهم حساباً مصرفياً أو علاقة أخرى مع البنك.

5.1.6 International Trade

International trade, which deals in the movement of goods and services, can be used either as a cover for the movement of illicit funds or as the money laundering mechanism itself. Criminals will utilize normal trade-related products and services offered by banks relating to import and export operations, such as letters of credit, guarantees, documentary bills for collection, trade financing services, etc., to legitimize the proceeds of their money laundering activities or to provide funding for terrorist organizations, with a relatively low risk of detection. The techniques used basically are: misrepresentation of the price (over-, under- and multi-invoicing of goods/ services), quantity (over- and under-shipments of goods/ services), or quality of imports or exports (falsely described goods/ services).

Banks should watch out for the following examples of red flag indicators that are commonly used to identify trade-based money laundering activities:

1. Discrepancies between the description of the goods on the invoice and bill of lading.
2. The size of the shipment or the type of goods appears inconsistent with the customer's regular business activities.
3. The letter of credit amount is unusually large or sudden surge in number of letters of credit issuance that appears to deviate from the customer's normal business activity.
4. The type of goods being shipped is designated as high risk or involves a high-risk jurisdiction.
5. The transaction involves receipt of payment (especially cash) from third parties with no apparent connection with the transaction.
6. The transaction involves the use of repeatedly amended or frequently extended letter of credit.
7. The transaction involves the use of front (or shell) companies.

٦,١,٥ التجارة الدولية

يمكن استخدام التجارة الدولية التي ترتبط بحركة المنتجات والخدمات إمّا كغطاء لحركة الأموال غير المشروعة أو كآلية بحدّ ذاتها لغسل الأموال, إذ يميل المجرمون إلى استعمال المنتجات والخدمات العادية المتصلة بالتجارة عبر ما تقدمه البنوك في إطار عمليات الإستيراد والتصدير، على غرار خطابات الإعتماد والضمانات وسندات التحصيل الموثقة وخدمات تمويل التجارة إلخ من أجل إضفاء صفة الشرعية على عائدات أنشطة غسل الأموال أو لتمويل المنظمات الإرهابية من دون التعرّض لخطر الإكتشاف. ومن الاساليب المستخدمة في ذلك على سبيل المثال وضع الأسعار بشكل مختلف (أي وضع فواتير عالية الثمن، أو متدنية جداً أو متعددة الأسعار للبضائع/الخدمات)، والكمية (الإفراط في أو التقليل من كمية شحنات البضائع/الخدمات) أو نوعية الواردات او الصادرات (وصف خاطيء للبضائع/الخدمات).

ويجب على البنوك الانتباه للأمثلة عن المؤشرات التالية للتعرّف على أنشطة غسل الأموال وتمويل الإرهاب التي ترتكز على التجارة:

١. الفروقات بين وصف المنتجات في الفاتورة وفي بوليصة الشحن.
٢. عدم تناسب حجم الشحنة أو نوع المنتجات مع أنشطة الأعمال الإعتيادية التي يمارسها العميل.
٣. تكون قيمة خطاب الإعتماد ضخمة على نحو غير إعتيادي أو حدوث زيادة مفاجئة في عدد خطابات الإعتماد التي يتم إصدارها والتي تخرج عن نشاط الأعمال العادية الذي يمارسه العميل.
٤. نوع المنتجات التي يتم شحنها تعتبر ذات مخاطر عالية أو على انها ترتبط بدول عالية المخاطر.
٥. تتضمن العملية إيصال بالدفع (لا سيما الدفع النقدي) من أطراف ثالثة لا يمّت إلى العملية بأي شكل من الأشكال.
٦. تتضمن العملية إستعمال خطاب إعتماد معدّل أو مجددة مدته باستمرار.
٧. تتضمن العملية استخدام شركات الواجهة (أو شركات صورية).

5.2 Country/ Geographic Risks

Country or geographic risks can be defined as risks posed by countries that are subject to sanctions by United Nations (UN), or warnings have been issued against them by other recognized sources, or if SAMA issues certain instructions about some countries and how to deal with the associated transactions due to one factor or a combination of factors, as determined by UN, FATF or SAMA, such as weak unappropriate AML/CTF laws, regulations and other measures, and noncompliance with instructions and recommendations issued by said entities, providing funding or support for terrorist activities; or having significant levels of financial criminal activities.

Banks and money exchangers should exercise additional due diligence and pay special attention to business relations and

٢,٥ مخاطر البلد /المخاطر الجغرافية

وهي المخاطر التي تسببها الدول الخاضعة لعقوبات مفروضة من الأمم المتحدة أو صادر بشأنها تحذيرات من مصادر معتمدة أخرى أو أن تصدر مؤسسة النقد العربي السعودي تعليمات خاصة ببعض البلدان وكيفية التعامل مع العمليات المرتبطة بها بسبب عامل أو مجموعة من العوامل وذلك وفقاً لما يتم تحديده من قبل الأمم المتحدة أو مجموعة العمل المالي أو مؤسسة النقد العربي السعودي، ومنها على سبيل المثال ضعف القوانين والتنظيمات او عدم الالتزام بتطبيق ما يصدر من تلك الجهات من توصيات وسائر التدابير المناسبة لمكافحة غسل الأموال وتمويل الإرهاب، وتقديم التمويل أو الدعم للأنشطة الإرهابية، أو وجود مستويات عالية من الأنشطة المالية الإجرامية.

لذا فإنه يجب على البنوك ومحلات الصرافة تعزيز إجراءات العناية الواجبة مع توجيه اهتمام

transactions with persons, including companies and banks working or doing such activities within these countries or regions. In addition to their duties relating to verification of names of persons and entities listed on the various types of lists and alarming data issued by the above mentioned, Banks and money exchangers should take appropriate countermeasures to reduce the risk of dealing with entities existing in the countries and regions that have weaknesses in their procedures regarding combating money laundering and terrorist financing or do not adequately apply the recommendations of the Financial Action Task Force (FATF). Procedures and measures to be applied by banks and money exchangers are the following:

1. Paying particular attention to business and transactions relations with persons (including legal persons and other financial institutions) from or in countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF).
2. Classification of the risk level of all countries indicated by international organizations, for example, without limitation, Financial Action Task Force (FATF), the Security Council or the Committee on Chapter VII of the UN Charter and others, that warning bulletins have been issued thereon in accordance with a specified risk rate of these entities as a minimum for the classification of the organizations. The actions to be taken to monitor transactions or limit the formation of business relationships and financial operations with concerned countries or persons in these countries.
3. Compliance with the application of instructions of those organizations, whether the warning issued by the Financial Action Task Force (FATF) or decisions of the Security Council and the Chapter VII Commission of the UN Charter, list of any transactions related thereto, preparation of detailed reports thereon, and follow up what relevant authorities issue and take necessary actions thereon.
4. intensification the customer identification requirements in order to know the identity of the beneficiaries owner before establishing work relationships with individuals or companies from these countries.
5. Immediate suspension of dealing with parties, persons or financial institutions of the countries against which financial prohibition decisions have been issued by Security Council and the Chapter VII Commission of the UN Charter. The suspension shall include all banking operations.
6. Exerting enhanced due diligence when making new dealing agreement or opening accounts for correspondent banks with countries of which warning bulletins were issued, whether by FATF, Security Council or Chapter VII Committee of the UN Charter, and making sure not to include the correspondent bank in domestic lists of penalties and prohibition or those issued by the UN.
7. Making immediate update for AML/CTF requirements and exerting enhanced due diligence procedures on all banking transactions of related parties in those countries.
8. Classifying all banking businesses and relationships the bank makes with entities relating to countries of which warning bulletins were issued (government relationships, correspondent banks relationships, companies or individuals commercial relationships, resident customers relationships, etc) at risks level consistent with the nature of those businesses, relationships and the risks level of these countries.
9. Verifying that all banking businesses and relationships, which the bank makes with individuals or entities relating to countries of which warning bulletins were

خاص إلى علاقات الأعمال والعمليات مع الأشخاص بما في ذلك الشركات والبنوك التي تعمل أو تمارس أنشطتها ضمن هذه الدول أو الأقليم. كما انه يجب على البنوك ومحلات الصرافة المرخصة بالاضافة الى واجباتها المتعلقة بالتحقق من اسماء الاشخاص والكيانات المدرجة على مختلف انواع القوائم والبيانات التحذيرية الصادرة من المشار اليها اعلاه القيام باتخاذ الإجراءات المضادة المناسبة التي من شأنها الحد من خطورة التعامل مع الجهات المتواجدة في الدول والأقاليم التي لديها ضعف في إجراءاتها في مجال مكافحة غسل الأموال وتمويل الإرهاب أو تلك التي لا تطبق أو لا تطبق بشكل كافٍ توصيات مجموعة العمل المالي (FATF)، ومن تلك الإجراءات والتدابير الواجب على البنوك ومحلات الصرافة القيام بها ما يلي:

١. إيلاء عناية خاصة بعلاقات العمل والعمليات مع أشخاص (بمن فيهم الشخصيات الاعتبارية والمؤسسات المالية الأخرى) من أو في الدول التي لديها ضعف في إجراءاتها في مجال مكافحة غسل الأموال وتمويل الإرهاب أو التي لا تطبق أو لا تطبق بشكل كافٍ توصيات مجموعة العمل المالي (FATF).
٢. تصنيف مستوى مخاطر جميع الدول المنوه عنها من المنظمات الدولية كافة ومنها على سبيل المثال لا الحصر مجموعة العمل المالي (FATF) أو مجلس الأمن أو لجنة الفصل السابع من ميثاق الأمم المتحدة ...وغيرها الصادر بشأنها نشرات تحذيرية بما يتوافق مع معدل المخاطر المحدد من قبل هذه الجهات كحد أدنى لتصنيف تلك المنظمات، وتحديد الإجراء اللازم اتخاذه بشأن مراقبة التعاملات معها أو الحد من تكوين علاقات العمل والعمليات المالية مع الدول المعنية أو الأشخاص في تلك الدول.
٣. التقيد بالعمل بما تضمنته بيانات تلك المنظمات سواءً التحذيرية الصادرة من مجموعة العمل المالي (FATF) أو قرارات مجلس الأمن وكذلك لجنة الفصل السابع من ميثاق الأمم المتحدة، وحصر أي تعاملات تتعلق بها وإعداد تقارير تفصيلية عنها، ومتابعة ما يصدر من الجهات ذات العلاقة واتخاذ الإجراءات اللازمة بشأنها.
٤. تشديد متطلبات التعرف على العملاء من أجل معرفة هوية المستفيد الحقيقي قبل إقامة علاقات العمل مع أفراد أو شركات من هذه الدول.
٥. التوقف الفوري للتعامل مع الجهات أو الأشخاص أو المؤسسات المالية للبلدان الصادر بحقها قرارات حضر التعامل المالي من مجلس الأمن وكذلك لجنة الفصل السابع من ميثاق الأمم المتحدة على أن يشمل التوقف جميع العمليات المصرفية.
٦. بذل العناية الواجبة المعززة عند إجراء اتفاقية تعامل جديدة أو فتح حسابات للبنوك المراسلة مع الدول الصادر بشأنها نشرات تحذيرية سواءً من مجموعة العمل المالي (FATF) أو مجلس الأمن أو لجنة الفصل السابع من ميثاق الأمم المتحدة ، والتأكد من عدم إدراج البنك المراسل ضمن قوائم العقوبات أو الحظر المحلية أو الصادرة عن الأمم المتحدة.
٧. إجراء تحديث فوري لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب واتخاذ إجراءات العناية الواجبة المعززة لكافة التعاملات المصرفية مع الأطراف ذات العلاقة بتلك البلدان.
٨. تصنيف كافة الأعمال والعلاقات المصرفية التي يجريها البنك مع الجهات التابعة للدول الصادر بشأنها نشرات تحذيرية (علاقات حكومية، علاقات بنوك مراسلة، علاقات تجارية لشركات أو أفراد، علاقات عملاء مقيمين وغيرها من الجهات) بمستوى مخاطر يتلائم مع طبيعة تلك الأعمال والعلاقات وكذلك مع مستوى مخاطر تلك الدول.
٩. التحقق من أن جميع الأعمال والعلاقات المصرفية التي يجريها البنك مع الأفراد أوالجهات التابعة للدول الصادر بشأنها نشرات تحذيرية هي لأغراض اقتصادية أو قانونية واضحة وتحديد المستفيدين الحقيقيين منها وفي ضوء ذلك يجرى تحديد درجة المخاطر ومتطلبات المتابعة اللازمة لها.
١٠. إذا لم يكن لهذه العمليات غرض اقتصادي أو قانوني واضح ينبغي دراسة خلفية تلك العمليات والغرض منها قدر الإمكان والاحتفاظ بنتائج تلك الدراسة بشكل كتابي وإتاحتها عند الحاجة لمساعدة السلطات المختصة.
١١. إجراء مراجعة شاملة لكافة العلاقات التجارية التي يجريها العملاء بما في ذلك

issued, are for clear economic or legal purposes and determining their beneficiaries owner, and in the light of that, determining the level of risk and necessary follow-up requirements.

10. Studying background and purpose of such transactions to the maximum extent possible if they have no clear economic or legal purpose, documenting the results thereof and making them available for the assistance of competent authorities when needed.
11. Conducting a comprehensive review of all customers' business relationships, including letters of credit and guarantees for defining them, determining their purposes and identifying their beneficiaries.
12. Acquainting the senior management and the compliance unit at the bank with current banking relationships established by the bank with entities connected with these countries and obtaining necessary approvals from the bank or supervisory entities to deal with such countries according to the risk level of each case.
13. Full compliance with instructions on reporting suspicious transactions in general, and enhancing reports to the Financial Investigation Unit about suspicious financial transactions with the countries, against which warning bulletins were issued.
14. Bearing in mind all relevant contents of international decisions and warning bulletins issued by different regional and international organizations, referring to these organizations' websites periodically and continuously, searching out in other trustworthy information sources, and taking necessary actions in respect thereof.
15. Sending notifications of supervisory instructions issued on these countries to corporate sector departments of banks or money exchangers, and ensuring the implementation of these supervisory instructions.
16. Compliance with any other additional instructions issued by SAMA to banks and money exchangers concerning certain countries and how to deal with transactions related thereto.

الإعتمادات، والضمانات لحصرها والتأكد من أغراضها وتحديد المستفيدين منها.

١٢. إحاطة الإدارة العليا وإدارة الالتزام في البنك بالعلاقات المصرفية الحالية التي يجريها البنك مع الجهات التابعة لتلك الدول ، وأخذ الموافقات اللازمة من البنك أو من الجهات الإشرافية بشأن التعامل مع تلك الدول حسب خطورة الحالة.

١٣. التقيد التام بتعليمات الإبلاغ عن العمليات المشتبه بها بصفة عامة، وتعزيز البلاغات المتعلقة بالعمليات المالية المشتبه بها مع تلك الدول الصادر بحقها نشرات تحذيرية إلى وحدة التحريات المالية.

١٤. الأخذ في الاعتبار مضمون القرارات الدولية ذات العلاقة كافة والنشرات التحذيرية الصادرة من مختلف المنظمات الإقليمية والدولية، والرجوع إلى المواقع الإلكترونية لتلك المنظمات بشكل دوري ومستمر، والبحث في المصادر المعلوماتية الموثوقة الأخرى واتخاذ الإجراءات اللازمة بشأنها.

١٥. التعميم على قطاعات الأعمال داخل البنك أو محل الصرافة لتشمل الفروع والشركات التابعة الداخلية والخارجية بشأن الإحاطة بالتعليمات الإشرافية الصادرة بهذا الشأن، والتحقق من تنفيذها.

١٦. الالتزام بتطبيق أي تعليمات إضافية أخرى تصدر من مؤسسة النقد العربي السعودي للبنوك ومحلات الصرافة بخصوص بعض البلدان وكيفية التعامل مع العمليات المرتبطة بها.

5.3 Risk Variables

A bank's or money exchanger's risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include:

1. The purpose of an account or relationship.
2. The level of assets to be deposited in relation to the customer's profile.
3. The level of regulatory oversight to which a customer is subject.
4. The regularity or duration of the relationship.
5. The familiarity with a country and regulatory structure.

٣,٥ تغيّرات المخاطر

ان إعتماد البنك أو محل الصرافة على أسلوب مرتكز على المخاطر قد يأخذ بعين الإعتبار تغيّرات المخاطر الخاصة بعميل أو عملية محددة. وقد تزيد هذه التغيّرات أو تقلّص من الخطر الذي قد يسببه عميل أو عملية محددة كما قد تشمل ما يلي:

١. الغرض من حساب أو علاقة ما.
٢. مستوى الأصول التي سيتم إيداعها بالنسبة إلى معلومات العميل.
٣. مستوى الإشراف التنظيمي الذي يخضع له العميل.
٤. مدى انتظام العلاقة أو مدتها.
٥. التعود على بنية البلد وإجراءاتها التنظيمية.

END OF POLICY DOCUMENT

6. Glossary

Account	"Account" should be taken to include, in addition to a bank account, any other similar banking relationships (such as credit card, remittance service relationships, etc.) between the bank or money exchanger and its customer.
Anonymous, Fictitious Name or Numbered Account	Anonymous, Fictitious Name or Numbered Account is generally a bank account for which the customer's name does not appear on the bank's records/ systems, documents and statements. Instead, a unique number or code-name is recorded. The customer's identify is known only to a small number of the bank's officials. While such accounts are offered by some banks in the world for a legitimate purpose, such as providing confidentiality and additional protection for private matters, they can also be misused to hide the proceeds of financial crimes.
Beneficial Owner	The natural person who ultimately owns or controls a customer and/ or the person on whose behalf a transaction is being conducted. It also includes a person who exercises ultimate effective control over a legal person or arrangement.
Competent Authority	All administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including SAMA and SAFIU.
Enhanced Due Diligence (EDD)	This is an additional due diligence process needed for all High Risk accounts/ relationships and where the bank/ME deems it necessary. EDD is needed for PEPs, private banking customers, correspondent banks, non-profit charity organizations, and for other types of customers categorized as high risk by the bank/ME.
Financial Action Task Force (FATF)	It is an international body entitled to oversee AML-CTF efforts. Saudi Arabia is a member of this organization through its membership of the GCC.
Financial Intelligence Unit (FIU)	The UN Convention adopted this definition, stating: "Each state shall consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering." Based on the Saudi AML Law of 2003, the Saudi Financial Intelligence Unit was established under the authority of the Ministry of Interior. This is the authority that receives and analyzes suspicious activity reports from all financial & non-financial institutions.
Intermediary	A professional intermediary is a firm or person (such as an accountant, banker, broker, lawyer or similar professional) who manages an account or transacts on behalf of a client.

٦. التعاريف

الحساب	ينبغي الاخذ بالاعتبار بان "الحسابات" تشمل إلى جانب الحسابات المصرفية علاقات العمل المشابهة الأخرى (البطاقات الإئتمانية، وعلاقة خدمة التحويل المالي، إلخ...) والتي تتم بين البنك أو محل الصرافة وعملائهم.
الإسم المجهول أو الوهمي أو الحساب المرقّم	إن الإسم المجهول أو الوهمي أو الحساب المرقّم هو عبارة عن حساب مصرفي لا يذكر إسم العميل في سجلات/نظم البنك، ومستنداته وكشوفاته بل يسجّل رقم أو إسم مرمّز ولا تعرف هوية العميل إلاّ من قبل عدد محدود من مسؤولي البنك ، وفي حين ان بعض البنوك حول العالم تقدّم هذا النوع من الحسابات لغاية شرعية كتأمين السرية والحماية الإضافية للشؤون الخاصة إلاّ انها عرضة للإستغلال بهدف إخفاء عائدات الجرائم المالية.
المستفيد الحقيقي	*المستفيد الحقيقي* هو الشخص الطبيعي الذي يمتلك أو يسيطر بالكامل على العميل و/أو الشخص الذي تتم العمليات نيابة عنه, كما يتضمن أيضاً الأشخاص الذين يمارسون سيطرة فعالة كاملة على شخصية اعتبارية أو ترتيب نظامي.
السلطات المختصة	*السلطات المختصة* هي كافة السلطات الإدارية وسلطات إنفاذ القانون المرتبطة بمكافحة غسل الأموال وتمويل الإرهاب بما فيها مؤسسة النقد العربي السعودي ووحدة التحريات المالية.
العناية الواجبة المعززة	يعني هذا المصطلح زيادة العناية الواجبة بغرض التحقق من هوية العملاء بالنسبة إلى كافة الحسابات/العلاقات المندرجة ضمن الفئات ذات المخاطر العالية وفي الحالات التي يعتبرها البنك/ محل الصرافة ضرورية. وتطبيق العناية الواجبة الإضافية على الأشخاص المعرفين سياسياً، وعملاء الخدمات المصرفية الخاصة، والبنوك المراسلة والمنظمات الخيرية وغير الهادفة للربح وللعملاء الآخرين المندرجين ضمن الفئات ذات المخاطر العالية بحسب تصنيف البنك/محل الصرافة.
مجموعة العمل المالي	هي منظمة دولية تتولّى الإشراف على الجهود المبذولة لمكافحة غسل الأموال وتمويل الإرهاب.والمملكة العربية السعودية هي عضو في هذه المنظمة من خلال عضويتها في مجلس التعاون لدول الخليج العربية.
وحدة التحريات المالية	إعتمدت الإتفاقية الصادرة عن الأمم المتحدة هذا التعريف على النحو التالي: "يجب على كلّ دولة البحث في إنشاء وحدة للإستخبارات المالية تعمل كمركز وطني لجمع وتحليل ونشر المعلومات المرتبطة بإحتمال غسل الأموال". وبناءً على نظام مكافحة غسل الأموال الصادر عام ٢٠٠٣م أنشئت المملكة وحدة التحريات المالية ووضعت تحت سلطة وزارة الداخلية وهي تمثّل السلطة المخولة بتلقى وتحلّيل بلاغات الأنشطة المشتبه بعلاقتها بغسل الاموال وتمويل الارهاب من كافة المؤسسات المالية وغير المالية.
الوسيط	يعنى به الوسيط المهني شركة أو شخصاً (كمحاسب ومصرفي وسمسار ومحام أو أي مهني مماثل) تدير/يدير حساباً أو تنفّذ/ينفّذ معاملة بالنيابة عن عميل ما.

Money Exchanger (ME)	A natural or legal person who provides a money/ currency changing service and/ or providing a money/ value transfer/ remittance service. The person must be registered by Ministry of Commerce and licensed by SAMA. These entities are subject to SAMA regulations as per authority given through the Banking Control Law, the AML Law (Bylaw 1.1) and the Ministerial Order # 31920.	**محلات الصرافة**	يُقصد بـ محلات الصرافة الشخص الطبيعي أو الإعتباري الذي يقدّم خدمة تبديل عملة ما و/أو يقدّم خدمة تحويل الأموال. ويكون هذا الشخص مسجلاً لدى وزارة التجارة ومرخصاً له من مؤسسة النقد العربي السعودي. ويخضع هذه الكيان لتنظيمات مؤسسة النقد بموجب السلطة المنوطة بها ومنها نظام مراقبة البنوك والقرار الوزاري رقم ٣١٩٢٠بتاريخ ١٤٠٢/٢/١٦هـ والى نظام مكافحة غسل الأموال ولائحة التنفيذية مادة ١,١.
Nominee	A person or firm (registered owner) into whose name securities or other assets are transferred and held under a custodial agreement in order to facilitate transactions, while leaving the customer as the actual owner (beneficial owner). A "nominee account" is a type of account in which a stockbroker holds shares belonging to clients, making buying and selling those shares easier.	**المعيّن**	يعنى بـ *المعيّن* الشخص أو الشركة (المالك المسجّل) الذي/التي تحوّل باسمه/ها الأوراق المالية أو الأصول الأخرى وتوضع تحت إتفاقية حراسة من أجل تسهيل المعاملات بينما يبقى العميل المالك الفعلي (المستفيد الحقيقي). و"الحساب المعيّن" هو نوع من الحسابات يحمل بموجبه المساهم أسهماً تعود إلى عملاء على نحو يسهّل بيع هذه الأسهم وشرائها.
Countries that do not apply or do not fully apply FATF's require-ments	FATF publishes reports and data on countries which do not comply adequately with requirements in the fight against money laundering. The list is maintained and updated by FATF and may be consulted on the FATF website. Banks/MEs should give special attention to business relations and transactions with customers from countries included in these reports, and exercise extra due diligence.	**الدول التي لا تطبيق أو لا تطبيق بشكل كافي متطلبات مجموعة العمل المالي (الفاتف)**	تصدر مجموعة العمل المالي سلسلة بيانات تحذيرية عن الدول التي لا تلتزم بالمتطلبات كما يجب من آجل مكافحة غسل الأموال وتمويل الإرهاب. وتضع قائمة بهذه الدول وهي متوفرة على الموقع الإلكتروني للمجموعة ويتم تحديثها ويجب على البنوك و محلات الصرافة إيلاء اهتمام خاص لعلاقات الأعمال والمعاملات مع العملاء المنتمين إلى الدول الواردة في تلك البيانات وتوخي العناية الواجبة الإضافية في التحقق من هوياتهم.
Payable-Through Account	This is a demand deposit account maintained at a local bank by a foreign bank or corporation, whereby the foreign bank channels deposits and checks of its customers (usually individuals or businesses located outside the country) into the account. The foreign customers have signing authority over the account and can thereby conduct normal international banking activities. This makes it impossible to implement KYC policy and monitoring of suspicious activity process for the customers using the account	**حسابات الدفع المراسلة**	*حسابات الدفع المراسلة* هي حسابات الإيداع تحت الطلب التي يفتحها بنك أو كيان أجنبي لدى بنك محلي لتوجيه الودائع والشيكات الخاصة بعملائه (وهم عادة من الأفراد أو شركات أعمال قائمة خارج البلد) نحو ذلك الحساب. ويتمتع العملاء الأجانب بسلطة التوقيع على الحساب مما يخوّلهم القيام بأنشطة أعمال عادية على المستوى الدولي. وفي هذه الحال يصبح من الصعب تطبيق سياسة "إعرف عميلك" ومراقبة الأنشطة المشتبه بها للعملاء الذين يستخدمون هذا النوع من الحسابات.
Shell Bank	Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.	**البنوك الصورية**	*البنك الصوري* البنك الذي ليس له وجود مادي في الدولة التي تأسس فيها وحصل على ترخيصه منها، والذي لا يتبع/ أي مجموعة خدمات مالية خاضعة لرقابة موحّدة فعالة. ويعني الوجود المادي وجود جهاز وإدارة فعلية داخل دولة ما، أما مجرد وجود وكيل محلي أو موظفين من مستوى منخفض فلا يشكل وجوداً مادياً.
Source of Funds	Source of funds is the activity which generates the funds for a relationship, e.g., a customer's occupation or business activities.	**مصدر الأموال**	تعني عبارة مصدر *الأموال* النشاط الذي يدر الأموال لعلاقة ما (مثل وظيفة العميل أو أنشطة أعماله)
Source of Wealth	Source of wealth is different from source of funds, and describes the activities which have generated the total net worth of a person both within and outside of a relationship, that is those activities which have generated a customer's funds and property.	**مصدر الثروة**	يختلف مصدر الثروة عن مصدر الأموال ويشير إلى الأنشطة التي انتجت وجاءت بالأصول الصافية الإجمالية لشخص ما داخل العلاقة وخارجها أي الأنشطة التي ولّدت أموال العميل وممتلكاته.
Subsidiaries	This refers to majority owned subsidiaries of a bank or money exchanger, inside or outside the country.	**الشركات التابعة**	يعنى بمصطلح *الشركات التابعة* الشركات التي تمتلك المؤسسة الأم (أي البنك أو محلات الصرافة) غالبية أسهمها سواء داخل البلد أو خارجه.

Suspicious Transaction	A suspicious transaction is one in respect of which a banks/ME has reason to believe that some type of wrongdoing or illegal activity may be involved. Suspicious transactions must be reported to the appropriate authorities through Suspicious Transaction Report (STR). The notifying bank/ME and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.	يقصد بـ"المعاملة المشتبه بها" المعاملة التي تعتقد البنوك أو محلات الصرافة لأسباب منطقية انها تنطوي على نشاط غير مشروع أو غير قانوني. ويجب الإبلاغ عن هذا النوع من المعاملات إلى السلطات المعنية من خلال تقرير المعاملات المشتبه بها.. ويعتبر البنك / محل الصرافة الذي قام بالإخطار بمنأى عن أي لوم أو تهمة لجهة عن أي إخطار حصل، سواء إتضح أن المعاملة سليمة أم لا، شرط أن يكون الإخطار قد حصل عن حسن نيّة.	**المعاملة المشتبه بها**
Trustee	A person (an individual or entity) who holds and administers the assets in a trust fund separate from the trustee's own assets, for the benefit of another person/s (the beneficiary/ies). The trustee invests and disposes of the assets in accordance with the settlor's trust agreement, taking into account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.	الأمين هو الشخص (الفرد أو الكيان التجاري) الذي يدير الأصول ويحتفظ بها في صندوق استئماني منفصل عن أصوله الخاصة لمصلحة شخص آخر أو أشخاص آخرين (المستفيد/المستفيدون). وهو يستثمر ويتصرف في هذه الأصول وفق عقد الوصاية المعقود مع المؤمن، آخذ في الاعتبار أية خطابات تتضمن رغباته. وقد يكون هناك أيضاً أمين له سلطة نقض مقترحات الأمناء أو استبعادهم، و/أو أمين قيّم يحتفظ بالأصول حسب أوامر الأمناء القائمين بالإدارة.	**الأمين**
Unusual Transaction	An activity or transaction that is inconsistent with or deviates from the expected pattern of activity within a particular customer, or with the normal business activities for the type of product or service offered. Unusual activity or transaction should alert banks to the possibility of suspicious transactions.	يقصد بـ *المعاملة غير المعتادة* أي نشاط أو معاملة لا ينطبق مع أو يخرج على النمط المتوقع للنشاط لدى عميل محدّد أو أنشطة الأعمال العادية لنوع المنتج أو الخدمة المقدمة ومن شأن النشاط أو المعاملة غير المعتادة أن ينبه البنوك من إمكانية وجود معاملات مشتبه بها.	**المعاملة غير المعتادة**

7. Appendices

٧. روابط وملحقات

SN	Topic	عنوان الموقع الإلكتروني ذات الصلة Related Website Address	الموضوع	رمز الملحق
A	Saudi AML Law & Bylaws	www.sama.gov.sa	النظام السعودي لمكافحة غسل الأموال ولائحته التنفيذية.	أ
B	FATF Recommendations	www.fatf-gafi.org/document	التوصيات الصادرة عن مجموعة العمل المالي (فاتف)	ب
C	FATF Member Countries	www.fatf-gafi.org/pages	الدول الأعضاء في مجموعة العمل المالي (فاتف).	ج
D	Basel Committee Standards	www.bis.org/publ	معايير لجنة بازل	د
E	UN Security Council Resolutions	www.un.org/sc/committees	قرارات مجلس الأمن– الامم المتحدة	هـ
F	Other Useful Resources & Links	www.menafatf.org www.customs.gov.sa/Customs	مصادر وروابط أخرى مفيدة	و

(٨) نموذج تقرير المعاملات المشتبه بها

تقرير المعاملات المشتبه بها

سرّي

رقم المرجع	
التاريخ / / هجري	
الموافق لـ: / / ميلادي	
الملحقات	

معلومات عن الجهة المبلّغة				
مؤسسة مالية (بنك أو محل الصرافة)	إسم البنك أو محل الصرافة	المدينة	الفرع	رقم الهاتف
مؤسسة غير مالية	إسم المؤسسة	المدينة	الفرع	رقم الهاتف

محتويات التقرير				
نوع النشاط/المعاملة	الإيداع	السحب	التحويل	العمليات الأخرى
	الشيك	الفرع		
	النقد	الصرّاف الآلي		
تاريخ تنفيذ المعاملة	الوقت	اليوم	التاريخ	الشهر/السنة
المبلغ الإجمالي	بالأرقام	بالأحرف	نوع العملة	
منفّذ المعاملة	رقم الحساب		إسم/رقم الفرع	البنك
الحساب				
اسباب الإشتباه	**مطلوب تكبير حجم المنطقة**			

المستفيد				
الإسم	رقم بطاقة الهوية	الجنسية	البلد	المدينة
رقم الحساب		إسم/رقم الفرع	البنك المستفيد	

تجدون أعلاه تقرير المعاملات المشتبه بها الذي نعرضه عليكم للمراجعة ولاتخاذ القرار المناسب بشأنه.

الختم الرسمي: التوقيع:

APPENDIX (8)

Suspicious Transaction Report

Confidential

Ref. Number	
Date	/ / H
Corresponding	/ / G
Annexes	

Reporting Party Information				
Financial Institution (Bank or Money Exchanger)	Bank or ME Name	City	Branch	Phone Number
Non-Financial Institution	Institution Name	City	Branch	Phone Number

Report Contents				
Activity/ Transaction Type	Deposit	Withdrawal	Transfer	Others
	Check	Branch		
	Cash	ATM		
Transaction Execution Date	Time	Day	Date	Month / Year
Total Amount	In Figures	In Words	Currency Type	
Transaction Executor	Account Number		Branch Name/ No.	Bank
Account				
Causes of Suspicion				

Beneficiary				
Name	ID Number	Nationality	Country	City
Account Number		Branch Name/ No.	Beneficiary Bank	

Please find above our Suspicious Transaction Report for your review and taking the appropriate decision.

Official Seal: Signature:

(٩) نموذج الإقرار (الإفصاح) النقدي

نموذج الإقرار النقدي

المملكة العربية السعودية **نموذج الإقرار**

وزارة المالية

الجمارك السعودية

التاريخ: الساعة:

يعبّئ هذا النموذج كلّ شخص يملك بحوزته مبلغ ٦٠،٠٠٠ ريال سعودي أو أكثر أو ما يعادله	
الإسم الثلاثي:	
الجنسية:	تاريخ الولادة:
رقم جواز السفر:	
تاريخ ومكان الإصدار:	
العنوان في المملكة العربية السعودية ورقم الهاتف:	
الغاية من السفر:	
البلد القادم منه:	البلد المتوّجه إليه:
إسم المطار/ المرفأ/ الحدود:	
رقم الرحلة:	
العملة / المعادن الثمينة	
نوع العملة:	
القيمة بالريال:	
المعادن: الذهب:	الألماس: المجوهرات الأخرى:
معادل القيمة بالريال:	
مصدر/الغرض من المبالغ النقدية/المعادن الثمينة:	
أقرّ بموجبه ان المعلومات المعلنة أعلاه صحيحة وأقبل بتحمّل المسؤولية الجنائية في حال حدوث أي إقرار كاذب.	
توقيع المسافر:	التاريخ:
للإستعمال الرسمي	
إسم الموظف:	الرقم:
التوقيع:	التاريخ:

ان عدم الإقرار يعرّضك للإستحواب القانوني.

APPENDIX 9

Cash Declaration Form

Kingdom of Saudi Arabia
Ministry of Finance
Saudi Customs

Declaration Form

Date / / Time .....

This form is required to be filled out by whoever having in his possession SR60,000 or more or its equivalent.
Full Name: .....
Nationality: ..... Date of Birth: .....
Passport No.: .....
Place & Date of Issue: .....
KSA Address & Tel. No.: ....
Purpose of Travel: .....
Arriving from: ..... Departing to: .....
Name of the Airport/ Seaport/ Crossing Border: .....
Flight No.: .....
Currency / Precious Metals
Currency Type: .....
Amount in Riyals: .....
Metals: ☐ Gold ☐ Diamond ☐ Other Jewelries .....
The Equivalent in Riyals: .....
Source/Purpose of cash amounts/ precious metals: ....
I hereby acknowledge that the information declared above is correct and I shall be criminally responsible for any mis-declaration. Traveler Signature: ..... Date: .....
Official Use
Employee Name: ..... No.: .....
Signature: ..... Date: .....

Not declaring will expose you to legal questioning .

10.Red Flag Indicators

A. Key Indicators of Regulatory & Legal Weakness (High Risk Geographies)

Money launderers can exploit any country or a geographical region that has weaknesses in its legal and regulatory framework and those involved in financing terrorism and can become a center for money laundering and terrorist financing. As money-laundering and terrorist financing transactions normally require a significant period to complete their stages, money launderers and terrorism financiers often focus on countries with serious shortcomings in their laws and procedures to base their operations.

The existence of the following weaknesses in the legislation of a country can generally create an environment that is conducive for money laundering and terrorist financing transactions to penetrate its banking system:

- Adopting and applying strict banking secrecy laws, thus hindering law enforcement authorities from identifying money-laundering transactions.
- Countries that have lax requirements for the formation and registration of companies and permit the use of bearer shares.
- Absence of any foreign exchange controls on incoming and outgoing funds.
- Countries that do not require or apply strict “Know Your Customer” principles, thus facilitating the opening of untraceable numbered accounts or accounts with fictitious names.
- Facilitating the issuance of financial instruments payable to bearers by banks.
- Countries in which money laundering and terrorist financing is not considered a crime.
- Countries that do not require banks/MEs to notify the concerned authorities of large or unusual fund transfers.
- Countries that do not necessitate notification of suspicious transactions to the concerned authorities.
- Absence of confiscation regulations, or lax enforcement or even non-enforcement of such regulations if they exist.
- Countries that have significant dealings in outgoing foreign draft transfers of cash instruments.
- Countries that have international markets in precious metals and where it is easy to transact such trades.
- Countries that permit the free trading of the U.S. Dollar and particularly where banks are allowed to accept dollar deposits.
- Countries that have banking control laws that facilitate the establishment of banks/MEs particularly in free trade zones where supervisory controls or banking regulations are lax or non-existent.

The classification of an account as high-risk based on the geography of where the customer conducts its business activities depends on whether or not the country is on the FATF list . Since the list keeps on changing, reference should be made to FATF website.

١٠ مؤشرات لعمليات قد تكون مشبوهة

أ. المؤشرات الرئيسة عن الضعف التنظيمي والقانوني (المناطق المدرجة في خانة المخاطر العالية)

يمكن لغاسلي الأموال إستغلال أي بلد أو منطقة جغرافية تعاني من أوجه ضعف في نظامها القانوني والتنظيمي واستغلال أيضاً الأطراف المتورطة في تمويل الإرهاب ليصبح ذلك البلد أو تلك المنطقة مركزاً لغسل الأموال وتمويل الإرهاب. وبما ان معاملات غسل الأموال وتمويل الإرهاب تحتاج عادة إلى فترة من الزمن لاستكمال كافة المراحل، فان غاسلي الأموال ومموّلي الإرهاب غالباً ما يركّزون على البلدان التي تعاني من قصوراً في قوانينها وإجراءاتها ليتخذوا منها قاعدة لعملياتهم.

وبشكل عام، تؤدي أوجه الضعف في النظام التشريعي لبلد ما إلى استحداث بيئة مناسبة لمعاملات غسل الأموال وتمويل الإرهاب بهدف اختراق النظام المصرفي لذلك البلد ونذكر منها:

- إعتماد وتطبيق قوانين صارمة بشأن السرّية المصرفية، الأمر الذي يمنع سلطات إنفاذ القانون من التعرّف إلى معاملات غسل الأموال.
- البلدان التي تضع متطلبات متساهلة بشأن تأسيس الشركات وتسجيلها وتسمح باستعمال الأسهم لحاملها.
- غياب ضوابط العملات الأجنبية على الأموال الواردة والصادرة.
- البلدان التي لا تطلب أو لا تُطبق مبادئ "إعرف عميلك" بشكل صارم، فتسهّل فتح الحسابات المرقّمة التي يصعب اقتفاء أثرها أو حتى الحسابات بأسماء وهمية.
- تسهيل إصدار الأوراق المالية المدفوعة من البنوك لحامليها.
- البلدان التي لا تُجرّم غسل الأموال وتمويل الإرهاب.
- البلدان التي لا تطلب من البنوك/محلات الصرافة إخطار السلطات المعنية بأي تحاويل ضخمة أو غير معتادة.
- البلدان التي لا تفرض إخطار السلطات المعنية بالمعاملات المشتبه بها.
- غياب التنظيمات الخاصة بالمصادرة أو التساهل بتنفيذ هذه التنظيمات لا بل عدم تنفيذها إطلاقاً، إن وجدت.
- البلدان التي تجري بكثرة حوالات أجنبية أو تصدر بكثرة شيكات مصرفية.
- البلدان التي تملك أسواقاً دولية للمعادن الثمينة والتي تسهّل التعامل بهذه التجارة.
- البلدان التي تسمح بالإتجار المجاني بالدولار الأمريكي، لا سيما تلك التي تسمح للمصارف بقبول ودائع بالدولار.
- البلدان التي تضع قوانين الرقابة المصرفية على نحو يسهّل إقامة البنوك/ محلات الصرافة في مناطق التجارة الحرّة بوجه خاص حيث تكون الضوابط الرقابية أو التنظيمات المصرفية متساهلة أو حتى منعدمة.

وان تصنيف الحساب في خانة المخاطر العالية على أساس المنطقة الجغرافية التي يمارس فيها العميل أنشطة أعماله يرتبط بإدراج البلد أو عدمه على بيانات مجموعة العمل المالي بما ان هذه البيانات تتغيّر باستمرار لا بدّ من الرجوع إلى الموقع الإلكتروني الخاص بالمجموعة.

B. Businesses Prone to Money Laundering Activities (High Risk Businesses) Money laundering and terrorist financing can adopt a variety of disguises, but there are certain types of businesses, which are more attractive to criminals. There is also a tendency to use countries that have adopted strict secrecy laws for banks and for companies, which make it difficult to obtain sufficient information to understand the nature and type of business activities being undertaken by these organizations. The following guidance provides an insight into what those businesses might be.	**ب. الأعمال التي تميل إلى أنشطة غسل الأموال (الأعمال المدرجة في خانة المخاطر العالية)** من الممكن إخفاء أنشطة غسل الأموال وتمويل الإرهاب بوسائل عدة، لكن ثمة أنواع من الأعمال تجتذب المجرمين أكثر من غيرها. ويميل هؤلاء أيضاً إلى استخدام البلدان التي اعتمدت قوانين صارمة في السرية المصرفية وسرّية الشركات، الأمر الذي يجعل من الصعب الحصول على معلومات كافية لفهم طبيعة ونوع أنشطة الأعمال التي يمارسها هؤلاء الأشخاص. وتعطي الإرشادات التالية نظرة عن حقيقة هذه الأعمال.
Shell Corporations Legitimate use of shell corporations often provides anonymity for the beneficial owners who may be involved in laundering money or terrorist financing. The use of "professional" nominees to act as directors provides further protection for the money launderer. This coupled with an offshore address can be very effective vehicle for money laundering. Types of businesses covered: Potentially any business. What to look for: The use of such companies where it appears to be an unnecessary complication and the using of less reputable legal and financial advisers to set up and/or maintain the corporation.	**الشركات الصورية** ان الإستخدام الشرعي للشركات الصورية غالباً ما يخفي هوية المستفيدين الحقيقيين الذين قد يتورطون في غسل الأموال أو تمويل الإرهاب. كما ان تولي المعيّنين "المهنيين" مناصب الإدارة في هذه الشركات يوّفر حماية إضافية لغاسلي الأموال. وإذا كان لهذه الشركات عنواناً خارج البلد، فقد تشكّل وسيلة فعّالة جداً لغسل الأموال. **أنواع الأعمال التي تغطيها الشركات الصورية:** أي أعمال محتملة **يجب البحث عن:** إستخدام هذه الشركات في الحالات التي تشكّل فيها تعقيداً كانت بغنى عنه والإستعانة بمستشارين قانونيين وماليين غير معروفين لإنشاء و/أو الحفاظ على الشركة.
Financial Institutions (Non-Bank) By the nature of their business, the receipt and payment of cash will not appear unusual, and some of these businesses will rely upon a casual rather than a regular customer base. Types of business covered: Money Exchangers. What to look for: Appropriateness of turnover levels, sudden fluctuations in turnover, variations in deposit/payment patterns due to a small number of large transactions; large purchases of travelers checks or money orders resulting in encashment from a variety of countries, or the reverse.	**المؤسسات المالية (غير المصرفية)** بحكم طبيعة الأعمال التي تمارسها المؤسسات المالية، فان استلام المال النقدي ودفعه يبدوا أمراً معتاد، لا بل تعتمد بعض هذه الأعمال على قاعدة عملاء مؤقته بدلاً من منتظمة. أنواع الأعمال التي تقوم بها المؤسسات المالية: عمليات الصرافة يجب البحث عن: مدى ملاءمة مستويات أرقام المبيعات، التقلّبات المفاجئة في ارقام المبيعات، التغيّرات في أنماط الإيداع/الدفع بسبب عدد ضئيل من المعاملات الضخمة، الإقبال الكثيف على شراء الشيكات السياحية أو التحاويل النقدية، ما يؤدي إلى قبض هذه الشيكات أو التحاويل من عدة بلدان أو العكس.
Travel Agencies Where such businesses operate a money exchange or travelers checks facility, and have a pattern of international payments as a norm, they are attractive to the money launderer for both placement and layering purposes. What to look for: Payments to countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF). outside of normal patterns; large purchases of travelers checks resulting in encashment from a variety of countries; fluctuations in transaction patterns out of line with normal business patterns.	**وكالات السفر** عندما تقوم تلك الوكالات بالاشتغال باعمال الصرافة أو خدمات الشيكات السياحية او تعتمد نمط المدفوعات الدولية، فهي تصبح جذّابة في عيون غاسلي الأموال لأغراض مراحل الايداع والتغطية. يجب البحث عن: المدفوعات الخارجة ذات الأنماط غير العادية لصالح البلدان المدرجة على "قائمة مجموعة العمل المالي للبلدان التي لا تطبق او لا تطبق بشكل كافٍ توصيات المجموعة"، شراء الشيكات السياحية بكميات ضخمة، ما يؤدي إلى قبضها في بلدان مختلفة، التقلبات في أنماط المعاملات الخارجة كلياً عن أنماط الأعمال العادية.
Import/Export Businesses This is the sort of business that can provide cover for either the placement or layering (through international payments) stages of a money-laundering scheme. These businesses are particularly vulnerable where they are small and where they trade in a variety of products, and/or where the supply or distribution end is conducted largely in cash (typically low value items).	**أعمال الإستيراد/التصدير** يوفّر هذا النوع من الأعمال الغطاء اللازم لمراحل الايداع او التغطية (من خلال المدفوعات الدولية) التي يتألف منها مخطط غسل الأموال. وتعتبر هذه الأعمال ضعيفة إذا كانت صغيرة الحجم وتتاجر بمجموعة متنوعة من المنتجات و/أو تجري عمليات التوريد أو التوزيع بالمال النقدي إلى حدّ كبير (بالنسبة إلى الأصناف المتدنية القيمة على وجه الخصوص).

Precious Commodities The placement of cash, but more usually layering can be facilitated within businesses where large value transactions are common, and the commodities traded are difficult to value objectively, thereby allowing inflated values to be used to support requests for payments. Types of business covered: Precious Metals, Jewel Store; Antique Shops and Fine Art Galleries. What to look for: Trading patterns with countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF)." not normally associated with the commodity in question; unusual fluctuations in turnover or types of financial instruments used.	**السلع الثمينة** تصبح مرحلة الايداع النقدي ومرحلة تغطيتها اسهل ضمن الأعمال التي تقوم على المعاملات الضخمة وحيث يصعب تثمين السلع المتاجر بها بشكل موضوعي، الأمر الذي يسمح باستعمال القيم المضخّمة لدعم طلبات الدفع. أنواع الأعمال التي يشملها هذا النشاط: المعادن الثمينة، محلات المجوهرات والتحف الأثرية ومعارض الفن الجميل. يجب البحث عن: أنماط التجارة مع البلدان المدرجة على "قائمة مجموعة العمل المالي للبلدان التي لا تطبق او لا تطبق بشكل كافٍ توصيات المجموعة" والتي لا ترتبط بالسلعة بحدّ ذاتها، التقلّبات غير المعتادة في أرقام المبيعات أو أنواع الأدوات المالية المستخدمة.
Cash Driven Businesses The types of business that normally accept cash are useful to the launderer at the placement stage, and could be used for layering purposes. Types of businesses covered: Used Car Dealers; Garages; Corner Shops (especially those in some countries who offer check encashment facilities); Electrical Good Stores; Leather Goods Shops; Building & Garden Supplies; Builders or Decorators. What to look for: Increases in cash deposits which do not seem to be matched by an increase in business; the maintenance of cash flow levels when business is falling off, unusual payment patterns from cash deposits seemingly unrelated to the business activities.	**الأعمال القائمة على المال النقدي** تعتبر الأعمال التي تقبل عادة المال النقدي وسيلة نافعة لغاسلي الأموال في مرحلة الايداع كما يمكن استعمالها لأغراض مراحل التغطية. أنواع الأعمال التي تشملها : تجار السيارات المستعملة، المآرب، المحلات الصغيرة (لا سيما تلك التي توفّر في بعض البلدان مرافق لقبض المال النقدي)، محلات الأدوات الكهربائية، محلات المنتجات الجلدية، أدوات البناء والحدائق، شركات البناء أو التصميم. يجب البحث عن: الزيادة في الودائع النقدية التي لا يبدو انها ترافق زيادة في الأعمال، الحفاظ على مستويات تدفق المال النقدي في ظلّ تراجع الأعمال، أنماط الدفع غير المعتادة من ودائع نقدية غير مرتبطة على ما يبدو بأنشطة الأعمال.
Offshore Financial Services Many of the laundering or terrorist financing operations, which have been uncovered, have involved the transfer of funds through offshore financial service companies to layer transactions and provide anonymity. As there is no underlying business against which to test the commercial basis for a transaction it is extremely difficult to detect "unusual" or "suspicious" transaction patterns. Type of businesses covered: Trust Companies; Commodity Traders, Financial Advisers. What to look for: Small operations that appear to have only one or two clients; unusually complex ownership structures; lack of interest in costs incurred when processing transactions; links with to countries that have a weakness in their actions in the fight against money laundering and terrorist financing or do not sufficiently apply recommendations of Financial Action Task Force (FATF) investing in instruments that carry anonymity (e.g. bearer bonds) when uneconomic to do so.	**الخدمات المالية أوفشور** إنطوت العديد من عمليات غسل الأموال وتمويل الإرهاب التي كشف النقاب عنها على عمليات تحويل للأموال إلى معاملات مقسّمة من خلال شركات الخدمات المالية أوفشور، كما أسهمت في إخفاء هوية الفاعلين. وفي ظلّ غياب أي قاعدة أعمال مرجعية يمكن اللجوء إليها لاختبار القاعدة التجارية لمعاملة ما، من الصعب بما كان رصد أنماط المعاملات "غير المعتادة" أو "المشتبه بها". أنواع الأعمال التي تشملها هذه الخدمات: شركات الإئتمان، تجار السلع، المستشارون الماليون. يجب البحث عن: العمليات الصغيرة التي لا تتعدى أكثر من عميل او عميلين، هياكل الملكية المعقّدة بشكل غير معتاد، نقص الفائدة على التكاليف المترتبة على هذه الخدمات أثناء تخليص المعاملات، وجود روابط مع البلدان على "قائمة مجموعة العمل المالي للبلدان التي لا تطبق او لا تطبق بشكل كافٍ توصيات المجموعة"، الإستثمار في الأدوات التي تخفي الهوية (مثلاً: الأسهم لحاملها) عندما يتعارض ذلك مع مبادئ الإقتصاد.
Charitable or Non-Profit Organizations When opening an account for a Charitable or Non-profit Organization, valid authorization from the appropriate government agencies and SAMA must be obtained.	**المنظمات الخيرية أو غير الهادفة للربح:** عند فتح الحساب لصالح منظمة خيرية أو غير هادفة للربح، يجب الحصول أولاً على تصريح ساري المفعول من الجهة الحكومية المختصة ومؤسسة النقد العربي السعودي.
C. <u>Key Indicators of ML/TF Transactions & Activities (High Risk Products/Services)</u> The purpose of this section is to increase the understanding of Bank/ME employees in order to help them in identifying money laundering and terrorist financing transactions. The existence of one or more of these indicators does not necessarily mean that a money laundering or terrorist financing transaction is taking place but it should raise some concerns and lead to further investigation. These indicators are not exhaustive and should be taken by Bank/ME employees for guidance purposes only. Bank/ME employees should depend on their experience, skills and expertise to make a sound judgment on suspected money laundering or terrorist financing transactions, when in doubt, contact the MLCU.	**ج. <u>المؤشرات الرئيسة لأنشطة غسل الأموال وتمويل الإرهاب (المنتجات/الخدمات المدرجة في خانة المخاطر العالية)</u>** يهدف هذا الجزء على زيادة الفهم لدى موظفي البنوك/ محلات الصرافة لمساعدتهم في التعرّف إلى معاملات غسل الأموال وتمويل الإرهاب. وان وجود مؤشراً واحداً أو أكثر لا يشير بالضرورة إلى حدوث معاملة لغسل الأموال أو تمويل الإرهاب بل من شأنه إثارة بعض المخاوف وفسح المجال أمام تحقيقات إضافية. ان هذه المؤشرات ليست وافية ويجب على موظفي البنوك / محلات الصرافة اعتمادها كمؤشرات إرشادية لا غير. فعليهم الاعتماد على خبراتهم، ومهاراتهم ودرايتهم للقيام بحكم سليم على معاملات غسل الأموال او تمويل الإرهاب المشتبه بها، وعليهم الاتصال بوحدة مراقبة غسل الأموال في حال ساورتهم أي شكوك.

General Indicators • A transaction whose general form is indicative of illegitimate or unknown purposes. • Existence of movements in the customer's account not related to his activities such as: - Continuous cash deposits in other companies and establishment accounts. - Unusual purchase of cashier checks and payment orders against cash. - Withdrawal of cash amounts after a short-term deposit. - Large deposits of checks, incoming drafts and payment orders that are inappropriate to the nature of customer's activity. - Large withdrawals or deposits inconsistent with customer's activities. - Transactions for unknown objectives, which do not adhere to the activity of the company its subsidiaries or branches. - Existence of a large number of deposits of small amounts, whether in cash, by check or by incoming draft whose total or approximate total amount deposited, is then transferred to another city or country in one transaction.	**المؤشرات العامة** • المعاملة التي يظهر شكلها العام وجود غايات غير مشروعة أو أهدافها غير معروفة. • وجود حركات في حساب العميل ليست مرتبطة بالأنشطة التي يمارسها، مثل - إستمرار الودائع النقدية في حسابات الشركات والمؤسسات الأخرى. - شراء الشيكات المضمونة وأوامر الدفع مقابل المال النقدي على نحو غير معتاد. - سحب مبالغ نقدية بعد وديعة قصيرة الأجل. - ودائع ضخمة من الشيكات، الكمبيالات وأوامر الدفع الواردة التي لا تتناسب مع طبيعة النشاط الذي يمارسه العميل. - إجراء سحوبات أو ودائع ضخمة على نحو لا يتناسب مع طبيعة النشاط الذي يمارسه العميل. - القيام بمعاملات من دون أهداف معروفة، لا تتلاءم مع نشاط الشركة والشركات التابعة لها أو فروعها. - وجود عدد ضخم من الودائع بمبالغ صغيرة، سواء بالمال النقدي، بالشيكات أو بالتحاويل الواردة بحيث يتم تحويل المبلغ الإجمالي أو التقديري الإجمالي المودع إلى مدينة أخرى أو بلد آخر ضمن معاملة واحدة.
Teller Transactions • Frequent cash deposits by the customer of dirty or excessively used notes. • Cash deposits of large amounts whose source is apparently one of the banks in the same region. • Exchange of a large cash amount consisting of small-denominated notes to the same amount and currency, in bigger denominated notes. • Purchase of cashiers check or precious metals in large amounts. • Transfer of an amount outside of the country without any clear reason. • Deposit of a large number of check or cash amounts by the customer or by other customers without any withdrawals.	**المعاملات لدى أمين الصندوق** • قيام العميل بصورة متكررة بوضع ودائع نقدية بأوراق مصرفية متسخة أو شديدة الإستعمال. • الودائع النقدية الضخمة التي يكون مصدرها أحد البنوك في المنطقة نفسها. • تصريف مبلغ نقدي ضخم يتألف من أوراق مصرفية بفئات صغيرة إلى المبلغ والعملة ذاتها، انما من فئات أكبر. • شراء الشيكات المضمونة أو المعادن الثمينة بمبالغ ضخمة. • تحويل مبلغ إلى الخارج من دون سبب واضح. • إيداع العميل أو العملاء الآخرين عدد كبير من الشيكات أو المبالغ النقدية من دون إجراء اي سحوبات.
Bank Accounts • Opening of more than one account by a customer in his name in the same bank without any clear reason, and existence of inter-account transfer among these accounts. • Accounts opened in names of Tellers in the bank who receive regular deposits or periodic incoming drafts. • Payments or transfers by many persons to a single account whether in cash or through internal drafts. • Opening by a customer of more than one account in the name(s) of his family members and being authorized to manage these accounts on their behalf. • Opening an account by a customer without him physically appearing in the bank or even being known to bank employees or ever visiting the branch for long periods of time. • The existence of bank accounts with address outside the geographical region of the bank. • Existence of large number of movements of big amounts in the account while the balance is kept low or fixed. • Opening of many accounts by the customer with normal balances while the total represents a big amount. • Current or savings account used only to receive incoming drafts from outside in a continuous manner without any justifiable reasons.	**الحسابات المصرفية** • قيام العميل بفتح عدة حسابات باسمه في البنك نفسه، من دون سبب واضح والقيام بتحاويل ما بين هذه الحسابات. • الحسابات المفتوحة باسم أمناء الصندوق (الصرافين) في البنك الذي يتلقى ودائع بانتظام أو حوالات واردة دورية. • قيام عدة أشخاص بمدفوعات أو تحاويل إلى حساب واحد، سواء بواسطة المال النقدي أو الحوالات الداخلية. • قيام العميل بفتح عدة حسابات باسم أفراد عائلته والتصريح له بإدارة هذه الحسابات بالنيابة عنهم. • قيام العميل بفتح الحساب دون الظهور شخصياً أمام البنك أو دون أن يكون معروفاً من موظفي البنك أو عدم زيارة الفرع لفترات طويلة من الزمن. • وجود حسابات مصرفية تحمل عناوين تقع خارج المنطقة الجغرافية للبنك. • حدوث عدد كبير من التحركات في مبالغ ضخمة في الحساب في حين يظلّ الرصيد ثابتاً أو منخفضاً. • قيام العميل بفتح حسابات كثيرة بأرصدة عادية بينما يشكّل المجموع مبلغاً ضخما. • إستخدام الحساب الجاري أو حساب الإدّخار للحصول على حوالات واردة فقط بصورة مستمرة من دون أي أسباب مبررة.
Credit Activities • Unexpected settlement by the customer, of a loan due without disclosing the source of funds. • Obtaining a loan or credit facilities against guarantees issued by a bank operating outside the Kingdom without a clear commercial reason. • Submittal by the customer, of company's shares of which the bank is unable to confirm its business activities, or as a guarantee for obtaining	**أنشطة الإئتمان** • قيام العميل، على نحو مفاجئ، بتسوية قرض مستحق من دون الإفصاح عن مصدر أمواله. • الحصول على قرض أو تسهيلات إئتمانية مقابل ضمانات صادرة عن بنك يعمل خارج المملكة العربية السعودية، من دون سبب تجاري واضح.

a loan or credit facilities. • Submittal, by unknown parties to the bank, of additional guarantees in favor of the customer such as the mortgage of assets or warranties while the bank is unable to define the relationships with the customer or existence of justified reason for such guarantees. • The bank grants loans to customers having deposit accounts in foreign banks in a country having strict banking secrecy laws. • A bank granting loans to foreign companies without a justifiable business reason. • A customer receives a loan and immediately requests the loan amount to be transferred to other bank(s). • Use of credit facilities given to the customer for purposes other than that mentioned in the loan application.	• تقديم العميل أسهم شركة ما لا يستطيع البنك التأكّد من أنشطة أعمالها أو كضمانة للحصول على قرض أو تسهيلات ائتمانية. • قيام أطراف مجهولة بتقديم ضمانات إضافية إلى البنك لمصلحة العميل، مثل رهن الأصول أو الكفالات في حين يعجز البنك عن تحديد الروابط مع العميل أو في ظل غياب سبب مبرر لتلك الضمانات. • قيام البنك بمنح قروض لعملاء يملكون حسابات للإدّخار في بنوك أجنبية في بلد يطبّق قوانين صارمة في مجال السرّية المصرفية. • قيام البنك بمنح قروض إلى شركات أجنبية من دون سبب تجاري مبرر. • حصول العميل على قرض ومطالبته فوراً بتحويل مبلغ القرض إلى بنك آخر أو بنوك أخرى. • إستعمال التسهيلات الإئتمانية الممنوحة للعميل لأغراض غير تلك الواردة في طلب القرض.
Drafts • The amount of draft does not fit with the physical appearance of the sender or the nature of his commercial activity. • The customer's intentional misrepresentation of information given to the bank. • Frequent transfers of large amounts against check under clearing or not cleared.. • Incoming drafts used immediately to purchase financial instruments such as (certificates of deposit, cashier check, etc.) in favor of other parties. • Continuous purchase of bank drafts by customers. • Frequent deposits by a customer of cashier's check issued by foreign banks into his account.	**الشيكات البنكية** • عدم مطابقة قيمة الشيك مع مظهر المرسل أو مع طبيعة نشاطه التجاري. • تعمّد العميل التضليل في الإعلان عن المعلومات إلى البنك. • حصول تحاويل متكررة إلى البنوك لمبالغ ضخمة مقابل الشيكات التي تكون قيد التحصيل. • استعمال الحوالات الواردة فوراً لشراء الأدوات المالية مثل (شهادات الإيداع، الشيكات البنكية، إلخ...) لمصلحة جهات أخرى. • الشراء المستمر للشيكات المصرفية من قبل العملاء. • إيداع العميل بشكل متكرر في حسابه شيكات بنكية صادرة عن بنوك أجنبية.
Customer • Customers who avoid identifying themselves while attempting to process account transactions or even providing incorrect or incomplete information. • The customer attempts to transfer a large amount and then withdraws this application because of the fear of the bank/ME notifying law enforcement authorities. • The customer tries to influence the bank/ME employee not to inform the authorities about a transaction being processed. • The customer refrains from providing information about his previous and current commercial activities and banking relationships and transactions. • The bank/ME employee is suspicious of the customer's identification documentation. • A customer who opens an account without having a local address or a person to verify his or her identity. • The customer gives special instructions to process his transactions by fax or telex without a justified reason to use this communications method.	**العميل** • العملاء الذين يتحاشون التعريف عن أنفسهم عندما يحاولون تخليص معاملات حساباتهم لا بل العملاء الذين يتقدّمون بمعلومات غير صحيحة وغير مكتملة. • محاولة العميل تحويل مبلغ ضخم من المال ثم يتراجع عن هذا الطلب خوفاً من قيام البنك / محلات الصرافة بإخطار سلطات إنفاذ القانون. • محاولة العميل التأثير على موظف البنك / محلات الصرافة لئلا يعلم السلطات بإحدى المعاملات التي يجري تخليصها. • إحجام العميل عن توفير المعلومات بشأن أنشطته التجارية السابقة والحالية وعلاقاته ومعاملاته المصرفية. • إشتباه موظف البنك / محلات الصرافة بصحة الأوراق الثبوتية التي قدّمها العميل. • قيام العميل بفتح حساب من دون امتلاك عنوان محلي أو وجود شخص للتحقق من هويته. • قيام العميل بإعطاء توجيهات خاصة لمعالجة معاملاته بالفاكس أو بالبرقيات من دون وجود سبب مبرّر لاستعمال هذا الأسلوب في التواصل.

Bank's & ME's Personnel

- An employee whose standard of living is not commensurate with his salary.
- An employee who works for very long periods without requesting vacations or having any sick days.
- The connection of an employee with many suspicious transactions while performing his or her duties.
- The employee attempts to facilitate rendering a banking service to customer (individual or company) without applying normal internal banking procedures.
- Changes in Branch Transactions
- Overriding or not implementing the bank's/ ME's internal control directives or intentional non-compliance with the bank's policies and procedures by an employee.
- Increase of money in circulation in large cash denominations that do not match with the nature of work, transactions or location of the branch.
- Material change in the volume of branch transactions with one or more correspondent banks.
- Unusual increase of the volume of drafts issued by a branch or a significant increase in its cash holdings.
- An increase of cashier's check or payment orders sold to Walk-in customers.

موظفو البنوك و محلات الصرافة

- الموظف الذي لا يكون مستوى معيشته متناسباً مع الراتب الذي يتقاضاه.
- الموظف الذي يعمل لفترات طويلة جداً من دون المطالبة بعطل أو الغياب بداعي المرض.
- وجود رابط بين الموظف والمعاملات المشتبه بها أثناء أدائه لمهامه.
- محاولة الموظف تسهيل تأدية خدمة مصرفية إلى أحد العملاء (أكان فرداً أم شركة) من دون تطبيق الإجراءات المصرفية الداخلية العادية.
- التغيير في معاملات الفرع.
- التحايل على توجيهات البنك / محلات الصرافة بشأن الرقابة الداخلية أو عدم تطبيق هذه التوجيهات أو عدم الإمتثال المقصود لسياسات البنك وإجراءاته.
- زيادة المال المتداول بفئات نقدية كبيرة لا تتطابق مع طبيعة العمل و المعاملات أو مع موقع الفرع.
- وجود تغيير مادي في حجم المعاملات التي يجريها الفرع مع بنك مراسل أو أكثر.
- زيادة غير معتادة في حجم الشيكات البنكية الصادرة عن الفرع أو زيادة ملحوظة في موجوداته النقدية.
- زيادة الشيكات االبنكية أو أوامر الدفع التي يتم بيعها للعملاء العابرين.

D. Terrorist Financing Indicators

Accounts

- Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.
- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.
- When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.
- An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).
- An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.)
- An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.
- The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.
- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization.
- An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income.

د. مؤشرات تمويل الإرهاب

الحسابات

- الحسابات التي تستقبل ودائع دورية تارة وتبقى جامدة لفترة من الزمنّ. ثم تستعمل هذه الحسابات لاستحداث خلفية مالية ذات مظهر شرعي لتسهيل القيام بأنشطة فاسدة إضافية.
- تلقي حساب جامد يتضمن مبالغ صغيرة وديعة أو مجموعة من الودائع المفاجئة يعقبها سحوبات نقدية يومية تستمر إلى حين انتهاء المبلغ الذي جرى تحويله.
- رفض العميل، عند فتح الحساب، تقديم المعلومات المطلوبة من المؤسسة المالية ومحاولته تخفيض المعلومات المقدّمة إلى الحدّ الأدنى أو تقديم معلومات مضللة أو يصعب التحقق منها.
- الحساب الذي يوقّع عليه عدة أشخاص مخوّلين بالتوقيع مع انهم لا يرتبطون ببعضهم البعض على الإطلاق (لا وجود لروابط عائلية أو علاقات عمل).
- الحساب الذي يفتحه كيان قانوني أو منظمة قانونية تقع على العنوان نفسه الخاص بكيانات أو منظمات قانونية أخرى وللأشخاص نفسهم سلطة التوقيع عليه في حين لا يوجد أي سبب إقتصادي أو قانوني واضح لقيام هذا الترتيب (مثلا: الأشخاص الذي يعملون كمدراء لشركات متعددة يقع مقرّها الرئيسي على العنوان نفسه، إلخ...).
- الحساب المفتوح باسم كيان قانوني تم تأسيسه حديثاً والذي يستقبل عدداً من الودائع يفوق الحدّ المتوقع بالمقارنة مع الدخل الذي يتقاضاه مؤسسو الكيان.
- الحسابات المتعددة التي يفتحها الشخص نفسه وتستقبل عدة ودائع صغيرة لا تتناسب بمجموعها مع الدخل المتوقع للعميل.
- الحساب المفتوح باسم كيان قانوني متورط في أنشطة إحدى الجمعيات أو المؤسسات التي ترتبط أهدافها بمطالب منظمة إرهابية.
- الحساب المفتوح باسم كيان قانوني، مؤسسة أو جمعية قد تكون مرتبطة بمنظمة إرهابية والذي يشهد تحركات للأموال فوق المستوى المتوقّع للدخل.

Deposits and Withdrawals

- Deposits for a business entity in combinations of monetary instruments that are a typical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security check).
- Large cash withdrawals made from a business account not normally associated with cash transactions.
- Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in check or other payment instruments.
- Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.
- Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.
- The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.
- The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.
- The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.
- The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

Wire Transfers

- Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.
- Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.
- Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.
- Characteristics of the customer or his/her business activities.
- Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).
- Stated occupation of the transaction is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
- Frequent transfers of amounts to other banks without mentioning the name of the beneficiary.
- The amount of draft does not fit with the physical appearance of the sender or the nature of his commercial activity.
- Frequent transfers of large amounts to and from countries known to be

الودائع والسحوبات

- الودائع الخاصة بكيان تجاري والتي توضع إلى جانب أدوات نقدية تعتبر نشاطاً نموذجياً يرتبط عادة بأعمال ذلك الكيان (مثلاً: الودائع التي تتضمن مزيجاً من الأعمال، جدول الرواتب وشيكات الضمان الإجتماعي).
- حصول سحوبات نقدية ضخمة من حساب إحدى الشركات من دون أن تكون مرتبطة بمعاملات نقدية.
- إيداع أموال نقدية ضخمة في حساب فرد أو كيان قانوني في حين تجري أنشطة الأعمال الظاهرة لذلك الفرد أو الكيان بموجب الشيكات أو أدوات الدفع الأخرى.
- مزج الودائع النقدية والأدوات النقدية في حساب واحد لا تبدو المعاملات فيه انها ترتبط بأي وجه كان بالإستعمال الطبيعي للحساب.
- تنفيذ معاملات متعددة في اليوم نفسه وفي فروع مختلفة لمؤسسة مالية واحدة في إطار محاولة لاستعمال أمناء صندوق مختلفين.
- عمليات إيداع أو سحب نقدي متكررة بمبالغ تقل بمقدار ضئيل عن السقوف المحددة لتطبيق متطلبات التعريف أو التبليغ.
- تقديم مبالغ غير معدودة لتنفيذ عملية، وخفض مبلغ العملية بعد عد النقد إلى حد يقل بمقدار طفيف عن السقف المقرر لتطبيق متطلبات التعريف أو التبليغ.
- إيداع أو سحب أدوات مالية متعددة بمبالغ تقل بمقدار بسيط عن السقوف المحددة لتطبيق متطلبات التعريف أو التبليغ, خصوصاً إذا كانت الأدوات المالية مرقمة تسلسلياً.

الحوالات البرقية:

- حوالات برقية بمبالغ ضئيلة الغرض منها تجنب تطبيق متطلبات التعريف أو التبليغ.
- حوالات برقية من/إلى فرد لا تتضمن بيانات المحول أو الشخص الذي أجريت الحوالة نيابة عنه إذا كان من المتوقع تضمين تلك البيانات في الحوالة.
- استخدام حسابات شخصية وتجارية متعددة أو حسابات منظمات غير هادفة للربح أو جمعيات خيرية لجمع وتحويل الأموال فوراً أو بعد فترة قصيرة إلى عدد ضئيل من المستفيدين الأجانب.
- عمليات العملات الأجنبية التي تنفذ نيابة عن عميل من قبل الغير ويتبعها تنفيذ حوالات برقية إلى مواقع لا يبدو أن لها علاقة جلية بالعميل أو إلى الدول المستهدفة التي تبعث على القلق بشكل خاص.
- توصيف العميل أو نشاطاته التجارية.
- الأموال المتأتية من نشاط مملوك لأفراد ينحدرون من نفس جهة المنشأ أو مشاركة أفراد متعددين ينحدرون من نفس جهة المنشأ ويتبعون لدول مستهدفة تبعث على القلق بشكل خاص يتصرفون نيابة عن نشاطات تجارية مماثلة.
- استخدام عناوين مشتركة لأفراد يشاركون في عمليات نقدية خصوصاً عندما يكون العنوان نفسه عنواناً لمنشأة تجارية و/أو لا يبدو متطابقاً مع المهنة المحددة (مثال: طالب، عاطل عن العمل، شخص يعمل لحسابه الخاص ... الخ).
- المهنة المذكورة لأغراض العملية غير متطابقة مع مستوى أو نوع النشاط (مثال: طالب أو شخص عاطل عن العمل يستقبل أو يرسل عدداً كبيراً من الحوالات البرقية أو يقوم بتنفيذ عمليات سحب نقدي يومية بالمبالغ القصوى من مواقع متعددة ضمن منطقة جغرافية واسعة).
- فيما يخص المنظمات غير الهادفة للربح أو الجمعيات الخيرية: العمليات المالية التي لا يبدو أن لها غرض اقتصادي واضح أو لا توجد صلة بين النشاط المحدد للمنظمة أو للجمعية والأطراف المقابلة في العملية.
- فتح صندوق أمانات نيابة عن منشأة تجارية عندما يكون النشاط التجاري للعميل غير معروف أو أن النشاط المذكور لا يبرر استخدام صندوق أمانات.
- حصول تحاويل متكررة للأموال إلى بنوك أخرى من دون ذكر اسم المستفيد
- حصول تحاويل متكررة للأموال إلى بنوك أجنبية من دون وجود تعليمات بالدفع نقداً إلى المستفيد

a source for drugs • Fragmenting a large amount into smaller amounts upon transfer. • Frequent transfers to banks in countries known with strict banking secrecy laws. • Cash transfers in large amounts. • Deposits in different accounts and then consolidating these amounts in one account and then transferring the total amount outside of the Kingdom. • Requests by the customer to the bank to transfer amounts to foreign banks against incoming drafts to the same account with equivalent amounts.	• حصول تحاويل متكررة لمبالغ ضخمة إلى ومن البلدان المعروفة بكونها مصدراً للمخدرات • تجزئة مبلغ كبير من الأموال إلى مبالغ صغيرة عند إجراء التحويل • حصول تحاويل متكررة إلى البنوك العاملة في البلدان التي تطبّق قوانين صارمة في مجال السرّية المصرفية • حصول تحاويل نقدية لمبالغ ضخمة • وضع ودائع في حسابات مختلفة، ثم ضمّها إلى حساب واحد قبل تحويل المبلغ الإجمالي إلى الخارج طلب العميل من البنك تحويل مبالغ إلى بنوك أجنبية مقابل حوالات واردة إلى الحساب نفسه بمبالغ معادلة
Transaction Linked to Locations of Concern • Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF • Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF). • A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern. • The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern. • A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations. • The opening of accounts of financial institutions from locations of specific concern.	**العمليات المرتبطة بمواقع تبعث على القلق:** • العمليات التي تنطوي على مبادلات العملات الأجنبية تتبعها بعد فترة قصيرة حوالات برقية لمواقع تبعث على القلق بشكل خاص (كالدول المستهدفة المحددة من قبل السلطات القومية أو الكيانات المدرجة في البيانات التحذيرية لمجموعة العمل المالية • عمليات إيداع تتبعها بعد فترة وجيزة حوالات مالية خصوصاً تلك التي تتم إلى أو من خلال موقع يبعث على القلق بشكل خاص (كالدول المستهدفة المحددة من قبل السلطات القومية أو الكيانات المدرجة في البيانات التحذيرية لمجموعة العمل المالية). • حساب تجاري ينفذ عليه عدد كبير من الحوالات البرقية الواردة أو الصادرة ولا يبدو أن هناك غرض تجاري أو اقتصادي منطقي لها خصوصاً عندما تتم هذه العمليات إلى أو من خلال موقع يبعث على القلق بشكل خاص. • استخدام عدد من الحسابات لتجميع الأموال ومن ثم تحويل المبالغ لعدد صغير من الأجانب سواءً كانوا أفراد أو مؤسسات تجارية خصوصاً إذا كانوا في مناطق تبعث على القلق. • حصول العميل على أداة ائتمانية أو إجراؤه لعمليات مالية تجارية تتضمن تحريك الأموال من أو إلى مواقع تبعث على القلق بشكل خاص في غياب أي أسباب تجارية منطقية للتعامل مع تلك المواقع. • فتح حسابات لمؤسسات مالية من مناطق تبعث على القلق بشكل خاص.