



مجموعة العمل المالي

لمنطقة الشرق الأوسط وشمال أفريقيا



مجموعة العمل المالي

تقرير التقييم المشترك

مكافحة غسل الأموال وتمويل الإرهاب

المملكة العربية السعودية

٤ مايو ٢٠١٠

:
:

() ()

©

:)

-

: .

(info@menafatf.org :

+

٢		
٤		
١٤		-
١٤		-
	١٩	-
٢١		-
٢٧		-
٢٨		-
٣٤		-
٣٤	()	-
٤٢	()	-
٤٧	()	-
٥٢	()	-
٥٩	()	-
	-	-
٧٢		()
٧٩	()	-
٨٧		-
٩٠		-
٩١	()	-
١١٩	()	-
١٢٣	()	-
١٢٥	()	-
١٣٢	()	-
١٤٠	()	-
١٤٧	(&)	-
١٥٣	()	٩.٣
)	-
١٥٤	()	()
١٧٨	()	-
١٨٢		-
١٨٢	()	-
١٨٩	()	-
١٩٤	()	-
١٩٩	()	-

٢٠١			-
٢٠١.....()		-	-
٢٠٣.....()		-	-
٢٠٤.....()			-
٢١٠.....			-
٢١٠.....()			-
٢١٣.....()			-
٢١٥.....()			-
٢٢٣.....()			-
٢٢٦.....()			-
٢٣٤.....			-
٢٣٤.....			-
٢٣٦.....		:	
٢٤٨.....		:()	
٢٦١.....()		:	

(CFT) (AML) ١

(FATF)
(CFT) (AML)

٢

(FATF) (MENAFATF) " "

) (FATF) (MENAFATF)

) (MENAFATF)
) (FATF)

((MENAFATF)

) (FATF)

) (FATF) (

((FATF)

(MENAFATF)

(AML/CFT)

(FIs)

(FT)

(ML)

(DNFBPs)

(AML/CFT) ٣

^١ في هذا التقرير، تشير كلمتا "المملكة" و"السعودية" إلى المملكة العربية السعودية.
^٢ كما تم تحديثها في أكتوبر عام ٢٠٠٨.

()

()

3

2

ملخص تنفيذي

١. معلومات أساسية

٥.

٦.

()

()

٧.

)

(

()

.(

^

)

9

.(

)

.)

(

)

/

))

.۱۲

()

.۱۳

()

()

.۱۴

.10

()

.16

.17

.18

.19

.20

)

(

.21

.22

(

)

.23

.۲۴

()
()

.۲۵

.۲۶

.۲۷

.۲۸

.۲۹

.۳۰

.۳۱

()

()

۳۲

/ /

۳۳

۳۴

۳۵

۳۶

()

.۳۷

.۳۸

.۳۹

.۴۰

.۴۱

.۴۲

٤٣

٤٤

٤٥

()

58

:

59

() :

60

:(")

()

61

()

62

" " " "

٦٣

() ()

(ML)

٦٤

(TF)

٦٥

٦٦

^٨ قال تعالى: "ولا تأكلوا أموالكم بينكم بالباطل (بأي طريق غير شرعي مثل السرقة والسلب والخداع،... إلخ) وتدلوا بها إلى الحكام (القضاة الذين يفصلون في قضاياكم) لتأكلوا فريقًا من أموال الناس بالإثم وأنتم تعلمون" (سورة البقرة، الآية رقم ١٨٨)
^٩ وفي السنة، يوضح النبي (صلى الله عليه وسلم) ذلك بقوله "إن الله إذا حرّم شيئاً حرّم ثمنه".
^{١٠} قال تعالى: "...وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان..." (سورة المائدة، الآية ٢)
^{١١} مرسوم مجلس الوزراء رقم (٤٣) (٥٦٥٧/ب/٧) الصادر في ١٤٢٨/٢/١ هجرية
^{١٢} بموجب مرسوم ملكي رقم م/٣٦ بتاريخ ١٤١٢/١٢/٢٩ هجرية.
^{١٣} قرار مجلس الوزراء رقم ٨/٢١١١ إلى ١٤٠٠/١٢/١ هجرية.

()

.٦٧

.٦٨

.٦٩

.٧٠

.٧١

()

^{١٥} دون احتساب الخسائر في الأرواح بين الإرهابيين، حيثما أمكن.

()

)		
	(
)
			.(
)
			(..

		• •		
		• • • •		
		• • • • • •		
		• • • •		

.۷۳

()

() (

)

() :

()

.(

)

/

.۷۴

)

(

(SAMA)

(-)

(CMA)

.۷۰

)

.(

.(

)

.(

)

.۷۶

.(

)

(

)

.(

)

.۷۷

)

.۷۸

(

۱۹۶۶

" " " ")
 .(" "
 .())
 %)
)
 ()
 .٧٩
 :) %
 ()
 ())
 () ()
)
 .٨١
 .(
 .
 .
 .٨٢
 ()
 ()

^{١٧} مرسوم ملكي رقم (٣٢/م) في ١٤٢٤/٦/٢ هجرية.

^{١٨} قرار وزارة المالية في ١٤٢٥/٣/١ هجرية.

^{١٩} يجب ملاحظة أنه وفقاً للسلطات، فإن شركات التأمين غير المرخصة تخضع أيضاً للإشراف، إلا أن فريق التقييم لم يلتقي بهذه الشركات غير المرخصة، وبالتالي، تعذر التحقق من ذلك.

^{٢٠} قرار وزارة المالية رقم ١٥٦٦/١ في ١٤٢٠/٧/٢١ هجرية.

٨٣ ()

()
)

.(

()

٨٤

)

(

٨٥

٨٦

٢١

٨٧

٢١ Arab News الجاسر قد يؤذن بدخول مرحلة مصرفية جديدة، الاثنين ٢ مارس ٢٠٠٩ (السادس من ربيع الأول ١٤٣٠)

.٨٨

.٨٩

.٩٠

.٩١

/

()

^{٢٢} الاسم الرسمي لهذا النوع من الترتيبات القانونية التي توجد في المملكة هو الوقف الخاص. وفي هذا التقرير، يستخدم مصطلح الصندوق الاستئماني أيضًا للدلالة على الوقف الخاص.

-

.٩٢

() :

()

()

()

()

() :

.٩٣

()

()

()

()

()

()

() :

.٩٤

()

.٩٥

.٩٦

.٩٧

() ()

^{٢٣} علمًا بأن الوقف العام هو منظمة غير هادفة للربح في حين أن الوقف الخاص هو ترتيب قانوني.

-
.
98

.
99

.00
()
(

.01
)

.(

١٠٢

١٠٣

١٠٤

١٠٥

١٠٦

)

(

^{٢٤} رقم (٥) في ١٧/١/١٤٢٠ هجرية.

.١٠٧

) ()
.(

.١٠٨

(SAFIU) .١٠٩

.١١٠

^{٢٥} مرسوم ملكي س/٢٠١٦٧، بتاريخ ١٠/١٠/١٤٢٢ هجرية الموافق (٢٥ ديسمبر عام ٢٠٠١).
^{٢٦} يتم استخدام مصطلح وحدة التحريات المالية السعودية ومصطلح وحدة التحريات المالية في هذا التقرير للإشارة إلى وحدة المعلومات المالية بالمملكة العربية السعودية، ما لم يرد خلاف ذلك.

.111

.112

.113

.114

/

.115

()
- ()

.116
-

	-
	.١١٧
()	.
()	.
()	.
	-
	.١١٨
	.١١٩
()	
()	
	.١٢٠
()	
()	

^{٢٧} يعد أحد الاعتبارات الهامة المتضمنة في توصيات مجموعة العمل المالي هو درجة مخاطر غسل الأموال أو تمويل الإرهاب بالنسبة لأنواع معينة من المؤسسات المالية أو أنواع معينة من العملاء أو المنتجات أو العمليات. وبناءً على ذلك، بإمكان أي بلد أن يضع المجازفة في الاعتبار وبإمكانه أن يقرر الحد من تطبيق بعض توصيات مجموعة العمل المالي شريطة استيفاء الشروط المحددة (راجع منهجية مجموعة العمل المالي لتقييم مدى الالتزام بالتوصيات الأربعين لمجموعة العمل المالي والتوصيات التسع الخاصة الصادرة عن مجموعة العمل المالي).

^{٢٨} مجلس التعاون الخليجي عضو في مجموعة العمل المالي، والمملكة العربية السعودية عضو في مجلس التعاون الخليجي. ولذلك أجريت تقييمات لدول مجلس التعاون الخليجي من قبل مجلس التعاون الخليجي بالتعاون مع مجموعة العمل المالي. وفي وقت التقييم السابق، لم تكن مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا لمكافحة غسل الأموال وتمويل الإرهاب موجودة.

-

()

-

--

.١٢١

)

()

(

.١٢٢

)

.(

.١٢٣

:

^{٢٩} قرار المحكمة على "س" بتاريخ ١٧/٠٩/١٤١٩ هجرية (٤ يناير ١٩٩٩ ميلادية).

١٢٤

:

() () () - () () ()]

.[() () () () ()

١٢٥

-

"

-

.

"

.

١٢٦

-)

.(

.() " "

١٢٧

." ")
.(- -)

١٢٨

31

١٢٩

(-)

^{٣٠} راجع الملاحق للحصول على نسخة كاملة من قانون مكافحة غسل الأموال.
^{٣١} القضية رقم ٢٨/٧٦، المحكمة العامة بالرياض، ٢٩/٠٣/١٤٢٩ هجرية.

" ")

(-)

()

()	() () ()	
.	() ()	
()	() ()	
	() ()	
	() ()	
	() ()	
	()	
	(-) ()	
	()	
- - /		
	() ()	

	()	
	() () ()	
- - -	() ()	
	()	
	() ()	
	() ()	
) (
() ()	()	
- - -	()	

.١٣١

) ()
(.
)
(

^{٣٢} قال تعالى "ولا تعتدوا إن الله لا يحب المعتدين" (سورة المائدة الآية ٨٧) وقوله تعالى "وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان".

١٣٢ . ()
()

١٣٣ . (/)
(-)

١٣٤ .

١٣٥ .
" "
" "
()

^{٣٣} القضية رقم ٢٨/٧٦، المحكمة العامة بالرياض، ٢٩/٠٣/١٤٢٩ هجرية.
^{٣٤} القضية رقم ٣٤/١٢٠، المحكمة العامة بالرياض، ١٠/٠٦/١٤٢٨ هجرية.

.١٣٦

-
-
)
(.

.١٣٧

" "

-

()

.١٣٨

.١٣٩

.١٤٠

) ()
() ()
() ()

^{٣٥} أشارت السلطات السعودية إلى تعريف الجريمة المنظمة الموجود في اتفاقية باليرمو ولكن لم يتم تطبيق أي حكم قانوني لهذا التعريف على المستوى الوطني. ومن الناحية العملية، لا يمثل ذلك أي مشكلة للسلطات السعودية. ولكن الفشل في تطبيق الاتفاقيات الدولية يجعل هذه المسألة غير واضحة بصورة كبيرة وبالتالي يصبح موضوع تطبيق مثل هذه الاتفاقيات من خلال القانون السعودي غامضاً.

()

.)

)

.۱۴۱

.)

)

.۱۴۲

"

"

.۱۴۳

(

)

.)

)

.۱۴۴

()				
(0)				
()				
()				
()				

)
(.

.١٤٧

.١٤٨

--

/	•	
-	•	
)	•	
(•	
()	•	
()	•	

()

-

--

.١٤٩

^{٣٧} قال تعالى: "إِنَّمَا جَزَاءُ الَّذِينَ يُحَارِبُونَ اللَّهَ وَرَسُولَهُ وَيَسْعَوْنَ فِي الْأَرْضِ فَسَادًا أَنْ يُقَتَّلُوا أَوْ يُصَلَّبُوا أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُمْ مِنْ خِلَافٍ أَوْ يُنْفَوْا

مِنَ الْأَرْضِ"

^{٣٨} قال تعالى: "وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَىٰ وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ" "فَالْإِنْسَانُ الطَّاهِرُ الَّذِي يَعِيشُ فِي بَيْتِ الْفَاسِدِينَ لَا يَنْتَمِي إِلَيْهِمْ فَفَقَط، بَلْ هُوَ وَاحِدٌ مِنْهُمْ" حيث يعتبر تمويل الإرهاب هو شكل من أشكال الاعتداء المهني حسب قول الله تعالى: "ولا تعتدوا إن الله لا يحب

/

١٥٠

()

()

()

(-)

() ()

() ()

١٥١

١٥٢

()

()

() :
 () ()
 ()

١٥٣
) .
 ()

() ١٥٤
 () ()
 ()

١٥٥
()

١٥٦
١٥٧
()

^{٣٩} القضية رقم ٣٤/١٢٠، المحكمة العامة بالرياض، ١٠/٠٦/١٤٢٨ هجرية.

.158

(.)

((: .() (.159 (

.160

()

.(.)

.161

() ()	" "	•		
()	" "	•		
)	(•		
		•		

()

-

--

.174

()

()

.170

()

()

.166

":

(- .

)
()

() ()

"

•

"

"

(. .) ."

"

•

.(.)"

" "

.167

.()

.()

()

.168

.()

/

.169

)

.(

"

	"	
	/	
)		.١٧٠
	(
.()	.١٧١
	(
)	.١٧٢
		.١٧٣
	(
)	()
		.١٧٤

^{٤٠} سورة الزمر الآية ٧: قال تعالى "إِن تَكْفُرُوا فَإِنَّ اللَّهَ غَنِيٌّ عَنْكُمْ وَلَا يَرْضَىٰ لِعِبَادِهِ الْكُفْرَ وَإِن تَشْكُرُوا يَرْضَاهُ لَكُمْ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ثُمَّ إِلَىٰ رَبِّكُمْ مَرْجِعُكُمْ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ إِنَّهُ عَلِيمٌ بِذَاتِ الصُّدُورِ".

--

()

.178

)

(

.179

."

")

.180

--

()	•	
:	•	
	○	
	○	
	•	
	○	
	○	
	○	

()

-

- -

.١٨١

()

.١٨٢

/ .١٨٣

) " (

^{٤١} تنص الفقرة الثانية من المذكرة التفسيرية للتوصية الخاصة الثالثة لمجموعة العمل المالي على: "إن هدف المتطلب الأول هو تجميد الأموال المرتبطة بالإرهاب أو الأصول الأخرى القائمة على أساس معقول للاشتباه أو الاعتقاد بأن مثل هذه الأموال أو الأصول الأخرى يمكن استخدامها لتمويل نشاط إرهابي. والهدف من المتطلب الثاني هو تجريد الإرهابيين من هذه الأموال أو أصول أخرى في حالة وجود أو عندما توجد روابط محددة بشكل سليم بين الأموال والأصول الأخرى وبين الإرهابيين والنشاط الإرهابي. أما القصد وراء الهدف الأول فهو وقائي بينما مع المتطلب الثاني هو في الأساس وقائي وعقابي. ويعتبر كل من المتطلبين أمر ضروري لتجريد الإرهابيين وشبكاتهم من وسائل القيام بنشاط إرهابي في المستقبل ومن الحصول على البنية الأساسية الخاصة بهم بالإضافة إلى العمليات".

١٨٤

٤٤

١٨٥

١٨٦

) "

"

.(

١٨٧

^{٤٢} برقية من سمو وزير الداخلية برقم (٣٥٨٣١/١) بتاريخ ١٤٢٨/٥/٢٥ هجرية.

^{٤٣} برقية من سمو وزير الداخلية برقم (٥١١٩٦/١) بتاريخ ١٤٢٨/٨/٦ هجرية.

^{٤٤} تعميم ١٢٠-أم أي تي-١٢٨٧٢، ١٢ رجب ١٤٢٢ هجرية

^{٤٥} والآلية ٣١٢٥ بتاريخ ١٤٣٠/٠٤/١٠ هجرية

(())

()

.188

()

()

.189

" "

()

()

.١٩٠

(

()

.١٩١

()

/ /

.١٩٢

^{٤٦} تطالب التوصية الخاصة رقم ٣ وكذلك قرار مجلس الأمن رقم ١٢٦٧ بالتالي: "يتم بدون تأخير تجميد الأموال أو الأصول الأخرى التي يملكها أو يتصرف فيها تنظيم القاعدة وحركة طالبان وأسامة بن لادن أو الأشخاص والكيانات المرتبطة بهم وذلك كما حددته لجنة الأمم المتحدة لعقوبات تنظيم القاعدة وحركة طالبان والتي تأسست وفقًا لقرار مجلس الأمن رقم ١٢٦٧ (عام ١٩٩٩ م)، وتتضمن الأموال المستمدة من أموال أو أصول أخرى يمتلكونها أو يتصرفون فيها، بشكل مباشر أو غير مباشر، أو بواسطة أشخاص يتصرفون بالنيابة عنهم أو بتوجيهاتهم مع التأكد من أن هذه الأموال أو غيرها من الأموال أو الأصول الأخرى ستكون متاحة، بشكل مباشر أو غير مباشر، لمنفعة هؤلاء الأشخاص، بواسطة مواطنيهم أو أي شخص موجود في مناطقهم".

()

.١٩٣

()

.١٩٤

()

()

.١٩٥

() ()

()

() .١٩٦

()

^{٤٧} سورة الزمر الآية ٧: قال تعالى "إِن تَكْفُرُوا فَإِنَّ اللَّهَ غَنِيٌّ عَنْكُمْ وَلَا يَرْضَىٰ لِعِبَادِهِ الْكُفْرَ وَإِن تَشْكُرُوا يَرْضَهُ لَكُمْ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ثُمَّ إِلَىٰ رَبِّكُم مَّرْجِعُكُمْ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ إِنَّهُ عَلِيمٌ بِذَاتِ الصُّدُورِ".
^{٤٨} يرى الفريق أيضًا أنه بافتراض وجود متطلب قانوني للمؤسسات المالية والأعمال والمهين غير المالية المحددة من أجل التجميد، سوف تعاني عملية متابعة هذا المتطلب من نفس أوجه القصور في الإشراف كما هو موضح في القسم ٣.١٠ من هذا التقرير.

()

.197

()

()

)

.198

(

.199

.200

.201

()

۲۰۲

()

۲۰۳

()

()

۲۰۴

۲۰۵

--

()	:	• • • •	
	:		

	• •		
--	--------	--	--

()

-

--

.٢٠٦

.٢٠٧

.٢٠٨

() :

()

()

()

()

^{٤٩} تعميم رقم ١ س هـ/٤٦٢٨٧ في ١/٨/١٤٢٦ هجرية والصادر من وزير الداخلية.

()

()

()

()

()

/

()

()

()

.209

)

(

%

.210

()

:

)

.(

.211

:

()

()

(i)

()

()

()

.212

() ()

() :

()

()

--	--	--	--	--

.۲۱۶

)						
		(
			-	-	-			
			-	-	-			

.۲۱۷

)
(.

						()
			-	-	()	
				-		
		-	-			

				-	-		
				-	-		
		-	-	-	-		
		-	-	-	-		
		-	-	-	-		
	-	-		-	-		
				-	-		
		-	-	-	-	()	
		-	-	-	-		
	-	-		-	-		
		-	-	-	-		
		-		-	-	()	
	-		-	-	-		

.۲۱۸

.()

.۲۱۹

.()
.()

.۲۲۰

.۲۲۱

)

(

.()

.۲۲۲

)

.(

)

.(

.۲۲۳

-)

.۲۲۴

(

:

.۲۲۵

()

()

)							(
		-		-	-	-	-	-						
		-		-	-	-	-	-						
		-		-	-	-	-	-						
				-	-									

.۲۲۶

%

)

(

.٢٢٧

.٢٢٨

(

)

.٢٢٩

(

)

.٢٣٠

)

(

%

^{٥١} وقد أشارت السلطات، وخاصة مؤسسة النقد العربي السعودي، إلى أن إرسال نسخة من تقرير المعاملات المشبوهة للمشرفين بخدم الهدف من الإحصائيات التي يتم القيام بها. وعلى الرغم من ذلك، يكفي أن تقوم وحدة التحريات المالية بالمملكة بالاحتفاظ بإحصائيات عن تقارير المعاملات المشبوهة، وليس أي هيئة من الهيئات الرقابية الأخرى. وبالإضافة إلى ذلك، أقرت السلطات بأن وجود نسخة من التقرير عن المعاملة المشبوهة لدى المراقبين يتيح لهم تقييم مدى الالتزام بقانون مكافحة غسل الأموال. ومع ذلك، يعتقد فريق التقييم أنه يكفي أن تقوم السلطات الرقابية بمراجعة سجلات المؤسسة المالية سواء ورد تقرير عن معاملة مشبوهة أم لا. ولهذه الأسباب، لم يقتنع فريق التقييم بوجهات نظر السلطات.

٢٣١.

(. . .)

٢٣٢.

()

٢٣٣.

()

()

()

٢٣٤.

()

^{٥٢} يمكن الدخول على الموقع من خلال: <http://sa.gov.moi>

٢٣٥

٢٣٦

)

.(

()

٢٣٧

)

)

() ()

() :

.(

()

() ()

() (

()

() ()

()

.()

٢٣٨

٢٣٩

/

.()

.()

)

.(

^{٥٣} انضمت وحدة التحريات بمجموعة في الاجتماع السنوي السابع عشر بالدوحة الذي استمر من ٢٤ وحتى ٢٨ مايو ٢٠٠٩. تم توقيع وثيقة الانضمام يوم الخميس ١٨ مايو في عام ٢٠٠٩. وقد كان ذلك خارج الإطار الزمني لهذا التقييم، ومع ذلك يجدر الإشارة إلى أن هذه العضوية ليست من المتطلبات الواردة بموجب توصيات مجموعة العمل المالي على أية حال.

٢٤٠

٢٤١

()

()

٢٤٢

()

٢٤٣

()

٢٤٤

)					
(
				-	
				-	

^{٥٤} المرسوم الملكي رقم م/٤٣ بتاريخ ١٣٩٣/٨/٢٨ (المادة ٧)، المرسوم الملكي رقم م/٩ بتاريخ ١٣٩٧/٣/٢٤ (المادة ٦٠) والمرسوم الملكي رقم م/٤٩ بتاريخ ١٣٩٧/٧/١٠ (المادة ١٢.١).

			-	-	

٢٤٥

٢٤٦

٢٤٧

()

()

٢٤٨

٢٤٩

--

.200

()
)

()

.201

.(

.202

()

.203

/

.204

.200

.207

--

-		
	• • •	

- () -

--

()

٢٥٧

٢٥٨

°° المواد ١٤ و ٢٤ و ٢٦ من نظام مكافحة غسل الأموال.

٢٥٩

) ()
.(

٢٦٠

) (")
.()
() :
()

() () () ,
.()

٢٦١

()

()) ٢٦٢

) (

.()

٢٦٣

^{٥٦} مرسوم ملكي رقم (٥٦/م) بتاريخ ١٤٠٩/١٠/٢٤ هجرية.

٢٦٧

(AIO)

٢٦٨

٥٩

٢٦٩

^{٥٧} القرار الوزاري رقم (٨/٢١١١) بتاريخ ١٤٠٠/١٢/١ هجرية
^{٥٨} برقية رقم -/٤٨٧٩/٣- بتاريخ ١٤٢٧/٦/١، والقرار رقم ١٢٥٥٤ بتاريخ ١٤٢٧/٦/٦ من مدير مكتب التحريات.
^{٥٩} قرار ملكي، وزير الداخلية رقم ٧١١٧ في ١٣-٩-١٤٢٨ هجرية وفقاً للقانون الأول رقم (٥٦٦٤) في ٢٣-٦-١٤٢٨ هجرية

()

.۲۷۰

.()

)
(

)
()

(

.۲۷۱

)

.(

.()

.۲۷۲

()

.۲۷۳

280

--

286

)

(

--

-		
	•	
	•	
	•	

()

-

--

.2007

.٢٨٧

.()

.٢٨٨

()

.()

/

.٢٨٩

.٢٩٠

.٢٩١

.٢٩٢

^{٦١} في السابق، كان لدى السعودية نظام إقرار مراقبة العملة بحد يبلغ ١٠٠٠٠٠٠ ريال سعودي.

^{٦٢} بينما تشير المواد ١-١٤ و ١٢-١٤ من نظام مكافحة غسل الأموال إلى النقد والأدوات لحاملها القابلة للتداول والمعادن النفيسة، تشير المادة ١٤ من نفس النظام إلى النقد والمعادن النفيسة فقط. ولا يمثل ذلك ثغرة قانونية، لأن المادة ١(٢) من نظام مكافحة غسل الأموال تعرّف الوثائق والعقود القانونية التي تثبت ملكية الأصول أو أي حق يتعلق بها على أنه نقد. علاوةً على ذلك، تعرّف المادة ١-١-١ من نظام مكافحة غسل الأموال والأوراق المالية القابلة للتداول لحاملها على أنها مظهرّة بدون قيود، لمصلحة شخص غير معروف أو مستفيد، مثل الشيكات السياحية والشيكات والسندات الإذنية وأوامر الدفع.

.۲۹۳

)

.۲۹۴

(

.۲۹۵

/

.۲۹۶

.۲۹۷

/

.(

)

/

()

()

()

۳.۲

۳.۳

/

/

- -

۳.۴

()

)

-

. ۳۰۵

.(

(UNSCR)

.(

)

. ۳۰۶

. ۳۰۷

()

. ۳۰۸

()

.309

()

.310

()

()

()

.311

/

()

" "

/

() /

() /

" "

() ()

()

	.	.			
.	.	.			
		.	.		
		.			

() (" ") " " ۳۱۲
 () ()

- -

۳۱۳

314

315

()

()

316

317

--

/	• • • •		

-

-

()

()

()

()

318

)

()

"

(

"

"

"

٣١٩

:

٣٢٠

)

(⁶⁵)

.()

٣٢١

(" ")

٣٢٢

”

٣٢٣

”

” ”

^{٦٥} قواعد البنوك وشركات الصرافة

^{٦٦} يشير قطاع الاستثمار إلى قطاع الأوراق المالية.

^{٦٧} يشير مصطلح الأشخاص المرخص لهم إلى أي كيان تُصدر له هيئة السوق المالية ترخيصاً (غالباً، كيانات قطاع الأوراق المالية).

	-			
	-			

- ۳۲۴

۳۲۵

()

۳۲۶

۳۲۷

-

۳۲۸

- -)

(

.

. ٣٢٩

- -

()

-

- -

. ٣٣٠

) (/ / / () (: ()

. ٣٣١

() .

. ٣٣٢

"

()

^{٦٨} يعتبر مواطنو مجلس التعاون الخليجي، من غير السعوديين، أجانبا إلا إنهم يتمتعون ببعض الامتيازات التي لا تُقدم للمواطنين من خارج بلدان مجلس التعاون الخليجي.

()

. ۲۳۳

. ۲۳۴

.(...)

. ۲۳۵

. ۲۳۶

. ۲۳۷

/

/

(/ ())

()

. ۲۳۸

" "

.۳۳۹

.۳۴۰

.۳۴۱

.۳۴۲

.۳۴۳

.۳۴۴

(- -)

()

" " ٣٥٠

"

."()

" " - - ٣٥١

"

:

٣٥٢

)

.(

-

٣٥٣

"

"

"

٣٥٤

"

--

.300

--

.306

.()

" "

.307

:

.308

.309

.37.

	"		. ۳۶۱
	"		. ۳۶۲
/			
	"		. ۳۶۳
	"		
(RBME)	--		. ۳۶۴
		%	
		() -	. ۳۶۵
		() -	
		()	. ۳۶۶
			. ۳۶۷
			. ۳۶۸
	"	"	
	"	"	
	"	"	
	"	"	

)
 .() ()
 . ۳۶۹
 " - -
 " " " ...
 () - - " .
 .
 .
 . ۳۷۰
 .
 (RAP) ()
 () , ۳۷۱
 . - ۳۷۲
 .
 . ۳۷۳
 .
 . ۳۷۴
 " - / .
 : "

--

. 370

. 376

()

()

. 377

(IFC)

(-)

()

. 378

. 379

:

.

.

-

. ۳۸۰

() - -
"

"

"

"

. ۳۸۱

(PEPs)

-

. ۳۸۲

.(- -)

- -

"

"

()

. ۳۸۳

()

384

"

"

(-)

385

:

386

)

(/

387

--

)

"

.(/

388

.(/)

/

389

390

391

() - -

() - -

392

()

393

. ۳۹۴

:

. ۳۹۵

.

. ۳۹۶



() - -

. ۳۹۷

/

. ۳۹۸

. ۳۹۹

. ۴۰۰

٤٠١

:

٤٠٢

/

-

٤٠٣

٤٠٤

:

٤٠٥

)

"

"

.(

٤٠٦

() - -

^{٦٩} العملاء الموجودون في تاريخ بدء سريان المتطلبات الوطنية.

()

--

٤٠٧

" "

-

٤٠٨

-

٤٠٩

()

٤١٠

٤١١

٤١٢

٤١٣

()

٤١٤

٤١٥

٤١٦

"

" "

() -

. ٤١٧

()

. ٤١٨

. ٤١٩

() 64 - 3 4-5-4)

. ٤٢٠

() - -

. ٤٢١

()

()

. ٤٢٢

)

(() -

(PEP)

٤٢٣

()

() - - ٤٢٤

" " () - - _____

"

" () ٤٢٥

" " " "

) ()

(

() ٤٢٦

() ٤٢٧

() ٤٢٨

٤٢٨

/

)

(

() - -
()

()

(RAP)

. ۴۲۹

() -

. ۴۳۰

. ۴۳۱

. ۴۳۲

()

"

"

- -

. ۴۳۳

()

333
--
()

330

336
--

337
--

338

339

)

(

	٤٤٠
	٤٤١
()	٤٤٢
	٤٤٣
	٤٤٤
(PTA)	٤٤٥
	٤٤٦
) " / (
.(") " (
.(") "	

^{٧٠} على سبيل المثال، تلك التي تم إنشاؤها لمعاملات الأوراق المالية أو تحويل الأموال سواءً لمؤسسة مالية خارجية كمقر رئيسي أو لعملائها.

()
()

()

()

() - ٤٤٧

- - , ٤٤٨

(RAP)

, ٤٤٩

, ٤٥٠

٤٥١

(, ,)

/ /

٤٥٢

/

() - ٤٥٣

() - - ٤٥٤

٥٥٥

() ٤٥٦

(-) ٤٥٧

(-)

(-)

()

()

)

(

-
-
-
-
-
-
-

•

•

•

•

()

•

•

()

•

--

()	•	
	•	

<p>.)</p> <p>.(</p> <p>/</p> <p>()</p>	<ul style="list-style-type: none"> • • • • 	
<p>" "</p>	<ul style="list-style-type: none"> • • • • 	

<ul style="list-style-type: none"> • • 		
<ul style="list-style-type: none"> • 		
<ul style="list-style-type: none"> • 		

()

-

--

"

--

٤٥٩

-

"

"

-

"

"

()

. ٤٦٠

. ٤٦١

()

. ٤٦٢

(

)

"

()

"

"

--

. ٤٦٣

()

. ٤٦٤

. ٤٦٥

()

.۴۶۶

--

.۴۶۷

.۴۶۸

()

.۴۶۹

.۴۷۰

)

.)

--

.۴۷۱

() ----

(GCC)

() - ()

(

)

(...

()

. ٤٧٢

()

()

. ٤٧٣

. ٤٧٤

(

)

()

--

. ٤٧٥

--

•

•

--

)	(•	
	(•	
	(•	

()

-

--

٤٧٦

()

)

(

)

.)

٤٧٧.

)

(

)

(

)

٤٧٨.

(

"

"

٤٧٩.

-

"

"

"

." (- -)

٤٨٠.

(

)

^{٧١} تعميم مؤسسة النقد العربي السعودي رقم م أ ت/٩٧ في ١٣/٤/١٤٢٤ هجرية

--

. ٤٨١

--

	•		
	•		

()

-

--

()

. ٤٨٢

. ٤٨٣

383

385

386

387

388

389

390

(

)

(

)

:

%		
%		
%		

%		
%		
%		

)

(

%		
%		
%		

()

..
"

.(

)

()

)

:(

•
•

.ε93

.() // //

()

-- .ε9ε

2002 14 (/ /5082)

":

."

.ε9ε

()
/

-- .ε9ε

."

" ." /

: ,

()
()

() - - . ٤٩٧

. ٤٩٨

. ٤٩٩

. ٥٠٠

() - - . ٥٠١

. ٥٠٢

() - - . ٥٠٣

. 0.2

() - -
() - -

. 0.0

() - -

. 0.6

) "

.(

. 0.7

() . . .

. 0.8

. 0.9

.()
)
(

.۵۱۰

.۵۱۱

.۵۱۲

.۵۱۳

--

•

--

<p> : () </p>	<p> ● ● ● </p>	
-------------------------------------------------	--------------------------------------------------------------	--

()

-

--

"

316

.()"

"
 .()"

510

()

" "

516

()

.۵۱۷

()

.۵۱۸

()

.۵۱۹

.۵۲۰

/

()

.021

()

.022

.023

.024

)

(

.025

.026

.027

()

(. .)

.028

" " "

"

.029

()

.030

()

.031

.032

"

"

.033

()

(RIC)

.034

.()
(-)

.()
" " " "

.()
" " " "

^{٧٢} لم تلائم أي من التعاميم المقدمة إفادات مجموعة العمل المالي والتي تدعو إلى الإجراءات المضادة.

(() . . .)

(())

. ۰۳۹

(-)

()

. ۰۴۰

(NCCT)

- -

. ۰۴۱

()

()

)

(.

٥٤٢

(-)

٥٤٣

٥٤٤

٥٤٥

٥٤٦

^{٧٣} لاحظ فريق التقييم أن الكثير من مناصب الإدارة العليا للبنوك يشغلها أفراد لا يتكلمون اللغة العربية ومن ثم فإن وجود إصدار رسمي دقيق لقانون مكافحة غسل الأموال باللغة الإنجليزية يتوافق مع اللغة العربية بعد أمر هاماً.

--

	<ul style="list-style-type: none">•••○○○		
	<ul style="list-style-type: none">•••		

)

-

(

--

(

)

(

)

٥٤٧

٠٤٨

(.)

٠٤٩

.(-)

٠٥٠

٠٥١

٠٥٢

.(

()

)

.(-) (" ")

.003

)

(

()

:

300

.000

()

.007

.007

(-) ()

:

()

.008

()

.009

(- -)

.070

.071

)

(

()

.072

()

.٥٦٣

(-)

.٥٦٤

.٥٦٥

--

.٥٦٦

^{٧٤} وقد أسست البنوك السعودية لجنة مراقبة ذاتية لتراقب عن قرب التهديدات التي يسببها الإرهاب وتحاربها ولكي تتسق كل الجهود لتجميد الأصول الخاصة بالأشخاص والكيانات المحددة. وتتألف اللجنة من كبار الموظفين من البنوك المسئولين عن السيطرة على المخاطر والمراقبة ووحدات غسل الأموال والنواحي القانونية والعمليات وتعمل في وجود مسئول مؤسس النقد العربي السعودي. المصدر: سفارة المملكة العربية السعودية على موقع واشنطن؛ (<http://www.net.saudiembassy.org/2001/page/statements.aspx>)

()

.067

)

.068

()

(

(.)

--

	<ul style="list-style-type: none"> • • ○ ○ ○ ○ 		

	•	
	•	
	•	
	•	
	•	
	•	
	○	
	○	
	○	
	○	

(&)

-

--

()

.069

"

"

"

"

-

.07.

--

()

.071

.072

()

.073

()

"

--

"

/

()

.074

()

"

"

.075

()

. (-)

/

. 076

--

. 077

. 078

. 079

()

. 080

. (- -)

()

٥٨١

٥٨٢

٥٨٣

:

()

:	:		
			/

:

:

٥٨٤

()	

.()

:

.080

(-)

.086

()

.087

.()

.()

.088

%

" "

()

.089

- .()

.090

.091

.092

--

.093

.094

٥٩٥

- -

	•	
	• •	

()

٩-٣

الوصف والتحليل

١-٩-٣

٥٩٦

"

"

٥٩٧

.098

--

.099

()

--

() () - -

--

()

. 7.0

:

-
-
-
-
-
-

. 7.1

. 7.2

()

. 7.3

()

٦٠٤

() . ()

٦٠٥

()

"

"

/ / /

()

- ()

)"

"

٦٠٦

"

()

() :

)"

٦٠٧

"

/

٦٠٨

() //

^{٧٥} قرار التوصية ٣/٩٢٠ بتاريخ ١٦/٢/١٤٠٢ هجرية (١٩٨١؟؟) بموجب قرار مجلس الوزراء ١٠١٢ وبموجب القرار الملكي ٨/١٠٦٤

7.9

() () // /
:

•

•

•

•

•

•

•

() ()

7.10

(

()

()

()

() :

7.11

()

()

		()		
		+		
	-			
		()		

^{٧٦} تم تعيين موظف إضافي واحد في شهر يونيو عام ٢٠٠٩ حسبما أفادت السلطات بعد الزيارة الميدانية.

	-			

" ()
"

.٦١٢

)
())
()

/

/ /

.(

- .٦١٣

.٦١٤

()
()

.٦١٥

.٦١٦

()
()

.٦١٧

.٦١٨

(-)

.٦١٩

. 620

.() .

" " " " . 621

. 622

()

. 623

.() .

()

. 624

()

()

()

. ٦٢٥

() / /

/

)

.(

.(

) /

.()

. ٦٢٦

/

()

. ٦٢٧

. ٦٢٨

(-)

_____ :

.٦٢٩

.٦٣٠

/

()

.٦٣١

()

/

.٦٣٢

)

(

()

.٦٣٣

(CICL)

.734

.730

:(() -)

: .1

;

: .2

;

: .3

;

: .4

: .5

.736

()

(-) // /

.737

-

()
()

.738

.

.739

" "

.740

()

.741

())
()
(-)

.742

)

.743

(

.()

.()

(-)

		-	-	-	-
-		-	-	-	(KYC)
		-	-		
		-	-	-	()
		-	-	-	()

()

:

.644

.()

/

()

.()

()

.640

.701

.702

.703

:(CICL)

.704

.()

.700

// /
// /
/

.707

(APR)

(RAP)

.707

()

.708

. ٦٥٩

() ()
() ()

()

() ()

()

. ٦٦٠

) ()

. ٦٦١

() ()

. (_____)

. ٦٦٢

. ٦٦٣

. ٦٦٤

-

					-	
-	-	-	-		-	
-	-	-	-	-	-	
-	-	-	-	-	-	
-		-	-		-	
-	-			-	-	
-	-			-	-	
-	-	-	-	-		
		-	-	-	-	
-		-)
						(

/							/
							/

/							
"							
"							
)
							(

.770

.()

			(CMA)
--	--	--	-------

. ٦٦٦

()

-

()

. ٦٦٧

-

) /- /

. ٦٦٨

()

. ٦٦٩

()

(/)

. ٦٧٠

)

()

.(

. ٦٧١

/ () % (//
% ()

.672

.673

(MVT)

/

.674

() : () ()

.675

) (

() 676
()
()

()

(FIs)

()

676

677

678

679

. ٦٨٠

()

. ٦٨١

()

()

. ٦٨٢

. ٦٨٣

(APs)

. ٦٨٤

- - -

•

•

()

•

•

•

•

•

•

•

•

- - -

	•	
()	• • • •	
	•	
	•	

()

-

()

- - -

/

()

780

.(" ")

()

)

" "

.(

(%)

%

%

(MVT)

:

(ATM)

.٦٨٦

.(-)

- -

.٦٨٧

()

- - (/)

- -

(/)

()

.٦٨٨

() -

^{٧٧} قاعدة بيانات الأعمال الاستراتيجية، ٣٠ يناير ٢٠٠٧.

^{٧٨} البوابة ٢٠٠٩ (www.albawaba.com), ٤ يوليو ٢٠٠٩.

^{٧٩} <http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentID=2010022164053>

. 789

)

. 790

(

.."

()

() () :

()

()

. 791

. 792

. 793

())

()

() ()

.٦٩٤

()

.٦٩٥

.٦٩٦

.٦٩٧

.٦٩٨

.٦٩٩

^{٨٠} طبقاً للمذكرة التفسيرية، فإن الوكيل هو أي شخص يقدم خدمات تحويل الأموال أو القيمة تحت توجيهه أو بموجب عقد مع جهة تحويل مسجلة أو مرخصة قانونياً (على سبيل المثال الجهات المرخصة ومقدمو الخدمات وأصحاب الامتياز).

(() ())
.(() ())

- -

- -

()	•	

- -

() -

()

: .Y.1

.(
.Y.1

.Y.2

:

•

()			

γ.6

:

/

-
-
-

γ.7

()

γ.8

-

- - •
 - - •
 :
 - - •

-)
 . : (-

--

.Y.9

. .
 // /
 ()
 .()

"

"

.Y11

:

.Y12

•

•

•

•

•

•

•

.Y13

)

.(

.Y14

:

.Y15

"

"

)

) /

.(

" (()

."

:

.Y16

•

•

•

•

)

.(

(TCSPs)

.Y17

--

.Y18

:

•

•

-

-

-

-

-

-

-
-
-
-
•
-
-
•

--

	○	
	○	
	○	
	○	
	○	
	○	

<p>(TCSPs)</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">○</p> <p style="text-align: right;">●</p>		
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

()

()

-

--

.Y19

" "

.۷۲۰

.۷۲۱

/

/

"

///

.۷۲۲

/

() () /

()

.۷۲۳

.()

/

.۷۲۴

"

-

"

.۷۲۵

.۷۲۶

.۷۲۷

.۷۲۸

200

.۷۲۹

.۷۳۰

()

:

--

.۷۳۱

.۷۳۲

.۷۳۳

)

.۷۳۶

.(
)

(

)

.(

.۷۳۷

.(

)

:

.

.۷۳۸

.

.(-)

.۷۳۹

:

//

.۷۴۰

()

...

//

()/

.۷۴۱

.۷۴۲

.۷۴۳

.۷۴۴

.۷۴۵

.۷۴۶

)

.)

)

.)

۷۴۷

(() / / / /)

() / / /

۷۴۸

/ / /

۷۴۹

۷۵۰

۷۵۱

- -

- -

()

:

•

•

•

•

.702

.()

.()

.703

.704

.700

--

•

•

•

•

(-)

--

•		
•		
•		
•		

()

-

-

--

.Y06

].

.[

.Y07

.(ATM))

(BTD)

:

•

(SPAN)

•

)

)

(

.(

(SADAD) " "

•

" "

(EBPP)

٧٥٨

--

•

--

)

-

-

-

(

--

(" ")

.Y09

("CRL")

:

.Y60

.Y61

" " " "

()

.Y62

.Y63

.Y64

/

.Y65

.Y66

.Y67

.Y68

.Y69

.Y70

...

•

•

--

-
()

--

.۷۷۱

.۷۷۲

) ()

(

() () () .۷۷۳

.۷۷۴

()

() /
()

٧٧٥

()

٧٧٦

()

--

()

-

--

٧٧٧

^{٨١} مرسوم ملكي رقم م/٦٤، ١٤ رجب ١٣٩٥ هجرية.

^{٨٢} لوائح الجمعيات والمؤسسات الخيرية (لوائح الجمعيات الخيرية) أصدرت بموجب قرار مجلس الوزراء رقم ١٠٧، بتاريخ ١٤١٠/٦/٢٥ هجرية الموافق (٢٣ يناير ١٩٩٠)

^{٨٣} القواعد التنفيذية للجمعيات الخيرية (القواعد التنفيذية للجمعيات الخيرية) أصدرها وزير الشؤون الاجتماعية بموجب القرار رقم ٧٦٠، بتاريخ ١٤١٢/١/٣٠ هجرية الموافق (١١ أغسطس ١٩٩١)

2003

() / / /

()

;

)

.(

()

:

.()

^{٨٤} خطاب مجلس الأمن التابع للأمم المتحدة س/٥٨٣/٢٠٠٣ بتاريخ ٢٩ مايو ٢٠٠٣ من رئيس لجنة مجلس الأمن طبقاً للقرار ١٣٧٣ (عام ٢٠٠١) الخاص بمكافحة الإرهاب، والموجه إلى رئيس مجلس الأمن.

^{٨٥} أشارت السلطات إلى أن الأفراد ممنوعون أيضاً من التبرع بأموالهم الخاصة إلى الخارج. ولم يتمكن فريق التقييم من تأكيد ذلك في القانون. يشكك فريق التقييم أيضاً في قدرة السلطات على تطبيق مثل هذا التدبير (نظراً للعدد الكبير من التحويلات البرقية وتحويل الأموال والقدرة القانونية الممنوحة للمواطنين بأخذ النقدية إلى خارج البلاد وتمويل مؤسسة خيرية من الخارج). غير أنه بالنظر لحقيقة أن التوصية الخاصة رقم ٨ لم تكن موجهة بنية أن تشمل الأفراد أو الدول، فقد قرر فريق التقييم ألا يتخذ قراراً نهائياً بشأن السماح أو عدم السماح للأفراد بالتبرع للخارج من أموالهم الخاصة.

٧٨٢

()
()

():

()

()

()
()
()

()

()

٧٨٣

()

()

()

()

2003

٧٨٤

//)

)

(

٧٨٥

^{٨٦} تعميم وزارة الشؤون الاجتماعية رقم ٤١٧٣٥ بتاريخ ١٤٢٤/٩/٢٢ هجرية

٧٨٦.

() () ():

/

٧٨٧.

() .

٧٨٨.

()

٧٨٩.

)
() () : () () () () ()

^{٨٧} تعميم حول الإبلاغ عن غسل الأموال/تمويل الإرهاب رقم (١٨٨/٩/٤)، بتاريخ ١٤٢٦/٨/١٥ هجرية

.Y90

.()

.Y91

.()

; () :

.Y92 ()

.(/ -)

.Y93

) / (

.Y9E

.()

.Y9O

).

.(

.Y9T

()

.()

.Y9Y

.۷۹۸

--

.۷۹۹

--

	•		
;			
.()	•		

-

()

-

--

()

٨٠٠
() : () ()
(PCMLA)

() :
()

٨٠١

)
(

٨٠٢

()
()

^{٨٨} قرار مجلس الوزراء رقم (٥) بتاريخ ١٤٢٠/١/١٧ هجرية
^{٨٩} مرسوم ملكي س/٢٠١٦٧، بتاريخ ١٤٢٢/١٠/١٠ هجرية الموافق (٢٥ ديسمبر عام ٢٠٠١).

. ۸۰۳

()

. ۸۰۴

()

. ۸۰۵

()

() -)
(

. ۸۰۶

() -)

)

(

- -

. ۸۰۷

--

()

-

--

.٨٠٨

.()

() ()
.()

.٨٠٩

)

.(

()

.٨١٠

()
)

() (

^{٩٠} قرار رقم ١٦٨ بتاريخ ١١/٨/١٤١٩ هجرية.

^{٩١} تتطلب التوصية ٣٥ تطبيق المواد ٧-٥، و١٠-١٦، و١٨-٢٠، و٢٤-٢٧، و٢٩-٣١ و٣٤.

^{٩٢} وتتطلب التوصية ٣٥ والتوصية الخاصة رقم ١ ضرورة تطبيق المواد من ٢ إلى ١٨ في اتفاقية مكافحة تمويل الإرهاب.

()

.٨١١

()

.٨١٢

- ()

()⁹³

(GCC)

()

.٨١٣

()⁹⁴

.⁹⁶

()⁹⁵

.
.٨١٤

11/8/1419

168

.٨١٥

(-)

⁹³ مرسوم ملكي رقم (٥٢/م) بتاريخ ٥ أكتوبر ٢٠٠٥ (١٤٢٦/٩/٢ هجرية).
⁹⁴ مرسوم ملكي رقم (٣١/م) بتاريخ ٣ نوفمبر ٢٠٠٠ (١٤٢١/٨/٥ هجرية).
⁹⁵ قرار مجلس الوزراء رقم (١٢٩) بتاريخ ٢٩ مارس ١٩٩٤ (١٤١٤/١٠/١٦ هجرية).
⁹⁶ مرسوم ملكي رقم (١٦/م) بتاريخ ٢ أكتوبر ١٩٩٨ (١٤١٩/٦/١٠ هجرية).

--

	•	
	•	
	•	
	•	

()

-

--

.۸۱۶

()

.()

.۸۱۷

.()

-)

.(

.(-)

():

()

.۸۱۸

()

()

()

.()

.()

.٨١٩

.٨٢٠

()

.٨٢١

)

.(

.٨٢٢

(24 23

)

(-)

()

^{٦٧} أمر ملكي رقم (١١٩٤/ب/٤) بتاريخ ١٤١٨/١/٢٣ هجرية والمواد ٢٣ و ٢٤ من قانون مكافحة غسل الأموال

.۸۲۳

.۸۲۴

)

(

)

(

.۸۲۵

.۸۲۶

()

.۸۲۷

.۸۲۸

()

.۸۲۹

%)

((GDP)

.۸۳۰

()

)

()
(

.۸۳۱

(..)

٨٣٢

٨٣٣

()
()

٨٣٤

^{٩٨} والأمانة على ذلك كما يلي: نصت المادة (٣٨) من اتفاقية الرياض العربية للتعاون القضائي على أن "يتعهد كل طرف متعاقد بتسليم المطلوبين الذين يعثر عليهم في منطقتهم والمسئولين عن ارتكاب جريمة معينة من قبل السلطة المختصة أو المدانين بالقيام بفعل هذا من قبل هيئة قضائية لأي من الأطراف المتعاقدة الأخرى، بموجب القواعد والشروط المدونة في هذا الجزء". ونصت المادة (٥) من الاتفاقية العربية لمنع الإرهاب على أن "تتعهد كل دولة من الدول الأطراف بتسليم المتهمين أو الأشخاص المدانين بجرائم إرهاب، المطلوب تسليمهم من قبل أي من هذه الدول وفقاً للقواعد والشروط المنصوص عليها في هذه الاتفاقية". تنص المادة (٦) من الاتفاقية العربية لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية على أن "تخطر كل دولة عضو وبدون تأخير الدولة الأخرى في حالة قيام أحد مواطني الدولة الأخيرة بارتكاب إحدى الجرائم المنصوص عليها في المادة (٢) الفقرة (١) من هذه الاتفاقية وتقوم بإخطار الجمعية العمومية". ونصت اتفاقية دول مجلس التعاون الخليجي لمكافحة الإرهاب فيما يتعلق بتسليم المطلوبين على أن "تتعهد كل دولة من الدول الأطراف بتسليم الأشخاص المتهمين أو المدانين بجرائم إرهاب، والمطلوب تسليمهم من قبل أي من هذه الدول وفقاً للقواعد والشروط المنصوص عليها في هذه الاتفاقية".

.(%)

.۱۳۵

) () :

()

(

) () (SCIPP)

.(

()

.۱۳۶

)

(

)

.۱۳۷

() -

.۱۳۸

.()

.۱۳۹

"

"

()

٨٤٠.

()

()

٨٤١.

" "

()

() ٨٤٢.

() .

()

٨٤٣.

" "

() -

.)

()

^{٩٩} توجد ترتيبات لتنسيق إجراءات ضبط المتحصلات ومصادرتها مع الدول الأخرى كما هو مقرر في الاتفاقيات الثنائية. والأمثلة على ذلك كما يلي: المادة ١ و ٨/٢ من اتفاقية التعاون مع جمهورية السودان، والمواد ١ و ٥/٢ من اتفاقية التعاون مع السنغال، والمواد ١ و ٨/٢ من اتفاقية التعاون مع إيطاليا، وأخيراً المواد ١/١ و ٣/٧ ج من اتفاقية التعاون مع المملكة المتحدة.

٨٤٤

()

)

.)

-

()

٨٤٥

--

٨٤٦

()

24 23

٨٤٧

)

٨٤٨

(

-

--

	• • • •		

	•		
	• • • •		
	•		

() -

--

٨٤٩

" ()

^{١٠٠} الاسم الرسمي هو اتفاقية الجامعة العربية لتسليم المطلوبين (١٩٥٤)
^{١٠١} مرسوم ملكي رقم (١٤/م) بتاريخ ١٢/٨/١٤٢٠ هجرية.
^{١٠٢} مرسوم ملكي رقم (١٦/م) بتاريخ ١٠/٦/١٤١٩ هجرية.
^{١٠٣} مرسوم ملكي رقم (٣/م) بتاريخ ٢٦/١٠/١٤١٥ هجرية

()

.()

.100

)

(

()

()

.101

-

-

.102

)

.(

.103

)

.(

.104

٨٥٥

٨٥٦

()
.()

(

--

٨٥٧

--

	•	
	•	
	•	
	•	

()

-

- -

.٨٥٨

()

()

.٨٥٩

()

.٨٦٠

)

.(

.()

()						
	104					
()	()	()	()	()		

.٨٦١

()

)

.(

^{١٠٤} نتيجة للزيارة الميدانية في مارس ٢٠٠٩، سوف تستعيد قاعدة الشهرين الطبيعية لإدخال المعلومات في التقييم أية إحصائيات من بعد ١١ مايو ٢٠٠٩. وعلى الرغم من ذلك، تم تضمين كل الإحصائيات لعام ٢٠٠٩ في المعلومات لتوضيح آخر التوجهات.

.٨٦٢

.٨٦٣

) () -
. (

.٨٦٤

) () -
. (

.٨٦٥

)
. (

.٨٦٦

. ()

)
. (

.٨٦٧

^{١٠٥} بعد منح عضوية إيغمونت لوحدة التحريات المالية السعودية (خارج الفترة الزمنية لهذا التقييم)، أرسلت وحدة التحريات المالية السعودية خطابات لعدد ٦٠ وحدة تحريات مالية أجنبية مع طلب لمذكرة تفاهم.

() () -)

.(

- - -

.178

)

-

.(

.179

()

)

.180

.(

.181

)

(

)

(

.182

.183

)

.(

		106

٨٧٦

: () : () : ()
 : () () : ()

٨٧٧

٨٧٨

	-	
	-	
	-	

١٠٦ المرجع السابق.
 ١٠٧ المرجع السابق.

	-	
	-	
	-	
	-	
	-	
	-	

(RILO)

.٨٧٩

(WCO)

()

()

()

.٨٨٠

.٨٨١

.٨٨٢

.٨٨٣

()

.()

١٠٨ الأمر الوزاري رقم ٤٥ بتاريخ ١٧/٣/١٤١٨ هجرية.

. ۸۸۴

)
(

. ۸۸۵

()

. ۸۸۶

)
(

. ۸۸۷

/

. ۸۸۸

)
(

•

•

•

(•		
)	(
.()		
	--		
		.٨٨٩	
	.()	
			.٨٩٠
			.٨٩١
			.٨٩٢

^{١٠٩} وعلى الرغم من ذلك، مع انضمام وحدة التحريات المالية السعودية مؤخرًا إلى مجموعة إيغمنت، تتحسن الفعالية بالفعل وبشكل سريع. ولكن هذا يقع خارج نطاق الإطار الزمني لهذا التقييم.

()	•	
()	•	
	•	
	•	

)	•	
(•	
:	•	
	•	
	•	
	•	

()	• • •		
-----	-------------	--	--

:
:
:
:
:

()

)
." "

/	•	-
-	•	-
)	•	
(•	
()	•	-
()	•	-
()	•	-
()	○	
()	○	
:	•	
()	○	
()	○	
	•	-

١١٠ يكون إدراج هذه العوامل مطلوباً فقط عندما تكون درجة الالتزام أقل من "ملتزمة".

<p> ) .(. : / . () </p>		
<p> . " " </p>		-

		-
		-
<p>_____</p> <p>) (</p>		-
		-
		-
		-
		-

<p>(TCSPs)</p>	<ul style="list-style-type: none"> • • • • • • • • • • • • • • 	
		-

<ul style="list-style-type: none"> • ○ ○ ○ ○ 		
<ul style="list-style-type: none"> • 		-
<ul style="list-style-type: none"> • 		-
<ul style="list-style-type: none"> • • • • • • • • • • 		-
<ul style="list-style-type: none"> • 		-
<ul style="list-style-type: none"> • 		-
<ul style="list-style-type: none"> • 		-
<ul style="list-style-type: none"> • 		-

	• • •	-
	• •	-
()	• • • •	-
	• •	- -
	• • • • •	-

	•	-

	•		
	•		
	•		-
	•		-
	•		-
) (•		-
	•		-
	• • • • • • •		-

()	•		
	•		- -
	•		- -

	• •		-
	• • • •		-
	•		-
	• • • •		-
	• • •		-
))) ()	• • •		-

<ul style="list-style-type: none"> • • ○ ○ ○ ○ 		:
<ul style="list-style-type: none"> • 		:
<ul style="list-style-type: none"> • <p>)</p> <p>(</p>		:
<hr style="width: 10%; margin-left: auto; margin-right: 0;"/> <ul style="list-style-type: none"> • • • <p>()</p> <p>()</p>		:
<ul style="list-style-type: none"> • <p>;</p> <p>)</p> <p>.(</p>		:
<ul style="list-style-type: none"> • • 		:

/		
---	--	--

:()

()	
	-
	-
• • •	- ()
• () • •	- ()
• • •	- ()
• •	-) (

	• •	
) .()	• • • •	- ()
	• • • • • •	-) (
		- -
		-
.()	• •	-) (

	<ul style="list-style-type: none"> • • • • •
<p>)</p> <p>(</p>	<ul style="list-style-type: none"> • • • • • • • <p>)</p> <p>(</p> <p>-</p>

	•	
	•	
	•	
	•	-
	•	()
	•	
	•	-
	•	()
	•	-
	•	()
	•	-
	•	()
	•	-
	•	()

	-
	- ()
	-) (
23) (24	-) (
	-) (



Anti Money Laundering ("AML") law

()

//

//

Article 1

Definitions

Terms shall mean the following corresponding meanings:

1. Money- Laundering: any actual or attempted act aimed at concealing or camouflaging the nature of illegally or illegitimately earned property to make it look as proceeds from legal sources.
2. Property: shall mean any kind of assets and property, whether material or immaterial, movable or immovable, and legal documents and instruments which prove the ownership of the assets or any right attached thereto.
3. Proceeds: shall mean any funds generated or earned directly or indirectly from money-laundering offences subject to sanctions hereunder.
4. Instrumentalities: shall mean anything used or was meant to be used in anyway in committing a crime subject to sanctions hereunder.
5. Financial and Non- Financial Institutions: any establishment in the kingdom engaged in any one or more financial, commercial or economic activity such as banks, money-exchangers, investment companies, insurance companies, commercial



companies, establishments, professional firms or any other similar activities set forth in the Implementation Rules.

6. Transaction: shall mean any action involving money, property or cash or in kind proceeds, including but not limited to: Deposits withdrawals, transfer, selling, buying, loaning, safekeeping or the like.
 7. Criminal activities: shall mean any activity sanctioned by Shariaa or law including the financing of terrorism, terrorist acts and terrorist organizations.
 8. Attachment: shall mean the provisional ban on transferring, exchanging, disposing with or moving funds and proceeds or attaching same pursuant to an order by a court or a competent authority.
 9. Confiscation: shall mean the expropriation of funds, proceeds or instrumentalities used in the crime pursuant to a ruling by a competent court.
 10. Supervisory Authorities: shall mean government authorities that have the power to license, supervise and/ or oversee Financial and Non- Financial Institutions.
 11. Competent Authorities: shall mean all government authorities that are authorized to combat money laundering each within its own jurisdiction.
-



Article 2

Anyone who commits any of the following actions shall be deemed a perpetrator of a money-laundering crime:

- a. Conducting any transaction involving property or proceeds with the know that such property or proceeds came as a result of a criminal activity or from an illegal or illegitimate source.
- b. Carrying, earning, using, keeping, receiving or transferring any property or proceeds with the know that such property or proceeds came as a result of a criminal activity or from an illegal or illegitimate source.
- c. Concealing or camouflaging the nature, movement, source, ownership or place and method of disposition with property or proceeds with the know that such property or proceeds came as a result of a criminal activity or from an illegal or illegitimate source.
- d. Financing terrorism, terrorist acts and terrorist organizations.
- e. Participating by way of agreement, assistance, incitement, advice, counsel, facilitation, collaboration, covering or attempt in committing a crime listed hereunder.

Article 3

Chairmen or members of the Board of Directors of Financial and Non- Financial Institutions, their owners, employees, authorized representatives, auditors or anyone acting in such capacity shall he deemed a perpetrator of a money- laundering offence if he commits or participates in any of the acts defined in article (2) thereof, with no prejudice to the criminal liability of the Financial and Non-Financial Institutions for such offences if committed in their name or to their account.



Article 4

Financial and Non- Financial Institutions may not carry out any financial, commercial or similar operations under anonymous or fictitious names. They must verify the identity of the client, on the basis of official documents, at the start of dealing with such client or upon concluding commercial transactions therewith in person or in proxy. They must further verify the official documents of juristic person that indicate the name of the entity, its address, name of its owners, managing directors and other data stated in the Implementation Rules.

Article 5

Financial and Non- Financial Institutions must maintain, for at least ten years from the data of concluding the operation or closing of the account, all records and documents that explain the financial, commercial and monetary transactions, whether local or foreign, the files of commercial accounts and correspondence and copies of the IDs.

Article 6

Financial and Non- Financial Institutions must 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.

Article 7

Upon gathering sufficient indications and evidence regarding complex unusual large or suspicious



transactions or operations related to money laundering, terrorist acts and terrorist organizations, Financial and Non- Financial Institutions must take the following measures:

- a. Inform the Financial Intelligence Unit (“FIU”) immediately as provided for in Article (11) of this Regulation.
- b.
- c. Prepare and submit to the FIU a detailed report including all available data and information on the parties involved therein.

()

Article 8

As an exception to the confidentiality provisions that normally apply, Financial and Non-Financial Institutions must provide the judicial or concerned authorities with documents, records and information in accordance with applicable regulations when requested.

Article 9

Financial and Non- Financial Institutions, their employees and other parties subject to these Regulations shall not alert or permit to alert clients or alert other related parties about suspicions regarding their activities.

Article 10

Financial and Non- Financial Institutions must develop programs to combat money- laundering, covering, as a minimum, the following:

- a. Developing and implementing policies, plans, procedures and internal controls, including the appointment of qualified employees at the level of senior management to implement same.
- b. Developing internal accounting and auditing systems to supervise the



availability of basic requirements to combat money- laundering.

- c. Developing ongoing training programs for specialized employees to keep them informed about new technologies in combating money- laundering and to upgrade their activities to identify such operations, their patterns and the method of combating them.

Article 11

A Financial Intelligence Unit shall be formed to combat money- laundering and to be responsible for receiving and analyzing reports and prepare reports on suspicious operations from all Financial and Non- Financial Institutions. The Implementation Rules of these Regulations shall define the location of its head office, its structure, its powers and the method of exercising its duties and connections.

Article 12

Upon confirming the suspicion, the FIU may order Financial and Non- Financial Institutions and direct the concerned authorities to attach properties, proceeds and instrumentalities committed in money- laundering for a period not exceeding 20 days. If further extension is needed, the order must come from the competent court.

Article 13

Under article (8) of these Regulations, information disclosed by Financial and Non- Financial Institutions may be shared with the concerned authorities if such information is connected with a violation of these Regulations. The concerned authorities should observe the confidentiality of such information and disclose it only to the extent it may be necessary for the investigations or judicial actions related to the violation of the provisions hereof.



Article 14

The Implementation Rules shall define the rules and procedures for the amounts of cash and precious metals that are permitted to be carried in or out of kingdom and are subject to declaration.

Article 15

If the confiscation of properties, proceeds or instrumentalities is ordered by court and if the order does not call for the destruction of such items, the concerned authorities may dispose with such items pursuant to applicable regulations. Or could be shared with concerned foreign authorities that are connected with the kingdom through valid agreements or conventions.

Article 16

The perpetrator of a money- laundering offence under article (2) hereof shall be subject to a jail penalty up to ten years and a financial fine up to SR 5,000,000 or to either punishment and the confiscation of the property, proceeds and instrumentalities connected with the crime. If such property and proceeds are combined with property generated from legitimate sources, such property shall be subject to confiscation pro rata with the estimated value of the illegitimate proceeds.

The competent court may relieve the owner, possessor or user of such property or proceeds if he reports to the authorities, before their knowledge, about the confiscated property, the proceeds and the identity of the accomplices without benefiting from the income of such property.



Article 17

The perpetrator of a money- laundering offence shall be subject either to a jail penalty up to less than 15 years and a financial fine up to less than SR 7,000,000 if the offence takes place under the following circumstances:

- a. Involvement in a crime committed by an organized gang with which the perpetrator is affiliated
- b. If violence or arms are used in the crime
- c. If the perpetrator was a public servant and the crime is connected with such position, or if the perpetrator used his influence and powers in the crime
- d. In case minors were lured or exploited
- e. If the offence was committed through a reform, charitable or educational institution or through a social service facility.
- f. If the perpetrator was subject to previous local or foreign sanctions, specifically for similar offences.

Article 18

With no prejudice to other regulations, any chairman or member of board of directors of Financial and Non- Financial Institutions, their owners, managers, employees, authorized representatives or anyone acting in such capacity shall be subject either to a jail penalty up to 2 years or a fine up to SR 500,000 if he violates any of the obligations stated in articles 4,5,6,7,8,9 and 10 hereof.

The penalties apply to anyone who practices the activity without a license

Article 19

Financial and Non- Financial Institutions that



violate the provisions of articles 2-3 hereof may, by a court ruling based on an action by the concerned authorities, be subject to a fine ranging from SR 100,000 up to the value of property involved in the offence.

(-)

Article 20

Anyone violating any provision not stated hereof shall be subject to a jail penalty up to six months and a fine up to SR 100,000 or to either punishment.

Article 21

The proceedings and sanctions provided for herein shall not apply to those acting in good faith.

International Cooperation

Article 22

As an exception to the confidentiality provisions that normally apply, disclosed information by Financial and Non-Financial Institutions could be shared with concerned foreign authorities that are connected with the Kingdom through valid agreements or conventions, or on the basis of reciprocity according to defined legal procedure.

Article 23

The judiciary may, pursuant to a request by a court or concerned authority in a foreign country connected with the kingdom through a valid agreement or convention on the basis of reciprocity, order the tracking of property, proceeds or instrumentalities connected with money-laundering in accordance with Saudi applicable regulations.

The concerned authority, upon a request from a concerned authority in a foreign country connected



with the kingdom through ratified agreements or on the basis of reciprocity may order the tracking of property, proceeds and instrumentalities connected with money- laundering in accordance with Saudi applicable regulations.

Article 24

Any court ruling, providing for the confiscation of property, proceeds or instrumentalities connected with money laundering, issued by a competent court in a foreign country connected with the kingdom through a valid agreement or convention, or on the basis of reciprocity, may be recognized by

the kingdom if the property, proceeds or instrumentalities covered by the court ruling are subject to confiscation under Saudi applicable law.

General Provisions

Article 25

Chairmen and members of board of directors of Financial and Non- Financial Institutions, their owners, employees, servants or authorized representatives, shall be relieved from criminal, civil or administrative liability that may be caused by performing the duties provided for herein or by violating the provisions of confidentiality, unless it is established that they acted in bad faith to hurt the involved person.

Article 26

Public courts shall have jurisdiction over all offences provided for herein.

Article 27

The General Prosecution and Investigation



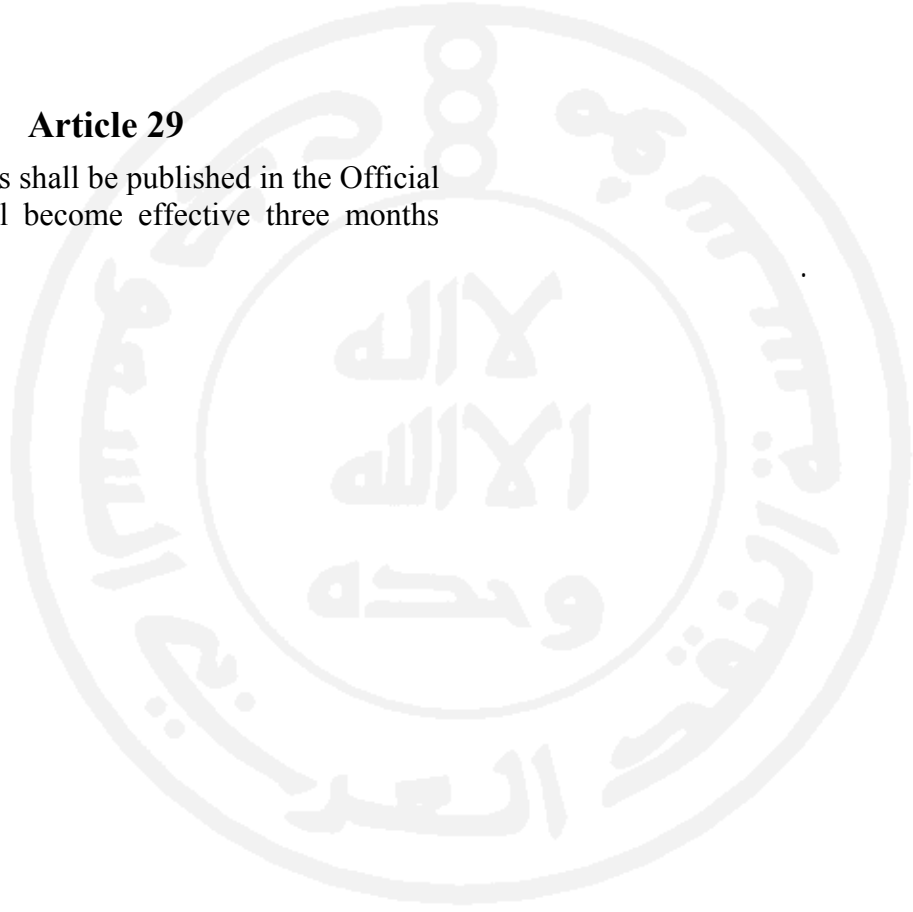
Authority shall investigate and prosecute crimes provided for in this Regulation before General Courts.

Article 28

The Ministry of Interior, in agreement with the Minister of Finance and National Economy, shall issue the Implementation Rules for these Regulations within ninety (90) days from the date of its promulgation.

Article 29

These Regulations shall be published in the Official Gazette and shall become effective three months thereafter.





الرقم /٤/٥١

التاريخ

التوايح

اللائحة التنفيذية لنظام مكافحة غسل الأموال

المادة الأولى:

يقصد بالألفاظ والعبارات الآتية أينما وردت المعاني الموضحة أمام كل منها ما لم يقتضي السياق خلاف ذلك :

١. غسل الأموال: 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.
٢. الأموال: الأصول أو الممتلكات أيا كان نوعها مادية كانت أو معنوية، منقولة أو ثابتة، والمستندات القانونية أو الصكوك التي تثبت تملك الأصول أو أي حق متعلق بها.
٣. المتحصلات: أي مال مستمد أو حصل عليه - بطريق مباشر أو غير مباشر - من ارتكاب جريمة من الجرائم المعاقب عليها وفقاً لأحكام هذا النظام.
٤. وسائط: كل ما استخدم أو أعد للاستخدام بأي شكل في ارتكاب جريمة من الجرائم المعاقب عليها وفقاً لأحكام هذا النظام.
٥. المؤسسات المالية وغير المالية: أي منشأة في المملكة تراول واحداً أو أكثر من الأنشطة المالية أو التجارية أو الاقتصادية، كالبنوك أو محلات الصرافة أو شركات الاستثمار والتأمين أو الشركات التجارية أو المؤسسات الفردية أو الأنشطة المهنية، أو أي نشاط آخر مماثل تحدده اللائحة التنفيذية لهذا النظام.
٦. العملية: كل تصرف في الأموال أو الممتلكات أو المتحصلات النقدية أو العينية. ويشمل على سبيل المثال: الإيداع، السحب، التحويل، البيع، الشراء، الإقراض، المبادلة أو استعمال خزائن الإيداع ونحوها مما تحدده اللائحة التنفيذية لهذا النظام.
٧. النشاط الإجرامي: أي نشاط يشكل جريمة معاقب عليها وفق الشرع أو النظام بما في ذلك تمويل الإرهاب و الأعمال الإرهابية والمنظمات الإرهابية.
٨. الحجز التحفظي: الحظر المؤقت على نقل الأموال والمتحصلات أو تحويلها أو تبديلها أو التصرف فيها أو تحريكها، أو وضع اليد عليها أو حجزها بصورة مؤقتة، استناداً إلى أمر صادر من محكمة أو سلطة مختصة بذلك.





الرقم /٤١٥١/

التاريخ

التوايح

٩. المصادرة: التجريد والحرمان الدائمان من الأموال أو المتحصلات أو الوسائط المستخدمة في الجريمة بناء على حكم قضائي صادر من محكمة مختصة.
١٠. الجهة الرقابية: الجهة الحكومية المختصة بمنح التراخيص للمؤسسات المالية وغير المالية والمختصة كذلك بالرقابة أو الإشراف على تلك المؤسسات.
١١. السلطة المختصة: كل جهاز حكومي منوط به مكافحة عمليات غسل الأموال وفق اختصاصه.

١/١- يعد من الأموال في الفقرة (٢) من هذه المادة الأدوات المالية القابلة للتداول لحاملها أو المظهرة بدون قيود لصالح مستفيد غير معلوم أو التي يصبح حق التملك فيها عند التسليم ومن ذلك المستندات غير المتضمنة أسم المستفيد مثل الشيكات السياحية والشيكات والمستندات الأذنية وأوامر الدفع.

٢/١- يعد من النشاطات الواردة في الفقرة (٥) من هذه المادة الآتي:-

- أ. قبول الودائع ، الاقتراض ، فتح الحسابات .
- ب. التامين ، التأجير التمويلي.
- ج. خدمات تحويل الأموال.
- د. إصدار وإدارة وسائل الدفع (بطاقات الائتمان، الشيكات السياحية، البطاقات المصرفية).
- هـ. إصدار الضمانات والإعتمادات.
- و. الاتجار والتعامل في الأوراق المالية أو الاشتغال بالعملات الأجنبية.
- ز. الوساطة التجارية والمالية.
- ح. معاملات العقارية والخدمات الإستثمارية.
- ط. تعامل في المعادن الثمينة أو الأحجار الكريمة أو السلع النادرة كالقطع الأثرية.
- ي. الاتجار بالسلع ذات القيمة المرتفعة كالسيارات الفخمة وما يعرض في دور المزادات.
- ك. أعمال المحاماة وخدمات الشركات.
- ل. أعمال المحاسبة والمراجعة.

٣/١- يعد من العمليات الواردة في الفقرة (٦) من هذه المادة الآتي:-

- أ- الرهن.
- ب- التحويل بين الحسابات.





الرقم / ٤١٥١٨

التاريخ

التوايح

ج - الهبة .

د - تبادل العملات.

هـ - تداول الأوراق المالية.

و- توثيق العقود والوكالات من قبل كتابات العدل.

٤/١- يقصد بالسلطة المختصة بالحجز التحفظي الواردة في الفقرة (٨) من المادة الأولى هيئة التحقيق والادعاء العام وفقاً لما نصت عليه المادة الثانية عشر من نظام غسل الأموال ومواده التنفيذية.

المادة الثانية:

يعد مرتكباً جريمة غسل الأموال كل من فعل أياً من الأفعال الآتية:

أ. إجراء أي عملية لأموال أو متحصلات، مع علمه بأنها ناتجة من نشاط إجرامي أو مصدر غير مشروع أو غير نظامي.

ب. نقل أموال أو متحصلات، أو اكتسابها أو استخدامها أو حفظها أو تلقيها أو تحويلها، مع علمه بأنها ناتجة من نشاط إجرامي أو مصدر غير مشروع أو غير نظامي.

ج. إخفاء أو تمويه طبيعة الأموال أو المتحصلات، أو مصدرها أو حركتها أو ملكيتها أو مكانها أو طريقة التصرف بها، مع علمه بأنها ناتجة من نشاط إجرامي أو مصدر غير مشروع أو غير نظامي.

د. تمويل الإرهاب والأعمال الإرهابية والمنظمات الإرهابية.

هـ. الاشتراك بطريق الاتفاق أو المساعدة أو التحريض أو تقديم المشورة أو النصح أو التسهيل أو التواطؤ أو التستر أو الشروع في ارتكاب أي فعل من الأفعال المنصوص عليها في هذه المادة.

١/٢- يشمل تمويل الإرهاب والأعمال الإرهابية والمنظمات الإرهابية الأموال المتأتية من المصادر المشروعة.

٢/٢- يستدل على وجود العلم من الظروف والملابسات الموضوعية والواقعية ليكون عنصراً من عناصر القصد الجنائي المكون لجريمة من الجرائم المنصوص عليها في هذه المادة.

٣/٢- من أمثلة النشاط الإجرامي أو المصدر غير المشروع أو غير النظامي التي يعتبر الاشتغال بالأموال الناتجة عنها من عمليات غسل الأموال ما يلي:-





الرقم /٤٠١

التاريخ

التوايح

- أ. الجرائم المنصوص عليها في المادة الأولى من اللائحة التنفيذية لاتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية لعام ١٩٨٨م المصادق عليها بقرار مجلس الوزراء رقم (١٦٨) وتاريخ ١١/٨/١٤١٩هـ .
- ب. الجرائم المنظمة الواردة في اتفاقية الأمم المتحدة لمكافحة الجرائم المنظمة عبر الوطنية (اتفاقية باليرمو) الصادرة في ديسمبر ٢٠٠٠م والمصادق عليها بالمرسوم الملكي رقم (م/٢٠) وتاريخ ٢٤/٣/١٤٢٥هـ .
- ج. الجرائم المنصوص عليها في الفقرة (٥) من المادة الثانية من اتفاقية الأمم المتحدة لقمع تمويل الإرهاب المصادق عليها بالمرسوم الملكي رقم (م/٦٢) وتاريخ ١٨/٧/١٤٢٨هـ .
- د. تهريب المسكرات أو تصنيعها أو المتاجرة بها أو ترويجها.
- هـ. جرائم تزيف وتقليد النقود المنصوص عليها في المرسوم الملكي رقم (١٢) وتاريخ ١٢/٧/١٣٧٩هـ .
- و. جرائم التزوير المنصوص عليها في نظام مكافحة التزوير الصادر بالمرسوم الملكي رقم (١١٤) وتاريخ ٢٦/١١/١٣٨٠هـ والمعدل بالمرسوم الملكي رقم (٥٣) في ٥/١١/١٣٨٢هـ .
- ز. جرائم الرشوة المنصوص عليها في نظام مكافحة الرشوة الصادر بالمرسوم الملكي رقم (٣٦) وتاريخ ٢٩/١٢/١٤١٢هـ .
- ح. تهريب الأسلحة والذخائر أو المتفجرات أو تصنيعها أو الاتجار فيها.
- ط. القوادة أو إعداد أماكن الدعارة أو الاعتقاد على ممارسة الفجور.
- ي. السلب أو السطو المسلح.
- ك. السرقات.
- ل. النصب والاحتيال.
- م. الاختلاس من الأموال العامة التابعة للجهات الحكومية أو التي تساهم بها الدولة، وكذلك الخاصة بالشركات والمؤسسات التجارية ونحوها.
- ن. مزاولة الأعمال المصرفية بطريقة غير نظامية المنصوص عليها في المادة الثانية من نظام مراقبة البنوك الصادر بالمرسوم الملكي رقم (٥) وتاريخ ٢٢/٢/١٣٨٦هـ .





الرقم ٤/٥١١ /

التاريخ

التوايح

- س. ممارسة الوساطة في أعمال الأوراق المالية بدون ترخيص المنصوص عليها في المادة رقم (٣١) والتداول بناء على معلومات داخلية المنصوص عليها في المادة رقم (٥٠) من نظام السوق المالية الصادر بالمرسوم الملكي رقم (م/٣٠) وتاريخ ١٤٢٤/٦/٢هـ.
- ع. ممارسة الوساطة في أعمال التأمين بدون ترخيص المنصوص عليها في المادة رقم (١٨) من نظام مراقبة شركات التأمين التعاوني الصادر بالمرسوم الملكي رقم (م/٣٢) وتاريخ ١٤٢٤/٦/٢هـ.
- ف. الجرائم المتعلقة بالأنشطة التجارية كالغش بالأصناف والأوزان والأسعار وتقليد السلع. والتستتر التجاري المنصوص عليه في المادة الأولى من نظام مكافحة التستتر التجاري الصادر بالمرسوم الملكي رقم (م/٤٩) وتاريخ ١٤٠٩/١٠/١٦هـ.
- ص. التهريب الجمركي الواردة في نظام الجمارك الموحد لدول مجلس التعاون لدول الخليج العربية الصادر بالمرسوم الملكي رقم (م/٤١) وتاريخ ١٤٢٣/١١/٣هـ.
- ق. جرائم التهريب الضريبي .

المادة الثالثة:

يعد مرتكباً جريمة غسل الأموال كل من فعل أيًا من الأفعال الواردة في المادة (الثانية) من هذا النظام أو اشترك فيه ، من رؤساء مجالس إدارات المؤسسات المالية وغير المالية أو أعضائها أو أصحابها أو موظفيها أو ممثليها المفوضين أو مدققي حساباتها أو مستخدميها ممن يتصرفون بمقتضى هذه الصفات ، مع عدم الإخلال بالمسؤولية الجنائية للمؤسسات المالية وغير المالية عن تلك الجريمة إذا ارتكبت باسمها أو لحسابها.

- ١/٣ - تسري أحكام هذا النظام ولائحته التنفيذية على المؤسسات المالية وغير المالية المقامة في المناطق الحرة الموجودة على أرض المملكة.
- ٢/٣ - تسري أحكام هذا النظام ولائحته التنفيذية على المؤسسات المالية وغير المالية في المملكة وفروعها والمؤسسات التابعة لها داخل وخارج المملكة.





الرقم /٤١٥١

التاريخ

التوايح

٣/٣- أن تكون الجريمة قد ارتكبت باسم أو لحساب المؤسسات المالية وغير المالية بهدف تحقيق مصلحة مادية أو معنوية مباشرة أو غير مباشرة.

المادة الرابعة:

على المؤسسات المالية وغير المالية ألا تجري أي تعامل مالي أو تجاري أو غيره باسم مجهول أو وهمي. ويجب التحقق من هوية المتعاملين استناداً إلى وثائق رسمية، وذلك عند بداية التعامل مع هؤلاء العملاء أو عند إجراء صفقات تجارية معهم بصفة مباشرة أو نيابة عنهم وعلى تلك المؤسسات التحقق من الوثائق الرسمية للكيانات ذات الصلة الاعتبارية، التي توضح اسم المنشأة وعنوانها وأسماء المالكين لها والمديرين المفوضين بالتوقيع عنها ونحو ذلك مما تحدده اللائحة التنفيذية لهذا النظام.

١/٤ على المؤسسات المالية وغير المالية وممارسي المهن غير المالية المحددة الالتزام التام بما تصدره الجهات الرقابية كوزارة العدل ووزارة التجارة والصناعة ومؤسسة النقد العربي السعودي وهيئة السوق المالية من تعليمات تتعلق بمبدأ اعرف عميلك والعناية الواجبة على أن تشمل كحد أدنى التالي:

١/٤/١ التحقق من هوية جميع المتعاملين الدائمين أو العرضيين مع المؤسسات المالية وغير المالية بالإطلاع على الوثائق الأصلية سارية المفعول المعتمدة نظاماً لإثبات الشخصية وذلك على النحو التالي:

أ- المواطنون السعوديون:-

• بطاقة الهوية الوطنية أو سجل الأسرة.

• عنوان الشخص ومكان إقامته ومحل عمله.

ب- الوافدون الأفراد:-

• الإقامة أو بطاقة الإقامة الخاصة ذات الخمس سنوات أو جواز السفر أو الهوية الوطنية

لمواطني دول مجلس التعاون لدول الخليج العربية أو البطاقة الدبلوماسية للدبلوماسيين.

• عنوان الشخص ومكان إقامته ومحل عمله.

ج- الأشخاص الاعتباريون:-

▪ الشركات والمؤسسات والمحلات المرخص لها:-

- السجل التجاري الصادر من وزارة التجارة والصناعة.

- الترخيص الصادر من وزارة الشؤون البلدية والقروية للمؤسسات والخدمات والمحلات الخاصة.





الرقم /٤/٥١١

التاريخ

التوايح

- عقد التأسيس إن وجد.
- بطاقة الهوية الوطنية للمواطن السعودي صاحب المنشأة التجارية أو شركة الخدمات المرخص لها للتأكد من أسم التاجر الوارد في السجل التجاري أو التراخيص مطابق لاسمه والنفاصيل الأخرى في بطاقة الهوية الوطنية وسريان مفعولها .
- قائمة بالأشخاص مالكي المنشأة الواردة أسمائهم في عقد التأسيس وتعديلاته أن وجد وصورة من هوية كل منهم.
- قائمة بالأشخاص المفوضين من قبل المالك المؤهلين تشغيل الحسابات حسبما ورد في مستند السجل التجاري أو بموجب وكالة صادرة من كاتب العدل أو توكيل معد داخل البنك وصورة من هوية كل منهم.
- الشركات المقيمة:

- صورة من السجل التجاري الصادر عن وزارة التجارة والصناعة.
- صورة من عقد التأسيس وملاحقه.
- صورة ترخيص مزاولة النشاط.
- صورة من هوية المدير المسئول.
- وكالة صادرة عن كاتب عدل أو تفويض خاص من الشخص " أو الأشخاص " الذي لديه بموجب عقد التأسيس صلاحية تفويض الأفراد بالتوقيع.
- صورة من هوية مالكي المنشأة الواردة أسمائهم في عقد التأسيس وتعديلاته.

- ٢/٤ - تحديد هوية العملاء والمستفيدين الحقيقيين والتحقق من أوضاعهم النظامية لكافة العملاء الطبيعيين الذين تعود إليهم الملكية أو السيطرة النهائية أو الذين يقومون بإجراء العمليات بالنيابة عنهم وذلك قبل فتح الحساب أو بداية التعامل مع أي من المؤسسات المالية وغير المالية.
- ٣/٤ - تحديث بيانات العميل والتحقق منها بصفة دورية أو عند ظهور شكوك بشأن دقة أو كفاية البيانات التي تم الحصول عليها مسبقاً في أي مرحلة من مراحل التعامل مع العميل أو المستفيد الحقيقي أو عند وجود اشتباه في حدوث عملية غسل أموال أو تمويل إرهاب بغض النظر عن حدود مبالغ العملية.





الرقم /٤/٥١

التاريخ

التوايح

٤/٤ - التحقق مما إذا كان العميل يعمل بالنيابة عن شخص آخر، واتخاذ التدابير اللازمة لتحديد هوية هذا الشخص والتحقق منها مع إيلاء اهتمام خاص بالحسابات وعلاقات العمل التي يتم إدارتها بموجب توكيل.

٥/٤ - تعزيز تدابير وإجراءات العناية الواجبة المكثفة تجاه العملاء وعلاقات العمل والعمليات ذات المخاطر العالية.

٦/٤ - لا تقبل التدابير المبسطة لإجراء العناية الواجبة في حالة الاشتباه بعملية غسل أموال أو تمويل إرهاب أو في حال وجود ظروف معينة تتطوي على مخاطر عالية.

٧/٤ - لا يقبل من الوكيل كالمحامي أو المحاسب أو الوسيط ومن في حكمهم التذرع بعدم إفشاء أسرار العملاء عند استيفاء بيانات التحقق من الهوية على النحو المشار إليه أنفاً.

المادة الخامسة:

على المؤسسات المالية وغير المالية الاحتفاظ - لمدة لا تقل عن عشر سنوات من تاريخ انتهاء العملية أو قفل الحساب - بجميع السجلات والمستندات، لإيضاح التعاملات المالية والصفقات التجارية والنقدية سواء كانت محلية أو خارجية، وكذلك الاحتفاظ بملفات الحسابات والمراسلات التجارية وصور وثائق الهويات الشخصية.

١/٥ - تحتفظ المؤسسات المالية وغير المالية بنسخة من إثبات هوية المتعاملين معها، وبكل مستند يتعلق بالمعاملات التي تقوم بها.

٢/٥ - تحتفظ المؤسسات المالية وغير المالية بسجل يشمل كافة تفاصيل التعاملات التي تجريها حتى يتم التأكد من:-

أ- استيفاء متطلبات نظام مكافحة غسل الأموال.

ب- تمكين وحدة التحريات المالية أو جهات التحقيق أو السلطات القضائية من تتبع كل عملية وإعادة تركيبها.

ج- الإجابة خلال المدة المحددة عن أية استفسارات تطلبها وحدة التحريات المالية أو جهات التحقيق أو السلطات القضائية.





الرقم / ٤/٥١

التاريخ

التوايح

٣/٥- عندما يطلب من المؤسسات المالية وغير المالية بمقتضى أحكام هذا النظام الاحتفاظ بالسجلات أو المستندات لمدة تزيد عن المدة النظامية فإنه يتعين عليها الاحتفاظ بها حتى نهاية المدة المحددة في الطلب.

المادة السادسة:

على المؤسسات المالية وغير المالية وضع إجراءات احترازية ورقابة داخلية لكشف أي من الجرائم المبينة في هذا النظام وإحباطها، والالتزام بالتعليمات الصادرة من الجهات الرقابية المختصة في هذا المجال .

١/٦- تضع الجهات الرقابية المختصة التعليمات والقواعد الواجب تطبيقها بشأن مكافحة الجرائم المبينة في هذا النظام واتخاذ الوسائل الكفيلة للتحقق من التزام المؤسسات المالية وغير المالية بالأنظمة والقواعد واللوائح المقررة نظاماً لمكافحة غسل الأموال وتمويل الإرهاب.

٢/٦- تتضمن الإجراءات الاحترازية والرقابة الداخلية التي تضعها المؤسسات المالية وغير المالية لكشف الجرائم المبينة في هذه المادة ما يلي:

أ- وضع ضوابط مكتوبة وفعالة تحول دون استغلال تلك المؤسسات في عمليات غسل الأموال وتمويل الإرهاب وتساعد على كشف العمليات المشبوهة وتحول دون استغلال التطورات المعلوماتية والتقنية في تمرير مثل هذه العمليات، وتنظم آليات التعامل مع أية مخاطر تتعلق بعلاقات العمل أو العمليات التي لا تتم وجهاً لوجه.

ب- أن تكون التعليمات الصادرة من الجهة الرقابية هي الحد الأدنى من التعليمات الواجب تطبيقها.

ج- القيام بالمتابعة والرقابة للتحقق من تطبيق التعليمات والتأكد من سلامة الإجراءات.

د- أن يتم تحديث تلك الضوابط دورياً بما يساير تطور عمليات غسل الأموال أو تمويل الإرهاب.

المادة السابعة:

على المؤسسات المالية وغير المالية - عند توافر مؤشرات ودلائل كافية على إجراء عملية وصفقة معقدة أو ضخمة أو غير طبيعية، أو عملية تثير الشكوك والشبهات حول ماهيتها والغرض منها أو أن لها علاقة بغسل الأموال أو بتمويل الإرهاب أو الأعمال الإرهابية أو المنظمات الإرهابية- أن تبادر إلى اتخاذ الإجراءات الآتية:





الرقم / ٤/٥/١

التاريخ

التوايح

أ- إبلاغ وحدة التحريات المالية المنصوص عليها في المادة الحادية عشرة من هذا النظام بتلك العملية فوراً.

ب- إعداد تقرير مفصل يتضمن جميع البيانات والمعلومات المتوافرة لديها عن تلك العمليات والإطراف ذات الصلة، وتزويد وحدة التحريات به.

١/٧- تقوم المؤسسات المالية وغير المالية بوضع المؤشرات الدالة على وجود شبهة عمليات غسل أموال أو تمويل الإرهاب، كما يجب العمل على تحديثها بشكل مستمر حسب مقتضيات تطور وتنوع أساليب ارتكاب تلك العمليات مع الالتزام بما تصدره الجهات الرقابية بهذا الخصوص، مع إيلاء عناية خاصة لجميع العمليات ذات الأنماط غير الاعتيادية التي لا يكون لها غرض اقتصادي أو قانوني ظاهر أو واضح.

٢/٧- تقوم المؤسسات المالية وغير المالية بإبلاغ وحدة التحريات المالية عن جميع العمليات المشتبه بها بما في ذلك أي محاولات متعلقة بإجراء مثل هذه العمليات.

٣/٧- يكون إبلاغ وحدة التحريات المالية وفق النموذج المعتمد من قبل الوحدة على أن يشتمل البلاغ كحد أدنى على المعلومات الآتية:-

أ- أسماء الأشخاص المتهمين ومعلومات عن عناوينهم وأرقام هواتفهم.

ب- بيان بالعملية المشتبه فيها وأطرافها وظروف اكتشافها وحالتها الراهنة.

ج- تحديد المبلغ محل العملية المشتبه بها والحسابات المصرفية أو الاستثمارية ذات العلاقة.

د- أسباب و دواعي الاشتباه التي استند إليها الموظف المسئول عن الإبلاغ.

٤/٧- يراعى بالتقرير المعد من قبل المؤسسات المالية وغير المالية عن العمليات المبلغ عنها الآتي:-

أ- تقدم المؤسسات المالية لوحدة التحريات المالية التقرير خلال عشرة أيام من تاريخ التبليغ على أن يتضمن الآتي:

- كشوف الحسابات لفترة ستة اشهر.
- صور من والوثائق المرفقة بمستندات فتح الحساب.
- بيانات عن طبيعة العمليات المبلغ عنها.
- مؤشرات ومبررات الشك والمستندات المؤيدة لذلك.





الرقم ٤/٥/١ /

التاريخ

التوايح

ب- تقدم المؤسسات غير المالية تقريرها عن البلاغات عند طلبها من الوحدة وذلك خلال أسبوعين من تاريخ الطلب ويمكن أن يشتمل الطلب على ما يلي:

- معلومات عن الطرف المبلغ عنه.
- بيان بالمعاملات التجارية أو المالية للمبلغ عنه أو الأطراف ذات الصلة.
- تقدم المبررات والمؤشرات الدالة على الشك مؤيدة بالمستندات.

المادة الثامنة:

استثناءً من الأحكام المتعلقة بالسرية المصرفية فان على المؤسسات المالية وغير المالية تقديم الوثائق والسجلات والمعلومات للسلطة القضائية أو السلطة المختصة عند طلبها.

١/٨- تقوم السلطة القضائية أو هيئة التحقيق والادعاء العام أو وحدة التحريات المالية بطلب الوثائق والسجلات والمعلومات من المؤسسات المالية وغير المالية عن طريق وحدة مكافحة غسل الأموال بمؤسسة النقد العربي السعودي بالنسبة للمؤسسات المالية الخاضعة لإشرافها وعن طريق وحدة مكافحة غسل الأموال بوزارة التجارة والصناعة بالنسبة للمؤسسات غير المالية وعن طريق وحدة مكافحة غسل الأموال بهيئة السوق المالية بالنسبة للمؤسسات المالية الخاضعة لإشرافها وعن طريق وزارة العدل بالنسبة للممتلكات الثابتة.

٢/٨- يتم تقديم كافة الوثائق والسجلات والمعلومات من المؤسسات المالية وغير المالية للسلطة القضائية أو هيئة التحقيق والادعاء العام أو وحدة التحريات المالية عند طلبها عن طريق وحدة مكافحة غسل الأموال بمؤسسة النقد العربي السعودي بالنسبة للمؤسسات المالية الخاضعة لإشرافها وعن طريق وحدة مكافحة غسل الأموال بوزارة التجارة والصناعة بالنسبة للمؤسسات غير المالية وعن طريق وحدة مكافحة غسل الأموال بهيئة السوق المالية بالنسبة للمؤسسات المالية الخاضعة لإشرافها وعن طريق وزارة العدل بالنسبة للممتلكات الثابتة بصفة عاجله.

٣/٨- لا يجوز للمؤسسات المالية وغير المالية الاحتجاج بمبدأ سرية الحسابات أو هوية العملاء أو المعلومات المسجلة طبقاً لأي نظام آخر.

المادة التاسعة:

على المؤسسات المالية وغير المالية والعاملين فيها وغيرهم من الملزمين بأحكام هذا النظام ألا يحذروا العملاء أو يسمحوا بتحذيرهم أو تحذير غيرهم من الأطراف ذات الصلة من وجود شبهات حول نشاطاتهم.





الرقم ٤/٥١ /

التاريخ

التابع

١/٩ يراعى في تطبيق هذه المادة ولتجنب التصرف الذي من شأنه تحذير العملاء أو غيرهم ما يلي:

- أ- القبول الشكلي للعمليات المشتبه بها وعدم رفضها.
- ب- تجنب عرض البدائل للعملاء أو تقديم النصيحة أو المشورة لتفادي تطبيق التعليمات بشأن العمليات التي يجرؤونها.
- ج- المحافظة على سرية البلاغات عن العملاء أو العمليات المشتبه بها والمعلومات المرتبطة بها المرفوعة لوحدة التحريات المالية.
- د- أن لا يؤدي إجراء الاتصال بالعملاء أو مع الأطراف الخارجية للاستفسار عن طبيعة العمليات إلى إثارة الشكوك حوله.
- هـ- عدم إخطار العملاء بان معاملاتهم قيد المراجعة أو المراقبة ونحو ذلك.

المادة العاشرة:

- على المؤسسات المالية وغير المالية أن تضع برامج لمكافحة عمليات غسل الأموال، على أن تشمل هذه البرامج كحد أدنى ما يلي:
- أ- تطوير وتطبيق السياسات والخطط والإجراءات والضوابط الداخلية، بما في ذلك تعيين موظفين ذوي كفاية في مستوى الإدارة العليا لتطبيقها .
 - ب- وضع نظم تدقيق ومراجعة داخلية تعني بمراقبة توافر المتطلبات الأساسية في مجال مكافحة غسل الأموال.
 - ج- إعداد برامج تدريبية مستمرة للموظفين المختصين لإحاطتهم بالمستجدات في مجال عمليات غسل الأموال، وبما يرفع من قدراتهم في التعرف على تلك العمليات وأنماطها وكيفية التصدي لها.

١/١٠- يكون المدير العام أو من يفوضه في المؤسسات المالية وغير المالية هو المسئول عن تطبيق وتطوير السياسات والخطط والإجراءات والضوابط الداخلية التي تتعلق بمكافحة غسل الأموال أو تمويل الإرهاب.





الرقم ٤/٥١ /

التاريخ

التوايح

٢/١٠- تقوم المؤسسات المالية وغير المالية بتكليف موظف أو قسم مسئول عن الإبلاغ والاتصال بوحدة التحريات المالية المنصوص عليها في المادة الحادية عشرة من هذا النظام. وبالنسبة للمؤسسات الفردية غير المالية الصغيرة فيكون التبليغ من قبل مالك المؤسسة مباشرة أو ممن يفوضه.

٣/١٠- تحدد المؤسسات المالية وغير المالية وحدة رقابية مختصة لإجراء برامج المراقبة والتدقيق الداخلي في شئون مكافحة غسل الأموال أو تمويل الإرهاب، على أن تتضمن مهمة مراجع الحسابات الخارجي في حالة وجوده برنامج خاص عن مدى التزام المؤسسات المالية وغير المالية بسياسات مكافحة غسل الأموال أو تمويل الإرهاب.

٤/١٠- تستعين المؤسسات المالية وغير المالية بالجهات الرقابية المختصة حين وضع الوسائل الكفيلة بالتحقق من الالتزام بالأنظمة واللوائح والقواعد المقررة نظاماً لمكافحة غسل الأموال أو تمويل الإرهاب.

٥/١٠- تضع المؤسسات المالية وغير المالية خطط وبرامج وميزانيات مالية مخصصة لتدريب وتأهيل العاملين فيها في مجال مكافحة غسل الأموال أو تمويل الإرهاب حسب حجمها ونشاطها وذلك بالتنسيق مع الجهات الرقابية عليها.

٦/١٠- يستعان في تنفيذ برامج الإعداد والتأهيل والتدريب في مجال مكافحة غسل الأموال أو تمويل الإرهاب بالمعاهد المتخصصة محلية كانت أو خارجية، ويراعى في إعداد البرامج التدريبية أن تشمل على الآتي:-

أ- الاتفاقيات والأنظمة والقواعد والتعليمات ذات الصلة بمكافحة غسل الأموال أو تمويل الإرهاب.

ب- سياسات وأنظمة الجهات الرقابية في مجال مكافحة غسل الأموال أو تمويل الإرهاب.

ج- المستجدات في مجال عمليات غسل الأموال أو تمويل الإرهاب والعمليات المشبوهة الأخرى وكيفية التعرف على تلك العمليات وأنماطها وكيفية التصدي لها.

د- المسؤولية الجنائية والمدنية لكل موظف بموجب الأنظمة واللوائح والتعليمات ذات الصلة.





الرقم ٤١٥١ /

التاريخ

التوايح

المادة الحادية عشرة:

تنشأ وحدة لمكافحة غسل الأموال تسمى (وحدة التحريات المالية)، ويكون من مسؤولياتها تلقي البلاغات وتحليلها وإعداد التقارير عن المعاملات المشبوهة في جميع المؤسسات المالية وغير المالية وتحدد اللائحة التنفيذية لهذا النظام مقر هذه الوحدة وتشكيلها واختصاصاتها وكيفية ممارسة مهامها وارتباطها.

١/١١ ارتباط الوحدة ومقرها :-

ترتبط وحدة التحريات المالية بمساعد وزير الداخلية للشؤون الأمنية. ويكون مقرها الرئيسي بمدينة الرياض ويجوز لها فتح فروع في مناطق المملكة .

٢/١١ تشكيل الوحدة: تتشكل من مدير ومساعد وعدد كاف من المتخصصين في مجال مكافحة جرائم غسل الأموال وتمويل الإرهاب في التخصصات المالية والمحاسبية والقانونية والحاسب الآلي والتخصصات الأمنية.

٣/١١ اختصاصات الوحدة:

تختص الوحدة بالاتي:

أ- تلقي البلاغات الواردة من المؤسسات المالية وغير المالية والجهات الحكومية الأخرى والأفراد عن العمليات التي يشتبه في أنها جريمة غسل أموال أو تمويل الإرهاب.

ب- إنشاء قاعدة بيانات تزود بكافة البلاغات والمعلومات الخاصة بغسل الأموال أو تمويل الإرهاب ويتم تحديث هذه القاعدة تبعاً مع المحافظة على سريتها، وجعلها متاحة للجهات ذات العلاقة.

ج- طلب وتبادل المعلومات مع الجهات ذات العلاقة واتخاذ ما يلزم من إجراءات بصدد مكافحة غسل الأموال أو تمويل الإرهاب.

د- طلب وتبادل المعلومات مع وحدات التحريات المالية الأخرى فيما يتعلق بمكافحة غسل الأموال أو تمويل الإرهاب وفقاً لما نصت عليه المادة الثانية والعشرون من هذا النظام .





الرقم ٤/٥١ /

التاريخ

التوايح

هـ- إعداد النماذج التي تستخدم في إبلاغ المؤسسات المالية وغير المالية عن العمليات التي يشتبه في أنها غسل أموال أو تمويل الإرهاب، تشتمل على بيانات تعينها على القيام بأعمال جمع المعلومات والتحليل والتحري والتسجيل في قاعدة البيانات وتحديثها إذا اقتضى الأمر.

و- القيام بجمع المعلومات عما يرد إليها من بلاغات بشأن العمليات التي يشتبه في أنها غسل أموال أو تمويل إرهاب وتحليلها وللوحدة في ذلك الاستعانة بمن تراه من الخبراء والمختصين من الجهات ذات العلاقة.

ز- تقوم وحدة التحريات المالية بالبحث والتحري الميداني ولها أن تطلب ذلك من الجهات الأمنية بالبحث والتحري بقطاعات وزارة الداخلية وعند قيام الدلائل الكافية بأن العمليات الواردة في البلاغ لها علاقة بغسل الأموال أو تمويل الإرهاب تقوم بإحالتها للجهة المختصة بالتحقيق مع إعداد تقرير مفصل يتضمن بيانات كافية عن الجريمة التي قامت الدلائل على ارتكابها وعن مرتكبيها وماهية هذه الدلائل مشفوعاً بالرأي ومرفق به كافة الوثائق والمستندات والمعلومات ذات الصلة.

ح- الطلب من هيئة التحقيق والادعاء العام القيام بالحجز التحفظي على الأموال والممتلكات والوسائط المرتبطة بجريمة غسل الأموال أو تمويل الإرهاب على النحو المبين في المادة الثانية عشرة من هذا النظام.

ط- التصرف في البلاغات التي يسفر التحليل بشأنها عن عدم قيام الدلائل أو الشبهة على ارتكاب أي من الأفعال المنصوص عليها في المادة الثانية من هذا النظام.

ي- التنسيق مع الجهات الرقابية على المؤسسات المالية وغير المالية لتهيئة الوسائل الكفيلة بالتحقق من التزام تلك المؤسسات بالأنظمة واللوائح والتعليمات المقررة لمكافحة غسل الأموال أو تمويل الإرهاب.

ك- توفير التغذية العكسية للمؤسسات المالية وغير المالية المبلغة والسلطات المختصة ذات العلاقة بمكافحة عمليات غسل الأموال وتمويل الإرهاب.

ل- المشاركة في إعداد برامج توعوية بشأن مكافحة غسل الأموال أو تمويل الإرهاب بالتنسيق مع اللجنة الدائمة لمكافحة غسل الأموال.

م- رفع التوصيات اللازمة للجنة الدائمة لمكافحة غسل الأموال حول الصعوبات والمقترحات في مجال مكافحة غسل الأموال أو تمويل الإرهاب.





الرقم ٤/١١ /

التاريخ

التوايح

ن- لوحدة التحريات المالية الدخول في مذكرات تفاهم مع وحدات التحريات المالية الأخرى وفقاً للأنظمة والإجراءات المرعية .

س- استكمال الإجراءات النظامية للانضمام إلى مجموعة وحدات التحريات المالية (مجموعة الاغumont (The Egmont group).

٤/١١ أقسام الوحدة:

تتألف الوحدة من الأقسام التالية:

أ- قسم البلاغات

ب- قسم جمع المعلومات والتحليل

ج- قسم تبادل المعلومات

د- قسم المعلومات والدراسات

أولاً: قسم البلاغات:

١- تلقي البلاغات حول العمليات التي تثير الشكوك والشبهات حول ماهيتها والغرض منها أو أنها لها علاقة بغسل الأموال أو تمويل الإرهاب.

٢- استقبال البلاغات بواسطة الفاكس أو أية وسيلة أخرى وعند الإبلاغ عن طريق الهاتف يتم تأكيده بأي طريقة كتابية في أسرع وقت ممكن .

٣- يكون استقبال البلاغات وفقاً للنموذج المعد من الوحدة والمبلغ لجميع الجهات ذات العلاقة والمؤسسات المالية وغير المالية.

٤- تسجيل البلاغات في سجلات خاصة برقم مسلسل تدون فيه كافة المعلومات الضرورية.

٥- إحالة البلاغات إلى قسم جمع المعلومات والتحليل للتأكد من قيام الشبهة وتوفير الدلائل على وجود جريمة غسل الأموال أو تمويل الإرهاب.

ثانياً: قسم جمع المعلومات والتحليل:

١- التأكد من توافر المعلومات الضرورية في البلاغ وإرفاق المستندات اللازمة للتحليل

٢- الطلب من الجهة ذات العلاقة عند الحاجة إلى معلومات أو وثائق أو تقارير أو مستندات يستلزمها التحليل.





الرقم ٤/٥١/

التاريخ

التوايح

٣- دراسة البيانات والمعلومات المتوفرة بالبلاغ ومقارنتها بما يتوفر للقسم من معلومات للتأكد من صحتها وتقدير مناسبتها مع الاستعانة بسجلات الأجهزة الأمنية والمالية والتجارية والأجهزة الأخرى ذات العلاقة .

٤- عند قيام الدلائل الكافية بأن العمليات الواردة في البلاغ لها علاقة بغسل الأموال أو تمويل الإرهاب وظهور الحاجة لتحريات ميدانية أو ضبط أشخاص أو تعقب الأموال أو الأصول محل اشتباه، تقوم الوحدة بذلك ولها أن تطلب ذلك من الجهات الأمنية المعنية بالبحث والتحري بقطاعات وزارة الداخلية ومن ثم إعداد تقرير تحليلي متضمناً مرئياتها مشفوعاً بالبلاغ والوثائق والمستندات ذات الصلة لاستكمال الإجراءات وإحالته للجهة المختصة بالتحقيق .

٥- الطلب من هيئة التحقيق والادعاء العام حجز التحفظي على الأموال والممتلكات والوسائط المرتبطة بجريمة غسل الأموال على النحو المبين في المادة الثانية عشرة من النظام.

٦- التصرف في البلاغات والمعلومات التي يسفر جمع المعلومات والتحليل بشأنها عن عدم قيام الشبهة أو الدلائل على ارتكاب أي من الأفعال النصوص عليها في المادة الثانية من النظام.

ثالثاً: قسم تبادل المعلومات والمتابعة:

١- تبادل المعلومات مع السلطات المحلية والوحدات المماثلة في الدول الأجنبية فيما يتعلق بمكافحة غسل الأموال أو تمويل الإرهاب.

٢- تزويد قسم المعلومات والدراسات بعدد الطلبات التي تلقاها القسم بشكل دوري كل شهر سواء الطلبات الداخلية أو الخارجية.

رابعاً: قسم المعلومات والدراسات:

١- إنشاء قاعدة معلومات للاتي:

أ- البلاغات عن العمليات المشبوهة التي تم تلقيها وتحليلها وتعقبها.

ب- البلاغات التي تمت إحالتها لجهات أمنية لاستكمال مجريات البحث والتحري أو إلى جهة التحقيق المختصة.

ج- التقارير التي أدت إلى الملاحقة القضائية أو الإدارية.

د- حالات الإدانة في قضايا غسل الأموال أو تمويل الإرهاب.





الرقم /٤١٥١

التاريخ

التوايح

هـ- طلبات تبادل المعلومات التي تلقتها الوحدة من السلطات المحلية والوحدات الأجنبية المماثلة.

و- عدد البلاغات التي تم حفظها ومبررات ذلك.

٢- رصد مؤشرات جرائم غسل الأموال أو تمويل الإرهاب في المؤسسات المالية وغير المالية وأساليب ارتكابها واقتراح الحلول والإجراءات الواجب اتخاذها لمكافحتها وإحالتها للجنة الدائمة لمكافحة غسل الأموال.

٣- إعداد تقرير سنوي عن أعمال الوحدة ورفعها لوزير الداخلية وتزويد اللجنة الدائمة لمكافحة غسل الأموال بنسخة منه.

٤- متابعة المستجدات الخاصة بجرائم غسل الأموال أو تمويل الإرهاب عبر المنظمات والهيئات الإقليمية والدولية المعنية.

٥- المشاركة في إعداد برامج توعوية بشأن مكافحة غسل الأموال أو تمويل الإرهاب بالتنسيق مع اللجنة الدائمة لمكافحة غسل الأموال.

المادة الثانية عشرة:

لوحدة التحريات المالية عند التأكد من قيام الشبهة أن تطلب من الجهة المختصة بالتحقيق القيام بالحجز التحفظي على الأموال والممتلكات والوسائط المرتبطة بجريمة غسل الأموال لمدة لا تزيد على عشرين يوماً. وإذا اقتضى الأمر استمرار مدة الحجز أطول من ذلك فيكون بأمر قضائي من المحكمة المختصة.

١/١٢- يقع الحجز التحفظي على جميع الأموال والممتلكات أو الوسائط التي للمتهم أو المتهمين عند الأفراد والشركات والمؤسسات المالية وغير المالية أو أي جهة أخرى.

٢/١٢- يصدر طلب الحجز التحفظي من رئيس وحدة التحريات المالية أو من ينيبه في ذلك.

٣/١٢- يتم طلب الحجز التحفظي بمذكرة تتضمن بياناً وافياً عن الآتي:-

أ- معلومات تفصيلية عن الأشخاص المراد الحجز على أموالهم أو ممتلكاتهم أو وسائطها.

ب- تحديد الأموال والممتلكات والوسائط المراد حجزها.

ج- الشبهات والحديثات والأسباب المؤكدة المؤيدة للطلب.

د- مدة الحجز التحفظي بما لا يزيد عن المدة المحددة في هذه المادة.





الرقم ٤/٥١ /

التاريخ

التوايح

٤/١٢- يرسل طلب الحجز التحفظي بالطريقة السرية المناسبة إلى هيئة التحقيق والادعاء العام ويبيت في طلب الحجز على وجه السرعة وإشعار وحدة التحريات المالية بما يتقرر خلال ٤٨ ساعة.

٥/١٢- تبدأ مدة الحجز التحفظي المحددة في هذه المادة من وقت إيقاعه.

٦/١٢- عند صدور موافقة هيئة التحقيق والادعاء العام على طلب وحدة التحريات المالية تتم مخاطبة وحدة مكافحة غسل الأموال بمؤسسة النقد العربي السعودي لتنفيذ أمر الحجز على الأموال المودعة في المؤسسات المالية ولوزارة التجارة والصناعة بالنسبة للممتلكات وما يتعلق بأنشطة المؤسسات غير المالية ووزارة العدل للحجز على الأراضي والعقارات والأمن العام للحجز على الوسائط ولمصلحة الجمارك الحجز على البضائع والوسائط التي لديها وهيئة السوق المالية بالنسبة للأوراق المالية وتبلغ وحدة التحريات بذلك.

٧/١٢- تتخذ إجراءات طلب استمرار الحجز أو الأمر به قبل نهاية مدة العشرين يوماً بوقت كافٍ .

٨/١٢- تتولى جهة التحقيق عند صدور أمر باستمرار الحجز التحفظي إبلاغ الجهات الرقابية والأمنية بإنفاذ أمر المحكمة وإشعار وحدة التحريات المالية بذلك .

٩/١٢- إذا قدرت الجهة المختصة بالتحقيق أن الأمر لا يقتضي الحجز التحفظي على الأموال والممتلكات والوسائط الوارد في الطلب المقدم من الوحدة كان لها الكتابة - وبصفة عاجلة جداً - للوحدة بعدم موافقتها على ذلك الطلب مع أبداء مرئياتها حول ذلك.

١٠/١٢- للجهات والسلطات الرقابية المعنية بمكافحة غسل الأموال أن تطلب عن طريق وحدة التحريات المالية إيقاع الحجز التحفظي بما يتوافق مع المدة المقررة بالنظام .

١١/١٢- يكون طلب استمرار الحجز التحفظي بصحيفة تودع إلى المحكمة ويجب أن تشمل على البيانات الآتية:-

أ- المحكمة المرفوعة لها الدعوى.

ب- تاريخ تقديم الطلب.

ج- موضوع الدعوى وما يطلبه المدعي العام وأسانيده.

د- مدة استمرار الحجز المطلوبة





الرقم ٤/٥١ /

التاريخ

التوايح

المادة الثالثة عشرة:

يجوز تبادل المعلومات التي تكشف عنها المؤسسات المالية وغير المالية - وفقا لأحكام المادة (الثامنة) من هذا النظام - بين تلك المؤسسات والسلطات المختصة حين تكون تلك المعلومات متعلقة بمخالفة أحكام هذا النظام. وعلى السلطات المختصة الالتزام بسرية تلك المعلومات وعدم الكشف عنها إلا بالقدر الذي يكون ضروريا لاستخدامها في التحقيقات أو الدعاوى المتعلقة بمخالفة أحكام هذا النظام.

المادة الرابعة عشرة:

تحدد اللائحة التنفيذية لهذا النظام قواعد وإجراءات الإفصاح عن المبالغ المالية النقدية والمعادن الثمينة التي يسمح بدخولها المملكة وخروجها منها، وتحدد مقدار المبالغ والأوزان الواجب الإفصاح عنها.

١/١٤- تقدر المبالغ النقدية أو الأدوات المالية القابلة للتداول لحاملها أو المعادن الثمينة التي يجب الإفصاح عنها عند الخروج أو الدخول إلى المملكة — "٦٠,٠٠٠" ستين ألف ريال أو ما يعادلها من العملات الأجنبية.

٢/١٤- يمنع خروج أو دخول المسافر بأي مبالغ نقدية أو أدوات مالية قابلة للتداول لحاملها أو معادن ثمينة تزيد عن الحد المسموح به دون تعبئة نموذج الإفصاح وفي حالة ضبطه من الجهات الأمنية أو الجمارك بالمبلغ أو الأدوات المالية القابلة للتداول لحاملها أو المعادن الثمينة التي لم يفصح عنها وتزيد عن الحد المسموح يحال للجمرك (مسئول الفترة) ليتحرى عن أسباب عدم الإفصاح وفي حال اقتناعه بالأسباب فيطلب من المسافر تعبئة نموذج الإفصاح وإكمال بقية الإجراءات الخاصة بالإفصاح ويسمح له بالمغادرة أو الدخول بما يحمله، أما في حال عدم قناعة مسئول الفترة في الجمرك بالأسباب أو عند الاشتباه بغسل الأموال أو تمويل الإرهاب فيحال المسافر إلى الجهة المختصة للتحقيق معه وإبلاغ وحدة التحريات المالية بذلك.

٣/١٤- في حال حمل المسافر المغادر معادن ثمينة تتجاوز قيمتها ستين ألف ريال ويرغب في إخراجها من المملكة فعليه مراجعة الجمارك في المنفذ للإفصاح عنها وختم النموذج الخاص بالإفصاح وتقديم فاتورة





الرقم ٤/٥١/

التاريخ

التوايح

الشراء للتأكد من قيمتها وإذا تبين أنها لأغراض تجارية يطبق بحقه نظام الجمارك الموحد ولائحته التنفيذية.

٤/١٤ - عند ضبط المسافرين المغادر أو القادم إلى المملكة في حالة تكرار عدم إفصاحه أو في حال إفصاحه وتولد اشتباه بعلاقة الأموال بعمليات مشبوهة بغسل أموال أو تمويل إرهاب أو تقديم بيانات إفصاح كاذبة عن حمله مبالغ نقدية أو أدوات مالية قابلة للتداول لحاملها أو معادن ثمينة تزيد قيمتها عن الحد المقرر يتم إعداد محضر من قبل الجهة الضابطة التي تحيله للجمارك ومن ثم تقوم الجمارك بإحالتة للجهة المختصة بالتحقيق للمطالبة بمعاقبته وفق المادة العشرون من نظام مكافحة غسل الأموال أو نظام الجمارك حسب مايتضح من التحقيق وإشعار وحدة التحريات المالية ويتم إيداع المبلغ الزائد عن الحد المسموح به من قبل الجمارك في حساب خاص بالأمانات والمعادن الثمينة يتم التحفظ عليها من قبل الجمارك إلى حين تلقي إشعار من جهة التحقيق بشأنها.

٥/١٤ - تقوم الجمارك بالتفتيش على أساس العينة العشوائية أو بناءً على توفر معلومات اشتباه بغسل الأموال أو تمويل الإرهاب للمغادرين لضبط الأموال النقدية أو الأدوات المالية القابلة للتداول لحاملها أو المعادن الثمينة.

٦/١٤ - عند إفصاح القادم إلى المملكة لموظف الجمارك عن حمله لأموال نقدية أو أدوات مالية قابلة للتداول لحاملها أو معادن ثمينة تزيد قيمتها عن الحد المقرر فعلى موظف الجمارك في المنفذ القيام بالتأكد من سلامة النقد من التزيف عن طريق مندوب مؤسسة النقد، وبالنسبة للمعادن الثمينة فإنه يطلب منه إثبات ملكيتها بموجب فاتورة الشراء وإذا تبين له أنها لأغراض تجارية فيطبق عليه نظام الجمارك الموحد ولائحته التنفيذية.

٧/١٤ - ترسل نسخة من معلومات نماذج الإفصاح بالطريقة التي يتفق عليها من مصلحة الجمارك لوحدة التحريات المالية المنصوص عليها في المادة الحادية عشر من نظام غسل الأموال لتقوم بالتحقق من علاقة الأشخاص بجريمة غسل الأموال أو تمويل الإرهاب أو أي جرائم أخرى.

٨/١٤ - في حالة عدم مراجعة أصحاب هذه الأموال أو المعادن الثمينة بعد انقضاء الفترة المحددة بـ "٩٠" تسعين يوماً تعامل المضبوطات وفق الأنظمة السارية.





الرقم ٤/٥١ /

التاريخ

التوايح

٩/١٤- تسري هذه الإجراءات على الشركات أو المؤسسات المالية وغير المالية ومحلات الذهب وبعثات الحج والعمرة وشركات الخدمات الخاصة بنقل النقد أو الطرود البريدية وغير البريدية والإرساليات مع الاحتفاظ بحقها بممارسة أعمالها.

١٠/١٤- على مصلحة الجمارك إعداد قاعدة بيانات بأسماء الأشخاص الذين سبق لهم الإفصاح أو عدم الإفصاح بغرض معرفة من يتكرر منه ذلك مع إشعار وحدة التحريات المالية.

١١/١٤- تقوم الجمارك بإعداد نموذج الإفصاح المشار إليه بهذه المادة بعد التنسيق مع وحدة التحريات المالية وتوزيعه على المنافذ.

١٢/١٤- تقوم وزارة الداخلية ووزارة المالية بالإجراءات اللازمة بإبلاغ هذه التعليمات بمختلف الوسائل المتاحة وتوفير اللوحات الإرشادية في عدة أماكن بارزة في مداخل ومخارج جميع المنافذ الحدودية موضحة الإجراءات والعقوبات التي ستطبق في حالة مخالفة النظام .

المادة الخامسة عشرة:

إذا حكم بمصادرة أموال أو متحصلات أو وسائط وفقاً لأحكام هذا النظام وكانت غير واجبة الإلتلاف فللسلطة المختصة أن تتصرف بها وفقاً للنظام، أو اقتسامها مع الدول التي تربطها مع المملكة اتفاقيات أو معاهدات سارية.

١/١٥- يقصد بالسلطة المختصة الواردة في هذه المادة والمعنية بالتصرف بالأموال أو المتحصلات أو الوسائط المصادرة هي الجهة المنفذة للحجز التحفظي.

٢/١٥- بينما يقصد بالسلطة المختصة الواردة في هذه المادة والمعنية باقتسام الأموال أو المتحصلات أو الوسائط المصادرة مع الدول التي تربطها مع المملكة اتفاقيات أو معاهدات سارية هي لجنة المساعدة القانونية المتبادلة بوزارة الداخلية.

٣/١٥- يرد النص على طلب مصادرة الأموال أو المتحصلات أو الوسائط في لوائح الادعاء وكذلك في الأحكام القضائية الصادرة من المحاكم بهذا الشأن.

٤/١٥- يشمل حكم المصادرة على الأموال والمتحصلات أو الوسائط محل الجريمة سواء المضبوطة وغير المضبوطة في الداخل أو الخارج.

٥/١٥- يراعى في تطبيق هذه المادة في شأن الأموال أو المتحصلات أو الوسائط المحكوم بمصادرتها الآتي:





الرقم ٤/٥١ /

التاريخ

التوايح

أ- المادة الرابعة والتسعون من نظام الإجراءات الجزائية ولائحته التنفيذية بخصوص

ما يتلف بمرور الزمن أو يستلزم حفظه نفقات كبيرة تستغرق قيمته.

ب- إدخال الأموال أو المتحصلات أو الوسائط المصادرة إلى خزينة الدولة.

ج- قرار مجلس الوزراء رقم (٤٧) وتاريخ ١٨/٢/١٤٢١هـ والذي يقضي بتحويل المبالغ

المضبوطة مع المتهمين في قضايا المخدرات وقيمة الأعيان التي صدرت أحكام قضائية

بمصادرتها إلى مؤسسة النقد العربي السعودي لإيداعها في حساب مستقل يتم الصرف منه على

احتياجات المديرية العامة لمكافحة المخدرات.

المادة السادسة عشرة:

يعاقب كل من يرتكب جريمة غسل الأموال المنصوص عليها في المادة (الثانية) من هذا النظام بالسجن مدة

لا تزيد على عشرة سنوات وبغرامة مالية لا تزيد عن خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، مع

مصادرة الأموال و المتحصلات و الوسائط محل الجريمة. وإذا اختلطت الأموال و المتحصلات بأموال

اكتسبت من مصادر مشروعة كانت هذه الأموال خاضعة للمصادرة في حدود ما يعادل القيمة المقدرة

للمتحصلات غير المشروعة.

وللمحكمة المختصة أن تعفي من هذه العقوبات مالك الأموال أو المتحصلات موضوع التجريم أو حائزها أو

مستخدمها إذا ابلغ السلطات قبل علمها بمصادر الأموال أو المتحصلات وهوية المشتركين، دون أن يستفيد

من عائداتها.

١/١٦- تقوم جهة التحقيق بتقدير القيمة المقدرة للمتحصلات غير المشروعة من خلال الاستعانة بأصحاب

الخبرة ويصدر بشأنها حكم من المحكمة المختصة.

٢/١٦- يتم تقديم طلب النظر في الإعفاء من تطبيق العقوبات على المبلغ من قبل الجهة المختصة بالتحقيق .

٣/١٦- عند تلقي مثل هذه البلاغات تتخذ إجراءات البحث والتحري للتحقق من عدم علم السلطات بالجريمة.





الرقم / ٤١٥١

التاريخ

التوايح

المادة السابعة عشرة:

تكون عقوبة السجن مدة لا تزيد عن خمس عشرة سنة و غرامة مالية لا تزيد على سبعة ملايين ريال سعودي إذا اقترنت جريمة غسل الأموال بأي من الحالات الآتية:

- أ- إذا ارتكب الجاني جريمة من خلال عصابة منظمة.
- ب- استخدام الجاني للعنف أو الأسلحة.
- ج- شغل الجاني وظيفة عامة واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.
- د- التغرير بالنساء أو القصر واستغلالهم.
- هـ- ارتكاب الجريمة من خلال مؤسسة إصلاحية أو خيرية أو تعليمية أو في مرفق خدمة اجتماعية.
- و- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني، ويوجه خاص في جرائم مماثلة.

المادة الثامنة عشرة:

دون الإخلال بالأنظمة الأخرى يعاقب بالسجن - مدة لا تزيد على سنتين وبغرامة مالية لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين- كل من اخل من رؤساء مجالس إدارات المؤسسات المالية وغير المالية أو أعضائها أو أصحابها أو مديريها أو موظفيها أو ممثليها المفوضين عنها أو مستخدميها ممن يتصرفون بمقتضى هذه الصفات بأي من الالتزامات الواردة في المواد (الرابعة، الخامسة السادسة، السابعة، الثامنة، التاسعة، العاشرة) من هذا النظام، ويسري تطبيق العقوبة على من يزاول النشاط دون الحصول على التراخيص اللازمة.

١/١٨- الأنظمة الأخرى المقصودة بهذه المادة كافة الأنظمة الصادرة من الأجهزة الإشرافية على المؤسسات المالية وغير المالية ومنها نظام الشركات ونظام السجل التجاري ونظام مراقبة البنوك ونظام السوق المالية.. ونحوها.





الرقم /٤١٥١١

التاريخ

التوايح

المادة التاسعة عشرة:

يجوز بحكم بناء على ما ترفعه الجهة المختصة أن توقع على المؤسسات المالية وغير المالية التي تثبتت مسؤوليتها وفقاً لأحكام المادتين (الثانية) و (الثالثة) من هذا النظام، غرامة مالية لا تقل عن مائة ألف ريال ولا تزيد على ما يعادل قيمة الأموال محل الجريمة.

١/١٩- الجهة المختصة في هذه المادة هي هيئة التحقيق والادعاء العام.

٢/١٩- تستند دعوى مسؤولية المؤسسات المالية وغير المالية على التقارير الفنية التي تصدر من الجهات الرقابية بالإضافة إلى طرق الإثبات الأخرى .

٣/١٩- لا يتعارض تطبيق العقوبات الواردة في هذه المادة مع الجزاءات الإدارية والتأديبية المنصوص عليها في الأنظمة الأخرى والتي يمكن أن توقع على المؤسسات المالية وغير المالية من قبل الجهات الرقابية حيال ثبوت مسؤوليتها.

المادة العشرون:

فيما عدا العقوبات المنصوص عليها في هذا النظام، يعاقب كل من يخالف أحكامه بالسجن مدة لا تزيد على ستة أشهر وبغرامة مالية لا تزيد على مائة ألف ريال ، أو بإحدى هاتين العقوبتين.

المادة الحادية والعشرون:

لا تطبق العقوبات الواردة في هذا النظام بحق من وقع في مخالفته بحسن نية.

١/٢١ يقدر حسن النية من الجهة القضائية المختصة ويسندل عليه من الظروف والملابسات الموضوعية.

المادة الثانية والعشرون:

يجوز تبادل المعلومات التي تكشف عنها المؤسسات المالية وغير المالية بين تلك المؤسسات والسلطات المختصة في دول أخرى تربطها بالمملكة اتفاقيات أو معاهدات سارية ، أو تبعاً للمعاملة بالمثل، وذلك وفقاً للإجراءات النظامية المتبعة، دون أن يشكل ذلك إخلالاً بالأحكام والأعراف المتعلقة بسرية أعمال المؤسسات المالية وغير المالية.





الرقم /٤/٥١

التاريخ

التوايح

١/٢٢- يقصد بالسلطات المختصة بالدول الأخرى الواردة في هذه المادة هي وحدة التحريات المالية أو ما يماثلها بالمهام.

٢/٢٢- يتم تبادل المعلومات التي تكشف عنها المؤسسات المالية وغير المالية فيما يتعلق بجريمة غسل الأموال أو تمويل الإرهاب عن طريق وحدة التحريات المالية.

٣/٢٢- يراعى عند تنفيذ تبادل المعلومات إعمالاً لأحكام الاتفاقيات أو المعاهدات السارية أو تبعاً للمعاملة بالمثل الآتي:-

أ- أن لا تستخدم المعلومات المتبادلة إلا في الغرض الذي طلبت من أجله.

ب- أن لا تقدم المعلومات المتبادلة إلى طرف ثالث إلا بعد موافقة وحدة التحريات المالية.

المادة الثالثة والعشرون:

للسلطة القضائية - بناءً على طلب من محكمة أو سلطة مختصة بدولة أخرى تربطها بالمملكة اتفاقية أو معاهدة سارية أو تبعاً للمعاملة بالمثل - أن تأمر بالتحفظ على الأموال أو المتحصلات أو الوسائط المرتبطة بجريمة غسل الأموال وفق الأنظمة المعمول بها في المملكة.

وللسلطة المختصة بناءً على طلب من سلطة مختصة بدولة أخرى تربطها بالمملكة اتفاقية أو معاهدة سارية أو تبعاً للمعاملة بالمثل - أن تأمر بتعقب الأموال أو المتحصلات أو الوسائط المرتبطة بجريمة غسل الأموال وفق الأنظمة المعمول بها في المملكة.

١/٢٣- تعد الطلبات الواردة من الدول الأخرى بشأن التحفظ أو التعقب على الأموال أو المتحصلات أو الوسائط المرتبطة بجريمة غسل الأموال أو تمويل الإرهاب من أعمال لجنة المساعدة القانونية المتبادلة ومقرها وزارة الداخلية والمشكلة بموجب قرار مجلس الوزراء رقم (١٦٨) في ١٤١٩/٨/١١ هـ المعدل بالقرار رقم (٣) في ١٤٢٤/١/٧ هـ وتتخذ بشأنها الإجراءات النظامية .

٢/٢٣- تحال الطلبات المتعلقة بالتحفظ على الأموال أو المتحصلات أو الوسائط المرتبطة بجريمة غسل الأموال إلى ديوان المظالم ليتم إصدار الأحكام القضائية لتنفيذه عن طريق الأجهزة الإشرافية المختصة وتبلغ وحدة التحريات بذلك.

٣/٢٣- تحال الطلبات المتعلقة بتعقب الأموال أو المتحصلات أو الوسائط المرتبطة بجريمة غسل الأموال أو تمويل الإرهاب إلى هيئة التحقيق والإدعاء العام لتنفيذه عن طريق الأجهزة الإشرافية المختصة.





الرقم /٤/٥١١

التاريخ

التابع

٤/٢٣- أي طلب يقدم وفقاً لهذه المادة يجب أن يشمل على الآتي:-

- أ- تحديد الجهة التي تقدم الطلب.
- ب- موضوع وطبيعة التحقيق أو الملاحقة أو الإجراءات القضائية التي يتعلق بها الطلب، واسم واختصاصات السلطة القائمة بهذه التحقيقات أو الملاحقات أو الإجراءات القضائية.
- ج- ملخص للوقائع والإجراءات المتخذة ذات الصلة بالموضوع.
- د- تحديد نوع الطلبات أو أي إجراء خاص يود الطرف الطالب أن يتم تعقبه.
- هـ- تحديد هوية أي شخص معني ومكانه وجنسيته.
- و- تحديد الأموال والمتحصلات والوسائل المطلوب التحفظ عليها أو تعقبها.
- ز- تحديد مدة التحفظ المطلوبة.
- ح- ما يثبت الاختصاص القضائي للدولة الطالبة.

المادة الرابعة والعشرون:

يجوز الاعتراف والتنفيذ لأي حكم قضائي بات ينص على مصادرة الأموال أو العائدات أو الوسائل المتعلقة بجرائم غسل الأموال صادر من محكمة مختصة بدولة أخرى تربطها بالمملكة اتفاقية أو معاهدة سارية أو تبعاً للمعاملة بالمثل، وذلك إذا كانت الأموال أو المتحصلات أو الوسائل التي نص عليها هذا الحكم جائزاً إخضاعها للمصادرة وفقاً للنظام المعمول به في المملكة.

١/٢٤- تعد طلبات تنفيذ الأحكام الواردة من الدول الأخرى المرتبطة بجريمة غسل الأموال أو تمويل الإرهاب من أعمال لجنة المساعدة القانونية المتبادلة.

٢/٢٤- تحال الطلبات المتعلقة بتنفيذ الأحكام الأجنبية المرتبطة بجريمة غسل الأموال إلى ديوان المظالم .

٣/٢٤- أي حكم يراد الاعتراف به وتنفيذه يجب أن يشتمل إضافة إلى الفقرات (من أ إلى ح) من المادة ٦/٢٣ من هذه اللائحة على الآتي :-

أ- أن تكون المصادرة بحكم قضائي بات واجب النفاذ في جريمة من الجرائم المنصوص عليها في المادة الثانية من هذه النظام.

ب- أن يكون حكم المصادرة قابلاً للتنفيذ في المملكة.





الرقم ٤/٥١ /

التاريخ

التوايح

ج- أن لا تكون الأموال أو المتحصلات المراد مصادرتها سبق وان حكم بمصادرتها نتيجة حكم قضائي آخر أو من جهة ذات اختصاص.

المادة الخامسة والعشرون:

يعفى رؤساء وأعضاء مجالس إدارات المؤسسات المالية وغير المالية وأعضاؤها أو أصحابها أو موظفوها أو مستخدموها أو ممثلوها المفوضون عنها - من المسؤولية الجنائية أو المدنية أو الإدارية التي يمكن أن تترتب على تنفيذ الواجبات المنصوص عليها في هذا النظام أو على الخروج على أي قيد مفروض لضمان سرية المعلومات وذلك ما لم يثبت أن ما قاموا به قد كان بسوء نية لأجل الإضرار بصاحب العملية.

١/٢٥ تقدر سوء النية من الجهة القضائية المختصة ويستدل عليه من الظروف الواقعية أو الموضوعية.

المادة السادسة والعشرون:

تختص المحاكم العامة بالفصل في كافة الجرائم الواردة في هذا النظام.

المادة السابعة والعشرون:

تتولى هيئة التحقيق والادعاء العام التحقيق و الادعاء العام أمام المحاكم العامة في الجرائم الواردة في هذا النظام.

المادة الثامنة والعشرون:

يصدر وزير الداخلية بالاتفاق مع وزير المالية والاقتصاد الوطني اللاحة التنفيذية لهذا النظام خلال تسعين يوماً من تاريخ صدوره.

١/٢٨- يتم مراجعة اللاحة التنفيذية لأغراض التحديث خلال خمس سنوات أو عندما تستدعي الحاجة لذلك.

المادة التاسعة والعشرون:

ينشر هذا النظام في الجريدة الرسمية، ويعمل به بعد مرور ستين يوماً من تاريخ نشره.



Banking Inspection
Department



Saudi Arabian Monetary
Agency

**قواعد
مكافحة غسل الأموال وتمويل الإرهاب**

**RULES GOVERNING
ANTI-MONEY LAUNDERING
&
COMBATING TERRORIST FINANCING**

Second Update

December 2008

4.1.1	Business Risk Assessment	16			..
4.2	AML/CTF Compliance Programs	17			.
4.3	Know Your Customer Standards	18		" "	.
4.3.1	Customer Due Diligence/ Know Your Customer	18		/	..
4.3.2	Customer Identification Process	19			..
4.3.3	Beneficial Owners (Natural & Legal)	20		()	..
4.3.4	Customer & Transaction Profiling	21			..
4.3.5	Name Checking of Designated Persons	22			..
4.4	Customer Risk Assessment	23			.
4.5	Customer Risks	23			.
4.5.1	Individual Personal Accounts	24			..
4.5.2	Walk-In Customers	25		()	..
4.5.3	Commercial Entities Accounts	26			..
4.5.4	Politically Exposed Persons	27			..
4.5.5	Private Banking Customers	28			..
4.5.6	Charity & Non-Profit Organizations	29			..
4.5.7	Trustees, Nominees & Intermediaries Accounts	30			..
4.5.8	Insurance Companies Accounts	31			..
4.5.9	Introduced & Referred Businesses	31			..
4.5.10	Correspondent Banking Relationships	32			..
4.6	Monitoring Customer Activity	33			.
4.6.1	Monitoring Process	33			..
4.6.2	Financial Investigation Process	35		()	..
4.6.3	Transaction Monitoring Threshold	36			..
4.7	Suspicious Transaction	36			.
4.7.1	Reporting Suspicious Transactions	36			..
4.7.2	Reporting Requirements	37			..
4.7.3	Tipping Off	37			..
4.7.4	Money Laundering Control Unit (MLCU)	38			..
4.8	Internal Controls	39			.
4.8.1	Internal Control Procedures	39			..
4.8.2	Assessment of Internal Controls	40			..
4.9	Staff Training & Hiring	40			.
4.9.1	Staff Training & Awareness	40			..
4.9.2	Staff Hiring & Appointment of Senior Positions	41			..
4.10	Record Keeping & Retention	41			.
5	AML/CTF Other Risks	42			
5.1	Product/ Service Risks	42		/	.
5.1.1	Cash	42			..
5.1.2	Wire Transfers	43			..
5.1.3	Alternative Remittances	44			..
5.1.4	Money Exchanging	45		()	..
5.1.5	Electronic Banking	45			..

SAMA RULES GOVERNING ANTI-MONEY LAUNDERING & COMBATING TERRORIST FINANCING

5.1.6	International Trade	46			..
5.2	Country Geographic Risks	46		/	.
5.3	Risk Variables	47			.
6	Glossary	48		()	
7	Appendices	51			
7- A	Saudi AML Law & Bylaws	51			-
7- B	FATF 40 Recommendations on Anti-Money Laundering	51		()	-
7- C	FATF 9 Special Recommendations on Combating Terrorist Financing	51		()	-
7- D	FATF Member Countries & NCCTs	51		.()	-
7- E	Basel Committee Standards	51			-
7- F	UN Security Council Resolutions	51			-
7- G	Other Useful Resources & Links	51			-
8	Suspicious Transaction Report (STR)	52			
9	Cash Declaration Form	55			
10	Red Flag Indicators	56			

<p>1.1.3 National Level</p> <ul style="list-style-type: none"> • Saudi Arabia enacted the Anti-Money Laundering Law and Bylaws, under the 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 Arabia 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. 	<p>..</p> <p>•</p> <p>//</p> <p>•</p> <p>•</p>
<p>1.2 SAMA Initiatives</p> <p>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 records as well as reporting of suspicious transactions to the competent authorities. These directives have since been put together into the following major regulatory manuals:</p>	<p>_____</p>
<p>1.2.1 AML/CTF Regulations</p> <p>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".</p> <p>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 its continued efforts to further improve and refine the regulations, and to keep abreast with the developing trends locally, regionally and globally, SAMA has issued this Second Update.</p> <p>Banks and money exchangers are required to make these regulations an integral part of their systems and procedures aimed at controlling, detecting, preventing, and reporting such 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 certification by external auditors.</p>	<p>..</p> <p>•</p> <p>•</p>
<p>1.2.2 Account Opening Regulations for Banks</p> <p>In May 2002, SAMA issued its first set of "Rules Governing Opening of Bank Accounts & General Operational 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</p>	<p>..</p> <p>•</p> <p>•</p>

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 keep abreast with the 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, and the thered Update on December 2008. 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:

- Guidelines for Combating Embezzlement & Fraudulent Transactions,(second issue) in August 2008
- Qualification Requirements for Appointment to Senior Positions in Banks, issued in April 2005
- Guidelines for Banks in Saudi Arabia for Organizing Audit Committees, issued in July 1996
- Internal Control Guidelines for Banks Operating in the Kingdom, issued in December 1989
- Other relevant SAMA Regulatory Circulars, issued on various dates

1.3 Objectives

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

1. To ensure banks and money exchangers in Saudi Arabia comply with the Saudi AML Law & Bylaws.
2. To help banks and money exchangers operating in Saudi Arabia to comply with the Banking Control Act, 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 40+9 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 financial criminal activities.
5. To maintain, enhance and protect the credibility, integrity and reputation of the Saudi Arabian banking and financial systems.
6. To provide security and appropriate degree of protection for costumers.

<p>1.4 General Developments & Trends</p> <p>By all accounts, worldwide money laundering activities, particularly those related to drugs, now constitute a multi-billion dollar business annually. It is inconceivable and unlikely that such large amounts of money can be stored or moved without the cooperation or willing 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.</p> <p>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 has carried out extensive work and issued 40+9 Recommendations to counter the spread of money laundering and terrorist financing.</p> <p>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.</p>	<p>()</p>
<p>2. Legal Framework & Regulatory Requirements</p>	
<p>2.1 The Saudi AML Law & Bylaws</p> <p>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.</p> <p>The AML Law, through its 29 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.</p>	
<p>2.2 SAMA – Regulatory & Supervisory Body</p> <p>The Saudi Arabian Monetary Agency (SAMA), in accordance with the authority and powers vested on it under the following 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 and effectively implement the relevant laws and regulations.</p> <ol style="list-style-type: none"> 1. The Charter of Saudi Arabian Monetary Agency – Articles 1 (c) and 3 (d). 2. The Banking Control Law – Article 16 (3). 3. The Anti-Money Laundering Law – Article 6 and its Bylaws 6.1 and 6.2. 4. Decision of the Minister of Finance & National Economy on Regulating Money Changing Business. <p>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</p>	<p>() () -</p> <p>() -</p>

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 body 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.

2.3 Overseas Branches & Subsidiaries of Saudi Banks & Money Exchangers

As per the Saudi AML Law Article 3 Bylaw 3.2, these regulations are also applicable to overseas branches and subsidiaries of all Saudi banks and money exchangers operating in the Kingdom. Therefore, 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.

<p>2.4 <u>Legal Responsibilities of Banks/ Money Exchangers & Employees</u></p> <p>The Saudi AML Law and Bylaws stipulate responsibilities, offenses, violations and penalties that have direct or indirect implications to the institution and to its staff personally. (For full details of the AML Law and Bylaws, refer to Appendix7- A):</p>	<p>_____ .</p> <p>(-)</p>
<p>2.5 <u>Financial Intelligence Unit (FIU)</u></p> <p>Information gathering, investigation and analysis processes are critical elements by the concerned authorities to effectively combat and prevent money laundering, terrorist financing and other financial crimes. In response, countries around the world have created specialized governmental agencies, known as Financial Intelligence Units, to be the central office for obtaining such financial information reports.</p> <p>Similarly, Saudi Arabia, as per Article 11 of the Saudi AML Law, has given a mandate to form a Financial Intelligence Unit (SAFIU) to be responsible for receiving, analyzing and disseminating to competent authorities disclosures of financial information reports on suspicious activities from financial and non-financial institutions. SAFIU has been established under the authority of the Ministry of Interior.</p>	<p>_____ .</p>
<p>2.6 <u>Cooperation Among Authorities & Banks/ Money Exchangers</u></p> <p>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 exchange and sharing should be coordinated and achieved only through SAMA to maintain controlled flow of confidential information.</p>	<p>_____ .</p>
<p>2.6.1 <u>Cooperation With Local Authorities</u></p> <p>Under Article 13 of 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:</p> <ol style="list-style-type: none"> 1. Establishment of a Money Laundering Control Unit (MLCU) or a designated Compliance Officer within the bank or money exchanger, responsible for internal reporting and informing FIU with a copy to SAMA, when money laundering or terrorist financing activities are suspected. (Refer to Rule 4.7.4 of these Rules for details 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, establishing the manner and form of such information. 5. In some instances, depending upon the case, a new or a different procedure may need to be developed. 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. 	<p>()</p> <p>_____ .</p> <p>()</p> <p>_____ .</p> <p>()</p>

<p>the proceeds of crime;</p> <ol style="list-style-type: none"> 2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; 3. The acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime. 	
<p>3.1.2 Processes of Money Laundering</p> <p>There are three stages of money laundering, explained as follows:</p> <p>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 security or insurance contract, check cashing services, the retail economy (through cash purchases), and smuggling of cash between countries.</p> <p>2. Layering The next phase is the layering, which usually consists of a series of transactions, through conversions and movements of funds, designed to conceal the origin of the funds. This may involve sending wire transfers to other banks, purchase and sale of investments, financial instruments, insurance contracts, phony investments or trade schemes, and the like.</p> <p>3. Integration The last phase is integration, which involves the re-entering of the funds into the legitimate economy. This is accomplished through the purchase of assets, securities/ financial assets, or luxury goods, and investment in real estate or business ventures.</p>	
<p>3.2 Terrorist Financing</p>	
<p>3.2.1 Definition of Terrorist Financing</p> <p>The Saudi AML Law Article 1.7 defines criminal activity as: any activity sanctioned by Shariah or law including the financing of terrorism, terrorist acts and terrorist organizations. The Bylaw 2.1 of the AML Law Article 2 describes "financing terrorism, terrorists' acts and terrorist organizations include property that comes from legitimate sources".</p> <p>The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism describes terrorist financing in the following way:</p> <p>"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:</p> <ol style="list-style-type: none"> 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." <p>Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards fighting terrorist financing and has criminalized financing of terrorism,</p> 	

<p>terrorist acts and terrorist organizations, under Article 2.d of the Saudi AML Law.</p> <p>SAMA requires strict compliance with UN and FATF directives. If a bank or money exchanger has any reason to believe that individual, commercial establishment 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, the bank or money exchanger must refrain from entering into transactions and must report the matter to the competent authorities.</p>	<p>()</p>
<p>3.2.2 Processes of Terrorist Financing</p> <p>The techniques used to finance terrorism are essentially the same as those used to conceal the sources and uses of money laundering, however, the main differences between the two are that (a) often small amounts are required to commit individual terrorist acts, making it difficult to track the terrorist funds; and (b) terrorists can be funded from legitimately obtained income, making it difficult to identify the stage at which legitimate funds become terrorist funds. Terrorists may derive their income from a variety of sources, often combining both lawful and unlawful funding. The forms of financing can be categorized into the following types:</p> <p>1. Financial Support This funding could be in the form of charitable donations, community solicitation and other fund raising initiatives, which may come from entities or individuals.</p> <p>2. Criminal Activity This funding is often derived from criminal activities such as money laundering, fraud and other financial crimes.</p> <p>3. Legitimate Source This form of funding may originate from legitimate business activity, established to fully or partially fund these illegal activities.</p>	<p>()</p>
<p>3.3 Typologies</p> <p>The various techniques or methods used to launder money or finance terrorism are generally referred to as <i>typologies</i>. A typology study is a useful tool to examine in depth a particular issue of concern with a view to providing insight and knowledge on emerging threats and how these might be addressed.</p> <p>FATF and MENA-FATF regularly issue documents relating to money laundering and terrorist financing typologies, and banks and money exchangers should update themselves with the new typologies applicable to their businesses. The following are examples of typical typologies relating to money laundering and terrorist financing:</p>	<p>(typologies)</p> <p>()</p> <p>()</p> <p>()</p>

<p>4. Policies & Standards</p> <p>4.1 Risk-Based Approach</p> <p>Banks and money exchangers should 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 allow resources to be allocated in the most efficient ways. Some of the benefits of utilizing risk-based approach in discharging banks' or money exchangers' AML/CTF responsibilities are:</p> <ol style="list-style-type: none"> 1. Allowing banks and money exchangers to differentiate between customers risk in a particular business by focusing on higher threats, thus improving the outcome of the overall process; 2. While establishing minimum standards, allowing a bank or money exchanger to apply its own approach to systems and controls, and arrangements in particular circumstances, thus allowing more flexibility to adapt as risks evolve; and 3. Helping to create better management of risks and cost effective system. <p>A risk-based approach will serve to balance the burden placed on individual banks and money exchangers and on their customers with a realistic assessment of the threat of a business being used in connection with money laundering or terrorist financing by focusing effort on areas where it is needed and has most impact.</p> <p>Banks and money exchangers may face some challenges that they need to consider while implementing the risk-based approach. These challenges should be regarded as offering opportunities to implement a more effective system in the fight against money laundering and terrorist financing activities. Some of these challenges can be summarized as follows:</p> <ol style="list-style-type: none"> 1. Risk Assessment Methodology: Identifying appropriate information to conduct a sound risk analysis and overall assessment. 2. Judgmental Decisions: Greater needs for more expert staff capable of making sound judgments regarding risk identification and evaluation. 3. Transitional Cost: Cost relating to transition from prescription method to risk based method. 4. Fear Factor: Regulatory response to potential diversity of practice. <p>The risk-based approach requires certain actions to be taken in assessing the most cost effective and proportionate ways to manage and mitigate the money laundering and terrorist financing risks faced by a bank. These actions are:</p> <ol style="list-style-type: none"> 1. Identifying the money laundering and terrorist financing risks that are relevant to the bank or money exchanger in order to ensure that the approach is built on sound foundation, and that the risks are well understood. 2. Assessing the identified risks presented by the bank's or money exchanger's particular aspect: <ol style="list-style-type: none"> a. Customers; b. Products and services; c. Delivery channels; d. Geographical area of operation. <p>The weight given to the above risk categories in assessing the overall risk of potential money laundering</p> 	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<p>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 determination as to the risk weights.</p> <ol style="list-style-type: none"> 3. Establishing and implementing controls to mitigate these assessed risks. 4. Monitoring and improving the effective operation of these controls. 5. Recording appropriately what has been done and explaining the reasons and rationale. 	
<p>4.1.1 Business Risk Assessment</p> <p>Banks and money exchangers should conduct and document the above business risk assessment. In particular, banks and money exchangers should update this assessment on annual basis, to identify changes in their business environments (such as organizational structure), its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services. Banks and money exchangers must build their AML/CTF programs based on the conclusions and the residual risk identified in the business risk assessment. To achieve an adequate assessment, a bank or money exchanger should establish that it has considered its exposure to money laundering and terrorist financing risk by:</p> <ol style="list-style-type: none"> 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 and capacity issues. 3. Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation. 4. Considering the type and nature of its customers and what they do. 5. Considering whether any additional risks are posed by the jurisdictions with which its customers (including intermediaries and introducers) are connected. Factors such as high levels of organized crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect money laundering and financing of terrorism will impact the risk posed by relationships connected with such jurisdictions. 6. Considering the characteristics of the products and services that the bank or money exchanger offers and assessing the associated vulnerabilities posed by each product and service, including delivery methods. For example: <ol style="list-style-type: none"> a. Products such as current accounts are more vulnerable because they allow payments to be made to and from third parties, including cash transactions. b. The use of third parties such as group entities, introducers and intermediaries to obtain information about the customer. c. Pooled relationships with intermediaries are more vulnerable, because of the anonymity provided by the co-mingling of assets or funds belonging to several customers by the intermediary. d. Conversely, those 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 it establishes and delivers products and services to its customers. For example, risks are likely to 	

be greater whether relationships may be established remotely (non-face-to-face), or may be controlled remotely by the customer (straight-through processing of transactions).

8. Recording, updating and retaining its business risk assessment.

4.2 AML / CTF Compliance Programs

Article 10 of the Saudi AML Law requires financial institutions to develop appropriate AML/CTF programs which should include, as a minimum, the following:

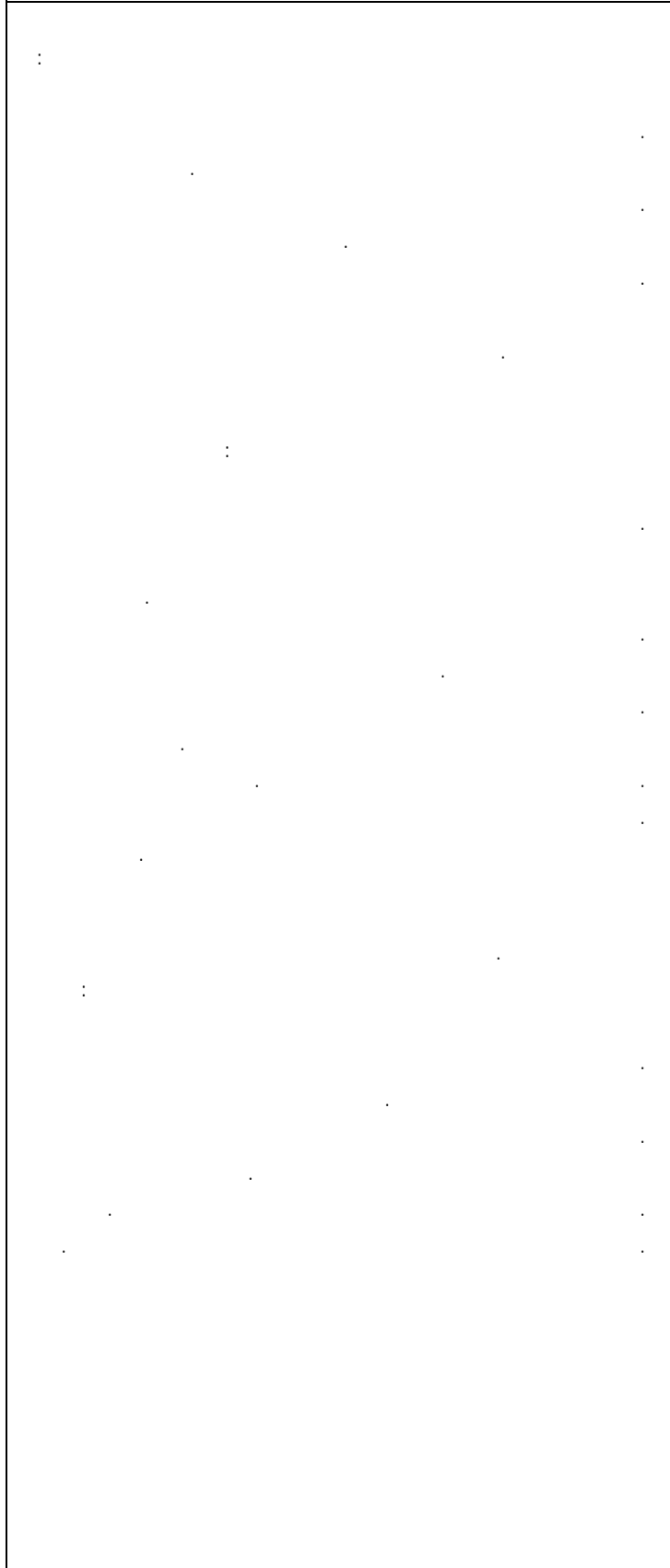
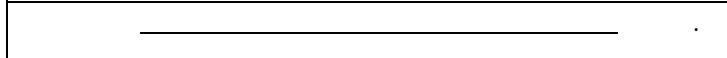
1. Developing and implementing policies, plans, procedures and internal controls, including the appointment of qualified employees at the level of senior management to implement the same.
2. Developing internal accounting and auditing systems to supervise the availability of basic requirements to combat money laundering and terrorist financing.
3. Developing ongoing training programs for specialized employees to keep them informed about new technologies in combating money laundering and to upgrade their skills to identify such operations, their patterns and the method of combating them.

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

1. Setting out in detail the above elements and the banks' or money exchangers' plans and strategies for ensuring compliance with its written policies and procedures to effectively cover AML/CTF requirements.
2. Including planned reviews and self-assessment processes to monitor effectiveness of AML/CTF controls.
3. Detailing assigned responsibilities and specific actions to be taken during the year in addition to any pending corrective actions based on audits and assessment reviews.
4. Including appropriate staff awareness and training efforts for the year.
5. The program should be prepared and reviewed on an annually basis, to reflect ongoing trends and risks of money laundering and terrorist financing in order to ensure its effectiveness.

The program should stipulate appropriately what has been done and why, in regards to the risk-based approach. Therefore, each bank or money exchanger should tailor the program policies and procedures for the AML/CTF to capture the following:

1. How the bank or money exchanger assesses the threats and risks of being used in connection with money laundering or terrorist financing.
2. How the bank or money exchanger implements the appropriate system and procedures, including due diligence requirements in the light of its risk assessment.
3. How the bank or money exchanger monitors and improves the effectiveness of its system and procedures.
4. Reporting process to senior management on the operation of its control procedures.



4.3 Know Your Customer Standards (KYC)**4.3.1 Customer Due Diligence/ Know Your Customer**

Customer Due Diligence/ Know Your Customer is intended to enable a bank or money exchanger to form a reasonable view that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. Bank's and money exchanger's procedures should include measures to:

1. Identify and verify the identity of each customer on a timely basis;
2. Take reasonable risk-based measures to identify and verify the identity of any beneficial owner;
3. Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions.

The starting point is for a bank or money exchanger to assess the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. Banks and money exchangers should determine the due diligence requirements appropriate to each customer, including the following:

1. A standard level of due diligence, to be applied to all customers.
2. The standard level being reduced in recognized lower risk scenarios, such as:
 - a. Publicly listed companies subject to regulatory disclosure requirements.
 - b. Other banks or financial institutions (domestic or foreign) subject to an AML/CTF regime consistent with the FATF Recommendations.
 - c. Individuals whose main source of funds is derived from salary, pension or social benefits from an identified and appropriate source and where transactions are commensurate with the source of funds.
 - d. Transactions involving small amounts or particular types of transactions.
3. Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.
4. An increased level of due diligence with respect of those customers that are determined to be of higher risk. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by the applicable law or regulation as posing higher risk, such as correspondent banking relationships and politically exposed persons.

When designing and implementing controls to manage and mitigate the assessed risks, under the risk-based approach, banks and money exchangers should include the following steps:

1. Managing and mitigating the identified and assessed risks, the bank or money exchanger will develop measures to verify the customer's identify; collect additional KYC information about the customer and monitor the customer's transactions.
2. Establishing control procedures to:
 - a. Introducing a customer identification program that varies the procedure in respect of customer appropriate to their assessed money laundering and terrorist financing risks.

<ul style="list-style-type: none"> b. Requiring the quality of evidence, documentary/ electronic/ third party assurance to be of certain standard. c. Obtaining additional customer information, where this is appropriate to their assessed money laundering and terrorist financing risks. d. Monitoring customer transactions/ activities. <p>3. Establishing a customer identification program that is graduated to reflect risk, involving:</p> <ul style="list-style-type: none"> a. A standard information database to be held in respect of all customers. b. A standard verification requirement for all customers. c. More extensive due diligence on customer acceptance for higher risk customers. d. Limited identity verification measures for specific lower risk customer/ product combination. e. An approach to monitor customer activity and transactions that reflect the risk assessed. <p>4. Understanding of where the customer's funds and wealth come from for customers assessed as carrying a higher risk.</p> <p>5. Developing monitoring guidelines for higher risk customers versus lower risk customers.</p>	
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<p>4.3.2 Customer Identification Process</p> <p>Article 4 of the Saudi AML Law requires financial institutions not to carry out any financial, commercial or similar operations under anonymous or fictitious names. SAMA also prohibits banks from opening numbered accounts. Banks and money exchangers must verify the identity of the client, on the basis of official documents, at the start of dealing with such client or upon concluding commercial transactions therewith in person or in proxy. Banks and money exchangers must further verify the official documents of juristic person that indicate the name of the entity, its address, name of its owners, managing directors, and other relevant data.</p> <p>Banks and money exchangers should apply the following rules, as a minimum, for appropriate customer identification:</p> <ul style="list-style-type: none"> 1. Establish valid identification by reference to proper, acceptable official documents in accordance with SAMA Account Opening Rules. 2. At the outset of the relationship or account, obtain a copy of the customer identification document and verify them against the original document. 3. Obtain SAMA approval for opening accounts or establishing relationships for any non-residents, except for GCC citizens. 4. Not to establish accounts or relationships for any non face-to-face customers (refer to SAMA Account Opening Rules), and subject all accounts to interview and identity verification. 5. Identification is not limited to customers having accounts with the bank; it should also include those who benefit from other banking/ financial services, such as credit cards, express remittances, large transfers/ transactions, foreign exchange transactions and safe deposit boxes, and should cover owners, authorized signers, powers-of-attorney, directors, trustees and partners. 6. Establish a systematic procedure for identifying customers and not to set up a relationship or process a transaction until the personal or commercial valid identity of the individual or legal entity has been established and satisfactorily verified. 7. Obtain customer personal information, such as name, address, signature, contact telephone numbers, occupation, source of funds/ income, and other 	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

information, depending on the type of customer, as stated in the SAMA Account Opening Rules.

8. Ask 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. Conduct further due diligence if there are doubts about the integrity or adequacy of previously obtained customer identification data, in which case re-verify the identity of the customer and re-assess the relationship.
10. Not to accept any transactions from walk-in customers, with the exception of permissible transactions as stated in the SAMA Account Opening Rules.
11. No new account, business relationship or transaction should be accepted, and any existing account, business relationship or transaction should be frozen, where:
 - a. Identity of the customer cannot be verified;
 - b. Identity of the beneficial owner is not known; and/or
 - c. There is a failure to obtain information on the purpose and intended nature of the business relationship.
 - In case banks or money exchangers identify any of the above cases, they should immediately report them to the SAFIU with a copy to SAMA.

4.3.3 Beneficial Owners (Natural & Legal)

Banks and money exchangers should establish the beneficial ownership for all accounts and relationships and should conduct due diligence on all principal beneficial owners identified in accordance with the following principles:

- 1. Natural Persons**
When the account or relationship is in the name of an individual, the bank or money exchanger should determine whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the customer is acting. Identity 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 purporting 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, the bank or money exchanger should understand the structure of 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, e.g., the directors and those with the power to give direction to the directors of the company.
With regards to a joint stock company, the bank or money exchanger should establish the identity of all shareholders 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 of the beneficial owners including the actual natural persons owning or controlling the entity.
In all the above cases, if a customer states that he/she is

/

()

/

%

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 on an annual basis, 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.

4.3.5 Name Checking of Designated Persons

Saudi Arabia is committed to all relevant United Nations Security Council Resolutions directed towards fighting terrorist financing and has criminalized financing of terrorism, terrorist acts and terrorist organizations, under Article 2 of the Saudi AML Law and Bylaws. 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 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, and check all transactions and transfers against these lists, to

<http://www.un.org/sc/committees/1267/consolist.shtml> :

avoid potential conflicts when conducting business with other countries' banks and entities, 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.

()

) (

4.4 Customer Risk Assessment

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 FATF's NCCTs, as explained in **Rule 5.2**;
2. High-risk businesses or customers, as explained in **Rule 4.5**;
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 at least on annual basis.

:

()

) (

(

4.5 Customer Risks

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 poses a higher risk and the potential impact of any mitigating factors on that assessment. 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:

:

4.5.1 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 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, efforts 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.

4.5.2 Walk-In Customers

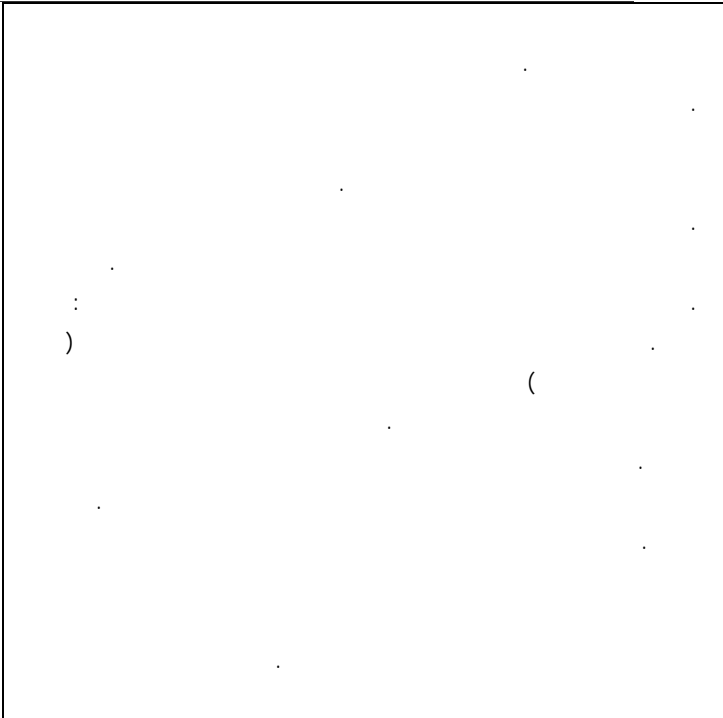
A walk-in or occasional customer is one who conducts a transaction with a bank or money exchanger but does not maintain an account or any type of relationship with the bank or money exchanger. These include residents as well as visitors on a temporary visa/ residence. As banks and money exchangers do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

- 1. Resident Non-Account Holders: 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.).
- 2. Visitors (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, banks checks, etc.
- 3. Visitors on a temporary visa/ residence, in addition, are permitted to exchange foreign currency bank notes upto SAR 7.500 per transaction per day, within the validity of the visa, but not exceeding the equivalent of SAR 60,000 in total. Amounts in excess of SAR 60,000 or equivalent should be reported to FIU with a copy to SAMA.
- 4. For the allowed transactions, a copy of the passport should be obtained including the page evidencing the visa. Other details such as home country address,

	/
	/
	()
	/

	()
	/
)
	(
	: _____
	()
	()
	: (_____)
	()
	/

- contact in Saudi Arabia and signature should be obtained.
5. In case of suspicion, the bank or money exchanger should report the transaction to FIU with a copy to SAMA, enclosing copies the passport and the transaction, and customer details.
 6. Banks and money exchangers should comply with SAMA Account Opening Rules relating to walk-in customers requirements.
 7. Incoming transfers and checks may be accepted for walk-in customers, in the following cases:
 - a. If the transfer or check is made from an account with the bank to a beneficiary (natural or legal) on any branch of the same bank, the transfer or check may be paid in cash to the beneficiary or his legal proxy.
 - b. If the transfer or check is from a local bank to another local bank within Saudi Arabia, it shall be required to be from the account of transferor to the account of the transferee.
 - c. If the transfer is received from outside Saudi Arabia in the personal name of the beneficiary, it should be paid through an account only, which may be opened by the customer upon receipt of the transfer, subject to SAMA Account Opening Rules.



4.5.3 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.

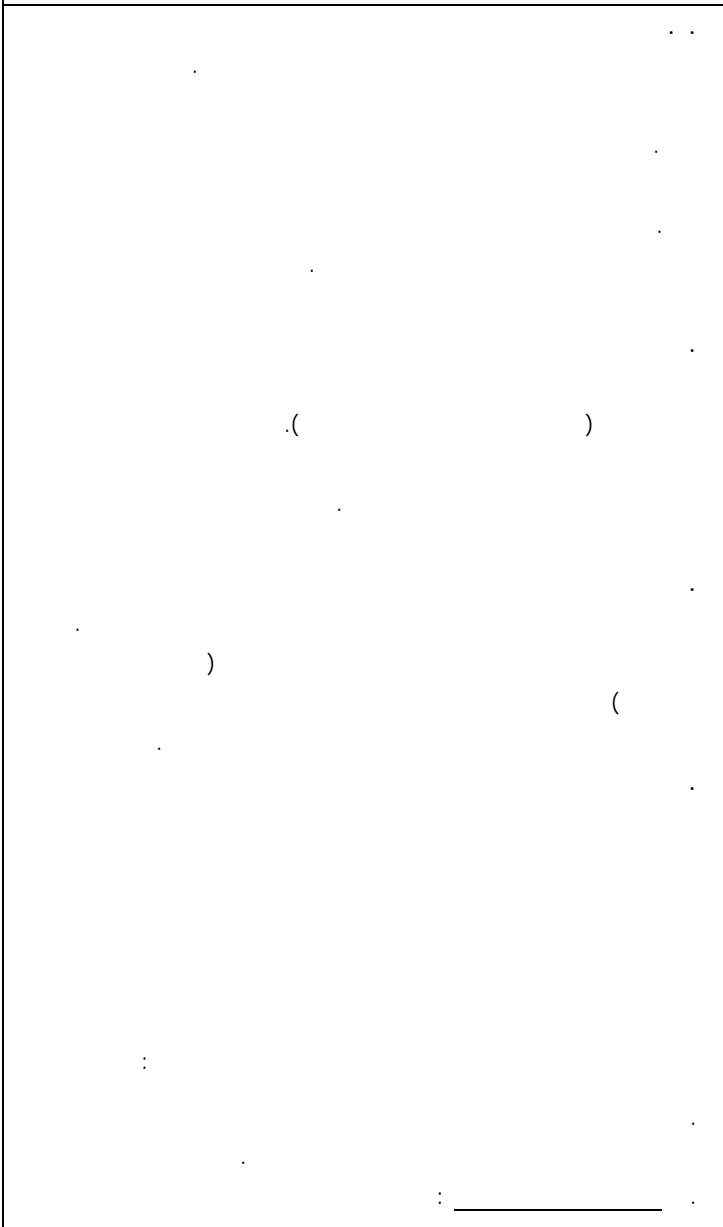
2. Corporations & Large Business Entities

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 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.
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 particular attention to cash deposits more than SAR 60,000 or equivalent.

4.5.4 Politically Exposed Persons

Individuals who are or have been entrusted with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. 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 more junior individuals in the foregoing categories.

The political influence and power of PEPs could give rise to misuse 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

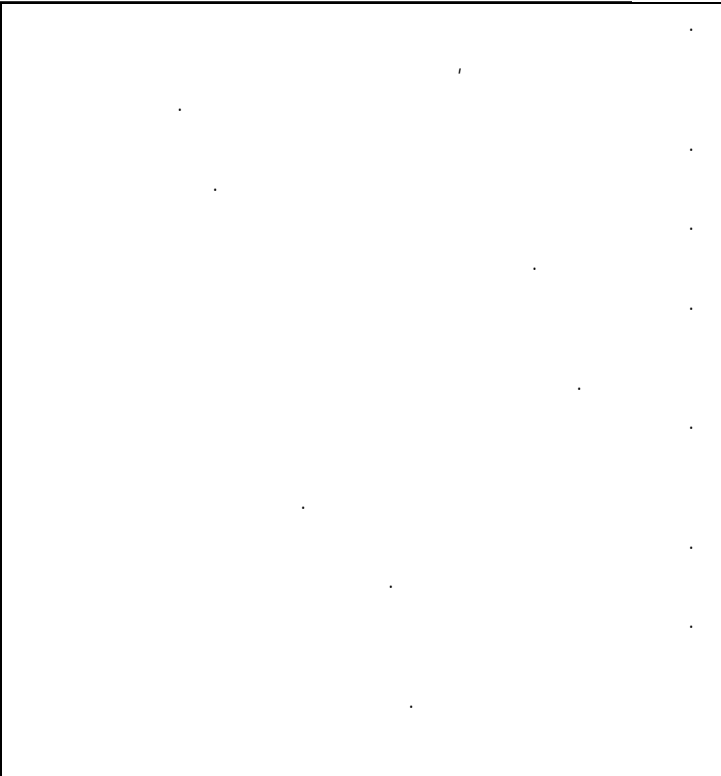
- relating to opening accounts for individuals.
2. Have policies in place to identify and categorize PEPs and related individuals for closer scrutiny. Identification of PEPs should include the existing & new customers as well as the beneficial owners.
 3. To put in place appropriate risk management systems 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 extra 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 on an annual basis and must be approved by General Manager, Managing Director, or CEO for retaining the relationship/ account.

4.5.5 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 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 risks inherent in this category of accounts. 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 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. 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



<p>transfers).</p> <p>e. References or other sources to corroborate reputation, where available.</p> <ol style="list-style-type: none"> 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 4.5.4 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 in excess of SAR 60,000 or equivalent should be scrutinized more closely. 	
<p>4.5.6 Charity & Non-Profit Organizations</p> <p>Charity or non-profit organization 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.</p> <p>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. When dealing with accounts, relationship or transactions of any charity organizations, banks and money exchangers should observe the following:</p> <ol style="list-style-type: none"> 1. Not to open account or set up a relationship for any charity organization (local or international) without SAMA's prior written approval and without 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 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 with the prior written approval from competent authorities through SAMA. This is regardless of whether the funds 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 with a copy to SAMA. 7. To freeze any transaction and immediately report the matter to FIU with a copy to SAMA, 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. 	<p>()</p> <p>()</p> <p>()</p>

<p>9. Not to allow any of their customers to transfer funds in favor of any known charity organizations outside the Kingdom of Saudi Arabia.</p> <p>10. In compliance with the FATF SR 7 on anti-terrorist financing, to provide the remitter's name, address and account number for all outgoing transfers.</p>	
<p>4.5.7 Trustees, Nominees & Intermediaries Accounts</p>	
<p>1. Trustee & Nominee Accounts</p> <p>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:</p> <ol style="list-style-type: none"> 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 that person. 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 nominee shareholders or shares in bearer form; obtain satisfactory evidence of the identity of beneficial owners of all such companies; and monitor the identity of material beneficial owners and hold such bearer shares in their custody to prevent the shares changing hands to unknown parties without the bank's knowledge. <p>2. Intermediaries' Clients Accounts</p> <p>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 (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.</p> <p>These types of accounts are potentially vulnerable to the layering of laundered funds subsequent to the placement phase. Specific vulnerable activities include:</p> <ol style="list-style-type: none"> 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. <p>Banks should have procedures in place and ensure the following:</p> <ol style="list-style-type: none"> 1. The intermediary is registered and regulated. 	

<ol style="list-style-type: none"> 2. Perform due diligence on the intermediary itself and the account should be classified as High Risk. 3. Verify and be satisfied with the intermediary's reputation and integrity. 4. Establish that the intermediary has in place a sound documented due diligence process, including KYC and identification requirements, and activity monitoring for its customers and beneficial owners, which is satisfactory to the bank. 5. Establish that the intermediary 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 intermediary 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 intermediary 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 beneficial owner, all beneficial owners 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 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. 	
<p>4.5.8 Insurance Companies Accounts</p> <p>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 although its vulnerability is not regarded to be as high as for banking sector.</p> <p>As insurance companies deal with their own customers, banks should exercise extra due diligence on these accounts, and, in addition to SAMA Account Opening Rules requirements, banks should have procedures and controls in place to implement the following:</p> <ol style="list-style-type: none"> 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.

4.5.9 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 excessive 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 as strong as 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. Banks should 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.

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 in addition to the referrals received. Such due diligence should include full verification of the customer's identification and information, including beneficial owners, comprising the following steps:

1. Banks must take all reasonable steps to recognize suspicious transactions. This should require banks to have a reasonable understanding of the normal character 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.

<p>g. The certification should be either renewed or confirmed by the correspondent bank every three years.</p>	
<p>4.6 <u>Monitoring Customer Activity</u></p>	
<p>4.6.1 Monitoring Process</p> <p>Article 6 of the Saudi AML Law requires all financial institutions to 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.</p> <p>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.</p> <p>Risk-based approach monitoring allows banks and money exchangers to create thresholds monetary value below which an activity will not be reviewed. Thresholds used for this purpose should be reviewed on a regular basis to determine capability with the risk levels established. Banks and money exchangers should also assess the adequacy of any systems and processes on a periodic basis.</p> <p>Banks and money exchangers should consider using an automated monitoring system (especially for those with large volumes of customer transactions) to facilitate the monitoring process through exception reports and alerts 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.</p> <p>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:</p> <ol style="list-style-type: none"> 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. 	

All the above may indicate that funds are being laundered through the account. The background and purpose of such transactions should be examined as far as possible and documented in writing, and suspicious transactions should be reported in writing to FIU with a copy to SAMA.

When applying risk-based approach for terrorist financing, the following points should be considered:

1. Transaction amount is not a factor on risk determination.
2. Focus is given for particular individuals, organizations and countries.
3. Before applying risk-based approach, banks and money exchangers should identify a more comprehensive set of indicators of the method and techniques used for terrorist financing, which can then be factored into strategies to assess terrorist financing risk and devise controls to mitigate such risk.

4.6.2 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. Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and additional customer due diligence information obtained;
6. Considering whether further improvements of the monitoring process is required (staff training, enhancing the monitoring system parameters, strengthening controls for more vulnerable products/ services);
7. Applying increased levels of monitoring to particular relationships;
8. 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.
9. 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 from the customer, and re-assessing the relationship.

4.6.3 Transaction Monitoring Threshold

Transaction monitoring threshold of SAR 60,000 or equivalent should be applied for all types of accounts and relationships. This threshold is applicable to a single transaction as well as an aggregate of transactions within a month. Banks and money exchangers, depending on satisfactory customer profiling, can apply product-related threshold limits that are consistent with the profile of the concerned customer.

4.7 Suspicious Transaction**4.7.1 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 Bylaws and SAMA Rules require banks and money exchangers to file Suspicious Transaction Report (STR) once a suspicion has been formed.

The risk-based approach should be useful in identifying suspicious activity in the following manner:

1. Directing additional resources at those areas a bank or money exchanger has identified as higher risk;
2. The depth of the investigation process could vary depending on the risk identified;
3. Bank and money exchanger will utilize information provided by authorities to inform its approach for identifying suspicious activity;
4. Bank or money exchanger should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

The AML Law and Bylaws apply not only to offenders but also to banks or money exchangers and their employees who participate in those transactions, if the employees concerned are aware that the fund is criminally derived. 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 Article 2 of the Saudi AML Law to have the requisite knowledge. However, Articles 21 and 25 of 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 acted in bad faith to hurt the involved person.

Banks and money exchangers reporting policy should mandate employees to do the following:

1. If an employee suspects that a money laundering or terrorist financing 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. The reporting of suspicious transactions should also include any attempted transactions, that is those transactions which have been identified as suspicious but prevented before processing.
3. Banks and money exchangers should make available, to the appropriate authorities all documents, statements and related transactions where applicable subject to SAMA's approval. Banks and money exchangers must cooperate fully with the local authorities.
4. All documents, reports and information relating to investigated cases, even if not reported to the authorities, should be maintained by the bank and money exchanger for record purposes.
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 notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith.

4.7.2 Reporting Requirements

Under Article 7 of the AML Law, financial institutions are required to inform, provide relevant information and file Suspicious Transactions Reports (STR) to FIU, comprising a detailed report including all available information and supporting documentation on the parties involved. A copy of the report should also be sent to SAMA. Reporting to FIU shall be done using the STR form adopted by FIU. Banks and money exchangers should follow the reporting process and format as described in the Saudi AML Law and Bylaws, as follows:

1. Names of suspected individuals/ entities, their identifications, 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.

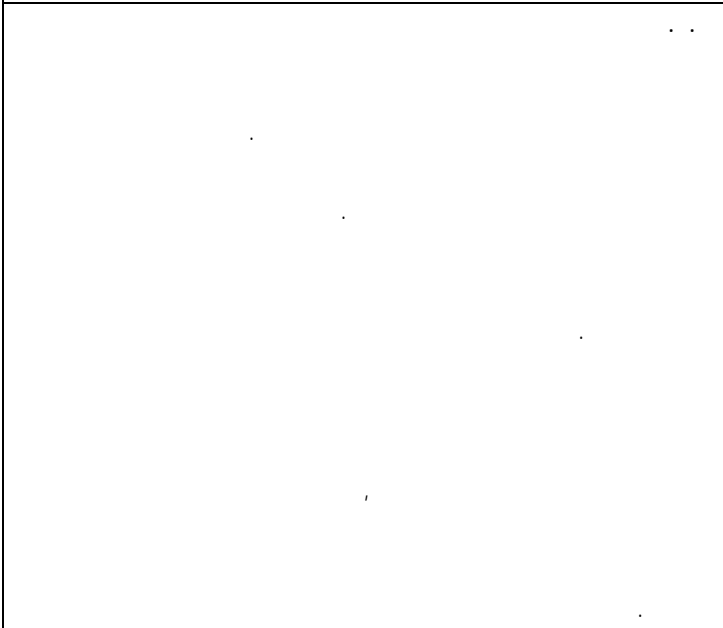
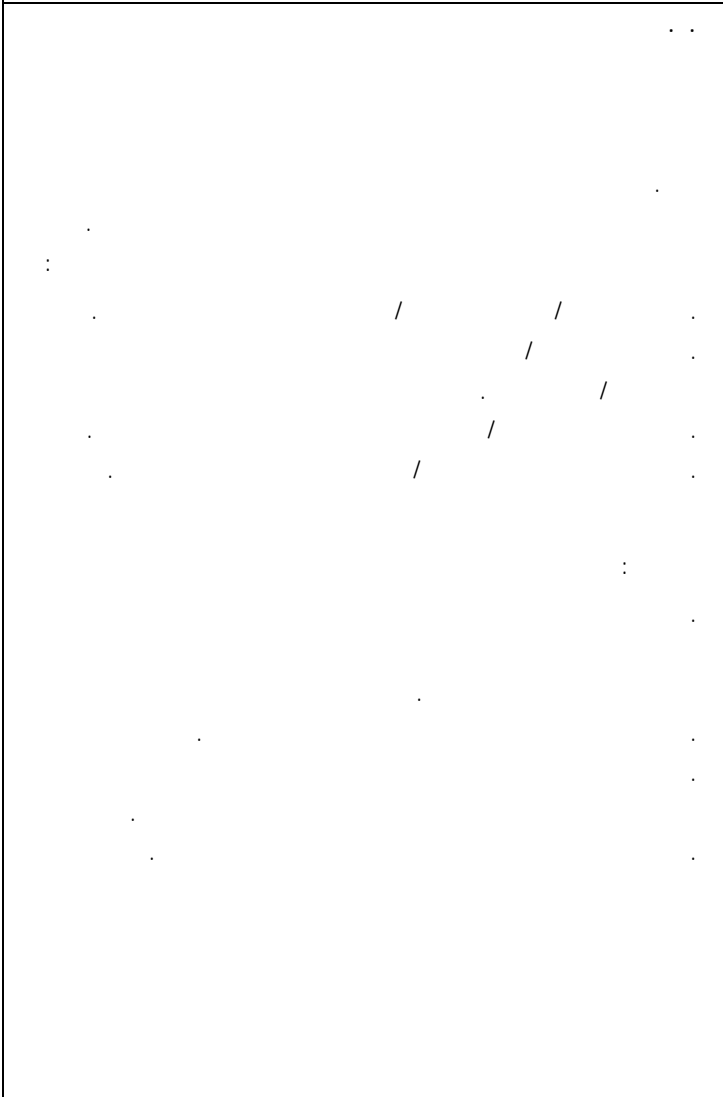
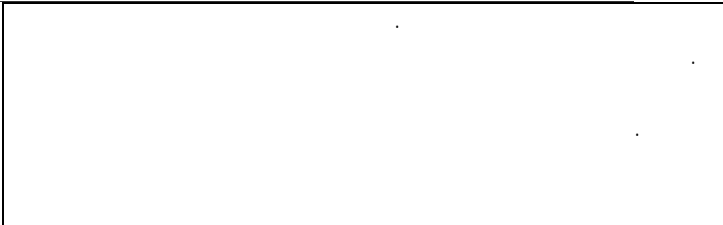
Banks and money exchangers should adhere to the following steps for submission of the STRs:

1. Prepare and 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. Send the original suspicious report, with the supporting documents, to the FIU;
3. Fax a copy of the above report, and then mail a hard copy, to the Money Laundering Control Unit, Banking Inspection Department, Saudi Arabian Monetary Agency;
4. Retain a copy of the report and its attachments for records and future reference.

4.7.3 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 with a copy to SAMA.

Article 9 of 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. Under Article 8 of 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 banking laws and regulations.



4.7.4 Money Laundering Control Unit (MLCU)

Banks and money exchangers must establish an independent and dedicated function to handle the money laundering control and reporting activities. For small-sized banks and money exchangers, with five branches and less, as a minimum, this function can be handled by the designated Compliance Officer for the bank or money exchanger. For large banks and money exchangers with more than five branches, an independent and dedicated Money Laundering Control Unit, should be established with adequate staff who should be all Saudis. In both the above situations, the designation of the MLCU staff or Compliance Officer to handle the money laundering 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 financial banking 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 and various internal departments of the bank or money exchanger, which should entail or augmented with the collection of information, analysis of the data collected, and making necessary decision for taking appropriate action, which should be documented in writing.
3. Reporting to the Saudi Financial Intelligence Unit (SAFIU), and providing a copy to SAMA, when suspicions have been determined, in accordance with established requirements, supported by a detailed technical report on the suspected case, and within the regulatory reporting timeframes.
4. Developing automated programs for controlling money laundering activities and updating the indicators that reflect existence of suspicious money laundering 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 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

<p>avoided and dealt with.</p> <p>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.</p> <p>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.</p> <p>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.</p>	
<p>4.8 Internal Controls</p>	
<p>4.8.1 Internal Control Procedures</p> <p>Under Article 10 of the Saudi AML Law, financial institutions are required to establish and maintain internal control procedures to prevent their institutions from being used for purposes of money laundering and terrorist financing.</p> <p>In order to have an effective risk-based approach, the risk-based process must be imbedded within the internal controls of the banks or money exchangers. 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. Strong senior management leadership and engagement in AML/CTF is an important aspect of the application of the risk-based approach. 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.</p> <p>In addition to other compliance internal controls, the nature and extent of AML/CTF controls will depend upon a number of factors, including:</p> <ol style="list-style-type: none"> 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 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. <p>The framework of internal control procedures should:</p> <ol style="list-style-type: none"> 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 	

<p>for managing the compliance function.</p> <ol style="list-style-type: none"> 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. 	
<p>4.8.2 Assessment of Internal Controls</p> <p>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.</p> <p>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.</p>	
<p>4.9 Staff Training & Hiring</p>	
<p>4.9.1 Staff Training & Awareness</p> <p>Article 10.c of the AML Law and Bylaws mandate all financial institutions to develop training programs to educate their employees and enhance their understanding of KYC procedures, money laundering and terrorist financing risks, trends and preventive methods. As employees become familiar with such activity, they can play an effective role in combating money laundering and terrorist financing through prevention and detection measures.</p> <p>Banks and money exchangers should therefore provide their employees with appropriate and proportional training, and ongoing awareness, with regard to money laundering and terrorist financing. A bank's or money exchanger's commitment to having successful controls relies 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.</p> <p>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:</p>	

<ol style="list-style-type: none"> 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 should be educated in the importance of AML/CTF policies while regular 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. <p>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 Articles 2, 3, 9, 17, 18, 21 and 25 of the Saudi AML Law.</p>	
<p>4.9.2 Staff Hiring & Appointment of Senior Positions</p> <p>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.</p> <p>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.</p>	
<p>4.10 Record Keeping & Retention</p>	
<p>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.</p> <p>Article 5 of 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.</p> <p>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:</p>	

1. Primary Records		
<u>Type of Record</u>	<u>Retention Form</u>	<u>Retention Period</u>
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		
<u>Type of Record</u>	<u>Retention Form</u>	<u>Retention Period</u>
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		
<p>Product or service risks are the potential risks inherent in the 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.</p>		
5.1.1 Cash		
<p>Physical cash is often the ideal and most commonly used method of value transfer for criminal activities, including money laundering and terrorist financing, simply because it 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</p>		

	/	/
	:	:
	-	-
	-)
		(...)
)
		(...
		/
	/	
	/	
	/	
	/	
		/
		()

so there will often be a high level of cash deposits associated with some of these accounts.

1. Cash Transactions

SAMA has been engaged 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 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

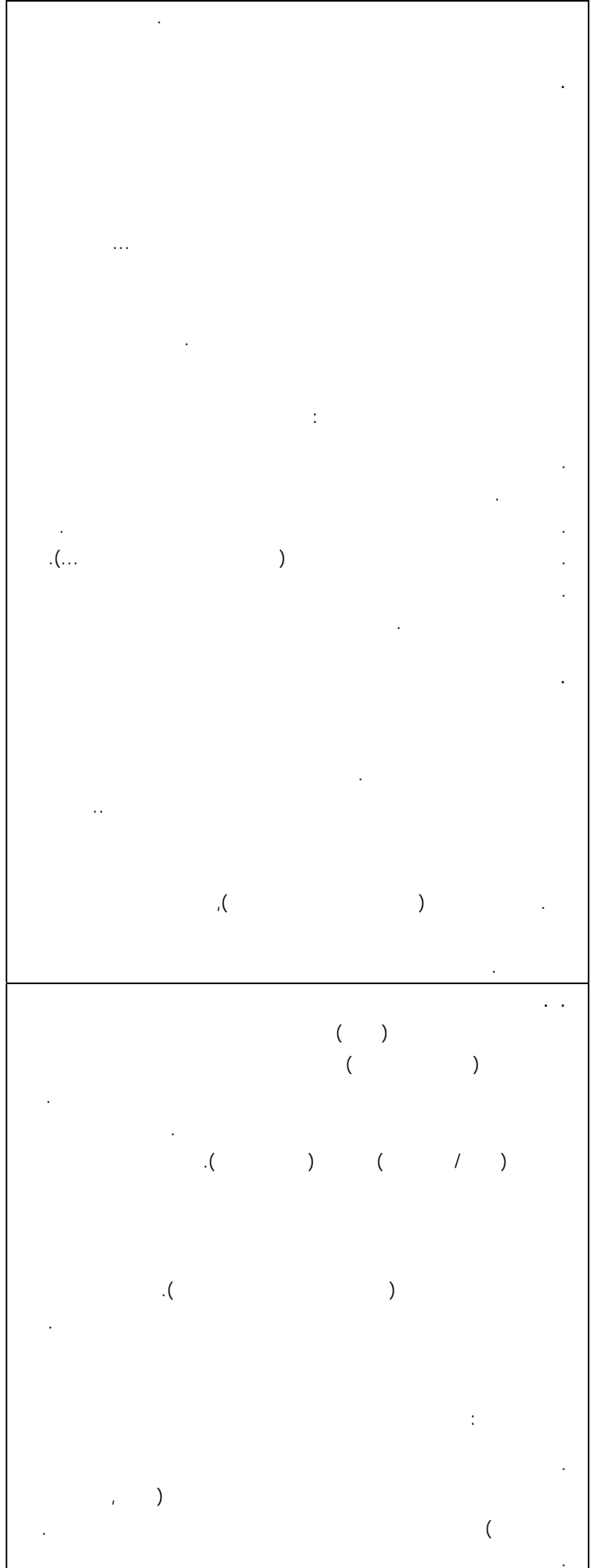
In accordance with Saudi AML Law Article 14 and related Bylaws, banks and money exchangers should comply with the requirements relating to cross-border transportation of cash coming into or going out of Saudi Arabia for their own use. The cash may be carried by banks and money exchangers or through cash transportation firms by way of cargo, postal parcels, air shipments, 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 more than SAR 60,000 or equivalent (or equivalent in foreign currencies), in accordance with SAMA Rules for Cash Transportation for Banks and Money Exchangers issued on 29 April 2007.

5.1.2 Wire Transfers

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. For all outgoing cross-border transfers, ensure to include full and accurate originator information (name, address and account number) on the funds transfers and related messages that are sent, and the information should remain with the transfer or related message in the



- payment chain.
2. For incoming cross-border transfers, ensure they contain full originator information (name, address and account number) for transfers of SAR 5,000 and above or equivalent and verify if needed. In case the incoming transfer does not contain complete originator information, the bank or money exchanger should hold the transfer and contact the remitting bank for the missing information. Failure to obtain the missing information may be considered as a cause for suspicion and reassessing the relationship with the remitting bank.
 3. 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.
 4. Retain all physical and system records of all funds transfers in accordance with the prevailing record retention periods.
 5. Exercise extra due diligence for funds transferred from or to NCCTs as periodically defined by FATF.
 6. Conducting KYC/ due diligence on the remitter/ originator is the responsibility of the remitting bank or money exchanger, whether foreign or local.
 7. Conduct a name check of the parties involved in the transfer (originator, beneficiary, intermediary bank) as per requirements in Rule 4.3.5 of this document.
 8. Exercise extra the required due diligence when processing transfers relating to PEPs.
 9. Not to accept any incoming or outgoing transfers outside Saudi Arabia, for any charity organizations, except with the prior written approval from competent authority through SAMA.
 10. When implementing any new electronic fund transfer and payment systems, ensure the systems 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 relationship with the bank or money exchanger.

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 traditionally operate outside the regulated conventional financial sector. The very features (efficiency, anonymity and lack of paper trail) which make alternative remittance system attractive to legitimate customers (mainly expatriates remitting money to relatives in home countries), also make the system conducive 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 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

()

()

)

(

/

/

....

)

)

(

.Hundi " " " " " "

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

(Hundi)

5.1.4 Money Exchanging

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, specifically indicating that they are allowed to conduct such activity. However, due to the nature of their business, these entities may be engaged in offering remittance service to the community. Therefore, they should be categorized as High Risk for an extra customer due diligence and closer scrutiny.

()

//

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, personal computers, 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 internet is growing considerably, with increasing range of services becoming available, including savings and deposit 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 anonymity (usage and funding), rapid transaction speed, and its wide geographic availability.

To prevent these risks, banks and money exchangers should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. 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, in which case the banks and money exchangers will have electronic records of the customers including identification and other personal information.

/)
.(

)

(

)

(

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.

..

)

) (/

) (/

.(/

:

)

.()

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 by other credible sources (e.g., FATF-NCCTs) due to one factor or a combination of factors, as determined by UN or FATF, such as lack of appropriate AML/CTF laws, regulations and other measures; providing funding or support for terrorist activities; or having significant levels of financial criminal activities.

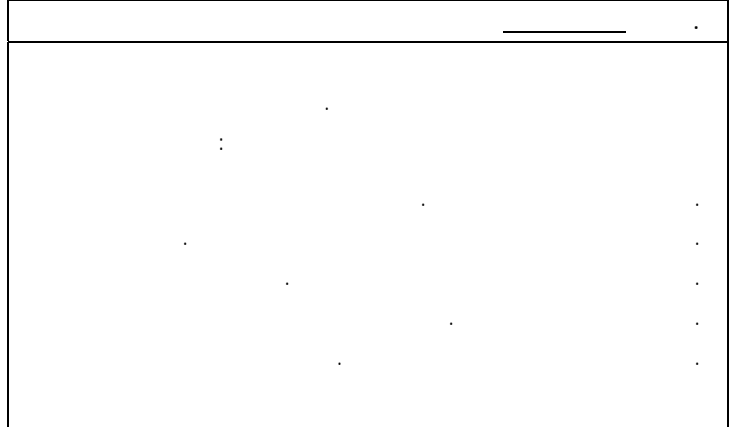
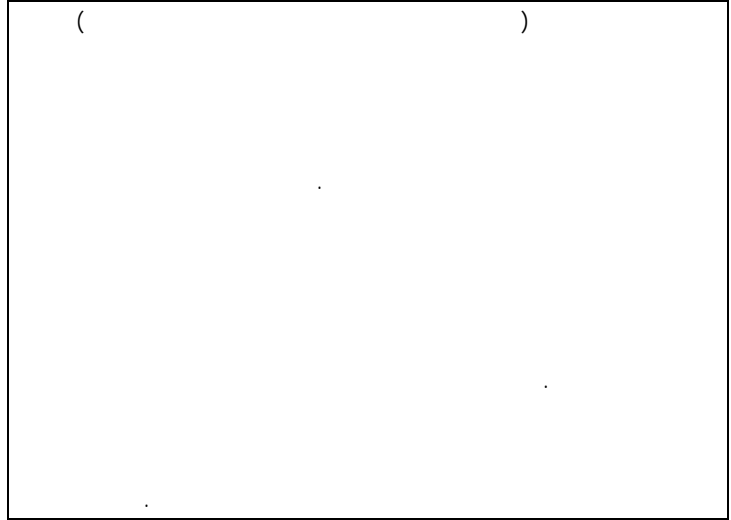
Banks and money exchangers should exercise additional due diligence and give special attention to business relations and transactions with persons, including companies and banks that are located in or whose geographical spheres of business activities are in jurisdictions that do not adequately apply FATF recommendations.

Whenever necessary, SAMA will issue instructions to banks and money exchangers about certain countries and on how transactions relating to these countries should be treated.

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.



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 bank account, credit card, express remittance service, 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.		
Extra 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, charity organizations, and for other types of customers categorized as high risk by the bank/ME.		
Financial Action Task Force (FATF)	Financial Action Task Force, the main ruling international body for overseeing 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.		

<p>Money Exchanger (ME)</p>	<p>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.</p>		
<p>Nominee</p>	<p>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.</p>		
<p>Non-Cooperative Countries & Territories (NCCT)</p>	<p>FATF publishes reports on countries which do not cooperate adequately in the fight against money laundering, known as Non-Cooperative Countries & Territories. 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 the NCCT list, and exercise extra due diligence.</p>		
<p>Payable-Through Account</p>	<p>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</p>		
<p>Shell Bank</p>	<p>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.</p>		
<p>Source of Funds</p>	<p>Source of funds is the activity which generates the funds for a relationship, e.g., a customer's occupation or business activities.</p>		
<p>Source of Wealth</p>	<p>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.</p>		
<p>Subsidiaries</p>	<p>This refers to majority owned subsidiaries of a bank or money exchanger, inside or outside the country.</p>		

<p>Suspicious Transaction</p>	<p>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.</p>		
<p>Trustee</p>	<p>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.</p>		
<p>Unusual Transaction</p>	<p>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.</p>		

7. Appendices				
<u>SN</u>	<u>Topic</u>	<u>Related Website Address</u>		
A	Saudi AML Law & Bylaws	www.sama.gov.sa		
B	FATF 40 Recommendations on AML	www.fatf-gafi.org/document	()	
C	FATF 9 Special Recommendations on CTF	www.fatf-gafi.org/document	()	
D	FATF Member Countries & NCCTs	www.fatf-gafi.org/pages	()	
E	Basel Committee Standards	www.bis.org/publ		
F	UN Security Council Resolutions	www.un.org/sc/committees	-	
G	Other Useful Resources & Links	www.menafatf.org		
		www.customs.gov.sa/Customs		

—

	/ /
	/ / :

)
				(

				/
/				
	/			

		/		

:

:

APPENDIX (8)

Suspicious Transaction Report

Confidential

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

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

<u>Report Contents</u>				
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				

<u>Beneficiary</u>				
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:

10.Red Flag Indicators	
<p>A. <u>Key Indicators of Regulatory & Legal Weakness (High Risk Geographies)</u></p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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 of Non-Cooperative Countries & Territories (NCCT). Since the list keeps on changing, reference should be made to FATF website.</p>	

<p>B. <u>Businesses Prone to Money Laundering Activities (High Risk Businesses)</u></p> <p>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.</p> <p>The following guidance provides an insight into what those businesses might be.</p>	
<p>Shell Corporations</p> <p>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.</p> <p>Types of businesses covered: Potentially any business.</p> <p>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.</p>	
<p>Financial Institutions (Non-Bank)</p> <p>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.</p> <p>Types of business covered: Money Exchangers.</p> <p>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.</p>	
<p>Travel Agencies</p> <p>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.</p> <p>What to look for: Payments to countries on the "FATF NCCT List" 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.</p>	
<p>Import/Export Businesses</p> <p>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).</p>	

<p>Precious Commodities</p> <p>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.</p> <p>Types of business covered: Precious Metals, Jewel Store; Antique Shops and Fine Art Galleries.</p> <p>What to look for: Trading patterns with countries on the "FATF NCCT List" not normally associated with the commodity in question; unusual fluctuations in turnover or types of financial instruments used.</p>	
<p>Cash Driven Businesses</p> <p>The types of business that normally accept cash are useful to the launderer at the placement stage, and could be used for layering purposes.</p> <p>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.</p> <p>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.</p>	
<p>Offshore Financial Services</p> <p>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.</p> <p>Type of businesses covered: Trust Companies; Commodity Traders, Financial Advisers.</p> <p>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 countries on the "FATF NCCT List"; investing in instruments that carry anonymity (e.g. bearer bonds) when uneconomic to do so.</p>	
<p>Charitable or Non-Profit Organizations</p> <p>When opening an account for a Charitable or Non-profit Organization, valid authorization from the appropriate government agencies and SAMA must be obtained.</p>	
<p>C. <u>Key Indicators of ML/TF Transactions & Activities (High Risk Products/Services)</u></p> <p>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.</p> <p>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.</p>	
<p>General Indicators</p> <ul style="list-style-type: none"> • A transaction whose general form is indicative of illegitimate or 	

<p>unknown purposes.</p> <ul style="list-style-type: none"> • Existence of movements in the customer's account not related to his activities such as: <ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> • • - - - - - - - -
<p>Teller Transactions</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • • • • • • •
<p>Bank Accounts</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • • • • • • • • • •
<p>Credit Activities</p> <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • • •

<p>a loan or credit facilities.</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • • • • • •
<p>Drafts</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • • • • • •
<p>Customer</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • • • • • • •

:

// /

/

//

:

()

// /

//

:

.

-

.

-

:

() ()

.

() ()

.

() ()

.

() ()

.

.

() ()

() ()

.

:

.

()

.

()

.

:

.

.

.

.

.

.

.

.

.

()

.

(%)

.

(%)

.

(% .)

(%)

.

.

(%) , ()

(%)

.

.

.

(%)

(%)

.

.

:

(

(

.

(

:

.

()

()

.

()

:

(

(

.

(.)

.

:

,

.

.

.

,

()

.

.

.

.

(%)

(%)

.

.

.

.

.

()

.

(%)

.

:

.

()

()

.

.

()

()

.

()

.

.

:

(

.

.

(

.

.

.

%

.

%

.

.

'

'

'

.

.

.

.

:

.

.

.

.

.

.

.

.

.

.

.

.

:

.()

.

.

- .

.

/

.

.

.

.

:

()

.

()

.

• ()

• ()

•

'
(, ,)

•

•

•

•

•

•

'

•

•

•

•

(. .)

•

•

.

.

.

.

:

//

/

/

//

//

//

//

/

//

/

()

:

:

-

:

:

-

.

-

:

-

()

.

()

.

()

.

()

.

()

.

()

.

()

.

()

.

()

.

-

:

-

.

()

()

//

//

.

()

.

()

.

()

//

/

.

-

.

-

.

-

.

-

.

-

.

:

-

:

-

.

-

:

()

()

()

()

.

()

()

()

.

-

.

:

:

-

:

:

()

.

(/)

:

(/)

.

-

.

-

.

(/)

.

(/)

.

(/)

:

()

.

(/)

(/)

.

(/)

.

. (/)

(/)

. (/)

: ()

. (/)

. (/)

. (/)

. (/)

: ()

. (/)

. (/)

. (/)

- -

.

. ()

()

.

()

-

:

:

()

()

()

()

:

:

-

-

.

-

-

-

.

-

-

.

-

.

-

.

-

.

-

.

-

.

..

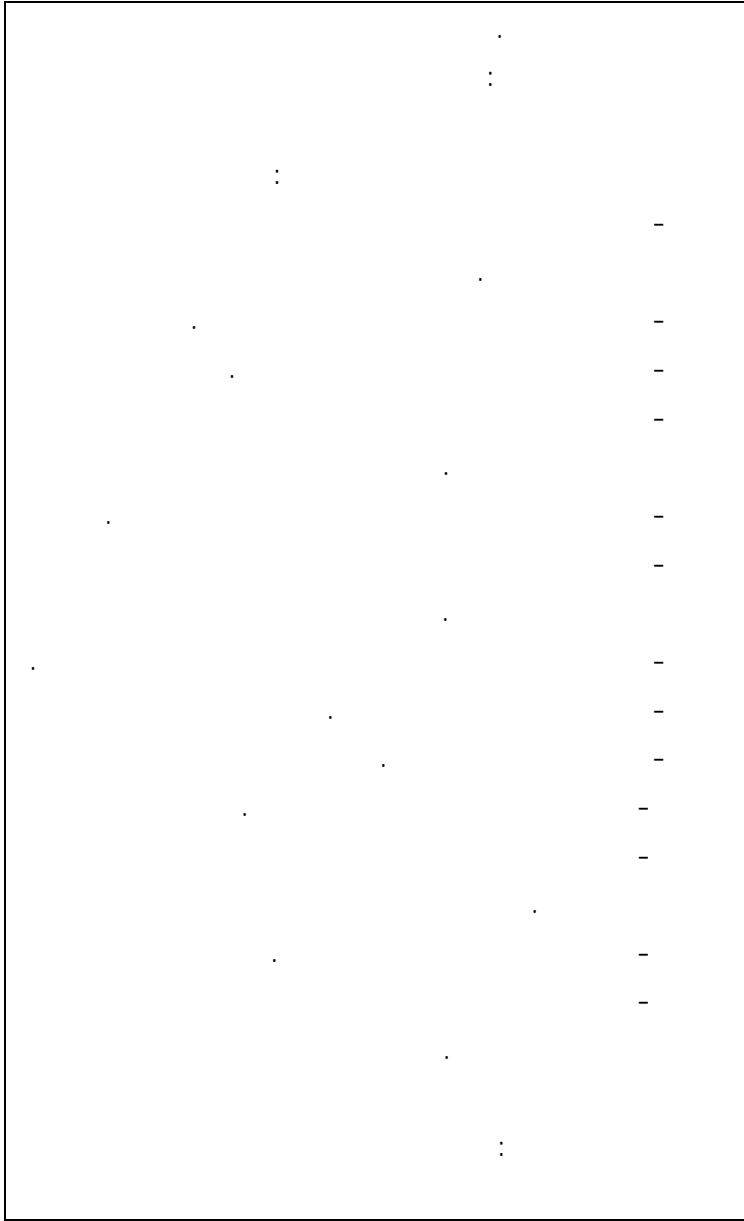
:

:	()	:)	
.	/	():	
.	()):		
:		(
/	-	()	(
.	//	:)	
/	-	()	(
.	//	:)	
/	-	(
.	//	()		
.	// /			
.	//			
.	// //			
):	

<p>()</p> <p>. ()</p>		<p>()</p> <p>:</p> <p>(</p> <p>()</p>		
<p>()</p>	<p>):</p> <p>(</p> <p>):</p> <p>(</p> <p>:</p> <p>,</p> <p>,</p> <p>(</p>	<p>):</p> <p>() (</p> <p>):</p> <p>(</p> <p>()</p>		
	<p>):</p> <p>(</p> <p>)"</p> <p>"</p>	<p>):</p> <p>): () (</p> <p>(</p>		

<p style="text-align: center;">// /</p>	<p style="text-align: center;">): (</p>	<p style="text-align: center;">): () () ()</p>		
<p style="text-align: center;">:</p> <p style="text-align: center;">:</p> <p style="text-align: center;">:</p> <p style="text-align: center;">-</p> <p style="text-align: center;">-</p> <p style="text-align: center;">-</p> <p style="text-align: center;">()</p> <p style="text-align: center;">:</p> <p style="text-align: center;">-</p> <p style="text-align: center;">-</p> <p style="text-align: center;">()</p> <p style="text-align: center;">:</p>		<p style="text-align: center;">):</p> <p style="text-align: center;">(</p> <p style="text-align: center;">()</p> <p style="text-align: center;">)</p> <p style="text-align: center;">() (</p>		

<p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p>				
----------------------------------------------------------------------------------------------------------	--	--	--	--

				
------------------------------------------------------------------------------------	--	--	--	--

<p> - - : : - - . </p>				
	<p> (): () </p>	<p>): () () </p>		
<p> / , / / </p>	<p>): () </p>	<p>):): () () </p>		

<p style="text-align: center;">// /</p> <p style="text-align: center;">// /</p>	<p>) :</p> <p>(</p>	<p>) :</p> <p>() (</p>		
<p>:</p> <p>- :</p> <p>-</p> <p>:</p> <p>-</p> <p>-</p> <p>-</p> <p>.</p>	<p>) :</p> <p>, ,</p> <p>, ,</p>	<p>) :</p> <p>(</p> <p>. ()</p>		

	<p>): : .): (): () </p>	<p>): (()): (): () () </p>		
<p> . // / </p>		<p> . : .): . .(</p>		
	<p>): (</p>	<p>): .(</p>		

):			
" ()	()"		
" "		"(())"		
" "		"(()		
):	:		
	():	" . , , , , "		
	(() (
):		
	() (() (
/ /):):		
()	:	(
	:			
	:			
	.(

. () ()): .		
: / :	:	() ():		
: . // :	.	() ()		
. : ()	.			

<p>: .</p> <p>()</p> <p>-</p> <p>-</p> <p>-</p> <p>:</p> <p>-</p> <p>-</p>				
-----------------------------------------------------------------------------	--	--	--	--

<p>()</p> <p>.</p> <p>()</p> <p>()</p> <p>:</p>				
----------------------------------------------------	--	--	--	--

<p>- . -</p> <p>. - :</p> <p>()</p> <p>(.) (.)</p> <p>/ /</p>				
--------------------------------------------------------------------	--	--	--	--