CENTRAL BANK OF YEMEN
HEAD OFFICE

البنك المركزي اليمني
المركز الرئيسي

Date 16/3/2021
No CBY/S/437/2021

التاريخ: / /
الرقم: .....

قطاع الرقابة على البنوك

منشور دوري رقم (2) لسنة 2021م

موجه إلى كافة البنوك وشركات / منشآت الصرافة العاملة في الجمهورية

الأخ/رئيس مجلس الإدارة/ المدير العام/ المدير الإقليمي **المحترم**

بنك/.....

الأخ/مدير الشركة /مالك المنشاة **المحترم**

شركة/منشاة/.....

بعد التحية:

الموضوع: ملحق للمنشور الدوري رقم (1) لسنة 2012م والمنشور الدوري رقم (1) لسنة 2013م والمنشور رقم (8) لسنة 2014م بشأن التعليمات والضوابط الرقابية للبنوك وشركات /منشآت الصرافة بشأن مكافحة غسل الأموال وتمويل الارهاب

بالإشارة إلى الموضوع أعلاه وبناء على توجيهات الأخ المحافظ، واستناداً للقانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب ولائحته التنفيذية رقم (226) لسنة 2010م وتعديلاتهما، والحاقاً للمنشور الدوري رقم (1) لسنة 2012م والمنشور رقم (1) لسنة 2013م والمنشور رقم (8) لسنة 2014م؛ بشأن التعليمات والضوابط الرقابية لمكافحة غسل الأموال وتمويل الإرهاب، وفي اطار سعي البنك المركزي لتحديث التعليمات بما يتوافق مع المعايير الدولية في هذا الخصوص؛ يتم الالتزام والوفاء بالمتطلبات الواردة في هذا المنشور.

أولا: الهدف من هذه التعليمات

تهدف هذه التعليمات إلى:

- التأكد من امتثال البنوك وشركات/منشآت الصرافة بالتقيد بأحكام القانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب ولائحته التنفيذية رقم (226) لسنة 2010م وتعديلاتهما.
- حماية القطاع المالي والمصرفي من عمليات غسل الأموال وتمويل الإرهاب وذلك من خلال امتثال البنوك وشركات/منشآت الصرافة بتطبيق السياسات والأنظمة والإجراءات والضوابط واللوائح والمبادئ التي تكفل اكتشاف ومنع أنشطة غسل الأموال وتمويل الإرهاب والتبليغ عنها طبقاً لأحدث المعايير الدولية.

- حماية البنوك وشركات/منشآت الصرافة من العمليات غير القانونية، ومنع استغلالها كقنوات لتمرير العمليات والمعاملات غير المشروعة التي قد تنطوي على غسل الأموال أو تمويل الإرهاب وأي أنشطة غير مشروعة أخرى.
- تعزيز سلامة القطاع المصرفي وحماية سمعته ونزاهته وبما يكفل حماية عملائه.

ثانيا: نطاق تطبيق المنشور:

جميع البنوك وشركات /منشآت الصرافة العاملة في الجمهورية اليمنية كلاً فيما يخصه.

ثالثا: التعاريف

مع عدم الإخلال بالتعاريف الواردة في القانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب ولائحته التنفيذية رقم (226) لسنة 2010م وتعديلاتهما، ولأغراض هذا المنشور يقصد بالكلمات والعبارات التالية حيثما وردت المعاني المبينة قرين كل منها:

القانون: القانون رقم (1) لسنة 2010م بشأن مكافحة غسل الاموال وتمويل الإرهاب وتعديلاته.

اللائحة التنفيذية: اللائحة التنفيذية للقانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاتها.

اللجنة: اللجنة الوطنية لمكافحة غسل الأموال وتمويل الإرهاب.

الوحدة: وحدة جمع المعلومات المالية.

الأموال: الأصول أياً كان نوعها مادية أو غير مادية، منقولة أو غير منقولة، التي يتحصل عليها بأي وسيلة كانت، والوثائق أو الصكوك القانونية أياً كان شكلها بما في ذلك الشكل الإلكتروني أو الرقمي والتي تدل على ملكية تلك الأموال أو مصلحه فيها.

وتشمل على سبيل المثال العملات بجميع أنواعها المحلية والأجنبية، والأوراق المالية والتجارية والاعتمادات المصرفية والشيكات السياحية والحوالات المالية والأسهم والسندات والكمبيالات وخطابات الاعتماد أو أية فوائد أو أرباح أو عوائد من هذه الأموال أو القيمة المستحقة منها أو الناشئة عنها.

غسل الأموال: هو الفعل المحدد في المادة (3) من القانون.

تمويل الإرهاب: هو الفعل المحدد في المادة (4) من القانون.

المستفيد الحقيقي: هو الشخص الطبيعي صاحب الملكية أو السيطرة الفعلية على العميل أو الذي تتم العملية لحسابه أو لمصلحته أو وفقا لإرادته؛ ويمكن معرفة المستفيد الحقيقي عبر الاسترشاد بالآتي:

1- أي شخص طبيعي (أشخاص) يملك في المحصلة النهائية، أو يمارس السيطرة الفعلية في نهاية المطاف سواء بشكل مباشر أو غير مباشر على العميل و/أو الشخص الطبيعي الذي تجري العملية بالنيابة عنه.

2- الأشخاص الطبيعيين الذين يمارسون السيطرة الفعلية في نهاية المطاف على شخص اعتباري أو اي كيان قانوني (Legal Arrangement)؛ وعليه تعتبر من حالات التملك و/او السيطرة غير المباشرة الحالات التي يكون فيها التملك و/او السيطرة من خلال عدة تملكات متتابعة او من خلال وسائل سيطرة غير مباشرة (مثل استخدام واحد أو أكثر من المساهمين المرشحين بشكل رسمي و/أو غير رسمي).

ويكون الشخص الطبيعي هو المستفيد النهائي من الشخص الاعتباري إذا كان الشخص الطبيعي:

1. يملك فعلا رأس مال الشخص الاعتباري أو أصوله الأخرى ويستفيد منها.
2. يمارس/ يمارسون بأي وسيلة سيطرة فعلية على الشخص الاعتباري.
3. يملك/ يملكون أو يسيطرون على 10٪ أو أكثر من رأس مال الشخص الاعتباري، سواء بشكل مباشر أو غير مباشر.

المؤسسة الوهمية او الجوفاء (Shell Entities): هي المؤسسة (سواء كانت مالية او غير مالية) التي ليس لها وجود مادي في الدولة التي تأسست فيها وحصلت على ترخيصها منها، والتي لا تتبع أي مجموعة خدمات مالية خاضعة لإشراف موحد فعال.

الوجود المادي: يتوفر الوجود المادي للمؤسسة من خلال:

- وجود مقر عمل ثابت لاستقبال العملاء وممارسة النشاط فعليا، ولا يكفي بمجرد وكيل محلي أو موظفين من مستوى منخفض.
- وجود إدارة فعلية.
- الاحتفاظ بسجلات للعمليات في موقع المؤسسة.
- الخضوع للتفتيش من قبل الجهات الرقابية والإشرافية سواء في البلد الذي تأسست فيه أو في البلد الذي تمارس نشاطها فيه.

الجريمة المالية عبر الوسائل الإلكترونية: هي كل فعل أو محاولة فعل، محلية أو عابرة للحدود، صادرة بإرادة جرمية عن أفراد أو مجموعات منظمة بهدف انتهاك الحسابات المصرفية أو المعلومات المالية والشخصية عبر

استخدام وسائل الكترونية وتقنية عدة، يدخل ضمن نطاق هذه الجرمية عمليات الاحتيال والسرقة والاختلاس والابتزاز والتخريب والتجسس عبر استخدام الوسائل الالكترونية.

رابعاً: المنهج المستند الى المخاطر:

1- يجب على البنوك تصنيف عملائها بما لا يقل عن ثلاث درجات؛ منخفض المخاطر، متوسط المخاطر، وعالية المخاطر، وعلى ان يتم مراجعة تصنيف العملاء وفقا لدرجة المخاطر على النحو التالي:
   - كل سنة للعملاء ذوي المخاطر المرتفعة
   - كل سنتين للعملاء ذوي المخاطر المتوسطة
   - كل أربع سنوات للعملاء ذوي المخاطر المنخفضة
2- يجب على كل بنك وضع استراتيجيات وإجراءات استباقية ومستمرة لتحديد ورصد وإدارة ومراقبة وتخفيف المخاطر التي ينطوي عليها كل عميل ومعاملاته.
3- يقوم كل بنك بمراجعة استراتيجية تصنيف المخاطر المعتمدة من قبله/قبلها خلال ستين يوماً بعد نهاية كل سنة ميلادية، وعلى ان يتم مراجعة هذه الاستراتيجية من قبل مراجع خارجي مستقل خلال خمسة عشر يوم عمل بعد انتهاء فترة الستين يوما المشار إليها طي هذه الفقرة، ويقدم تقريره الى قطاع الرقابة على البنوك في البنك المركزي.
4- يقوم كل بنك خلال ستون يوماً من نهاية كل سنة مالية او عند اصدار منتج جديد او عند الاندماج مع مؤسسة اخرى بمراجعة التقييم السنوي للمخاطر المذكور في الفقرة (3) على ان يشمل التقييم جميع المخاطر الحالية والمحتملة المرتبطة بالعملاء والمعاملات والمناطق الجغرافية، وعلى ان يتم مراجعة إعادة التقييم من قبل مراجع خارجي مستقل في موعد لا يتجاوز خمسة عشر يوم عمل بعد انتهاء فترة الستين يوم المشار إليها، ويتم تقديم تقرير اعادة التقييم إلى قطاع الرقابة على البنوك في البنك المركزي مع استراتيجية التخفيف من كل خطر.
5- يقوم كل بنك بإعداد تقييم مخصص للمخاطر كلما ظهرت مؤشرات تدل على حدوث تغيير جوهري في المخاطر المرتبطة بعميل معين أو بمعاملة معينة. يجب توثيق هذا التقييم وتقديمه إلى قطاع الرقابة على البنوك في البنك المركزي، مرفقا به الاستراتيجية المتبعة للتخفيف من كل خطر يظهر حديثا، في غضون خمسة عشر يوم عمل بعد رصد التغيير في المخاطر.

خامساً: تدابير العناية المشددة على الخدمات المالية مرتفعة المخاطر:

أدوات قابلة للتداول لحاملها: يجب أن يكون لدى البنك او شركة/منشاة الصرافة السياسات والإجراءات والأنظمة والضوابط الوافية للعناية الواجبة الخاصة بمكافحة غسل الأموال وتمويل الإرهاب بالنسبة للمخاطر المرتبطة باستخدام الأدوات القابلة للتداول لحاملها، وقبل أن يدخل البنك او شركات/منشآت الصرافة أو يشترك في معاملة تتضمن أداة قابلة للتداول لحاملها وتحويلها إلى نموذج مسجل بغرض دفع الأرباح أو رأس المال، فيتعين على البنك تطبيق تدابير العناية الواجبة المشددة واستيفاء البيانات التالية كحد أدنى:

1- فيما يتعلق بالشخص الطبيعي الذي يملك أسهماً لحاملها:
   - قائمة مفصلة بجميع الأسهم التي يملكها هذا الشخص.
   - وثيقة معتمدة لإثبات الهوية.
   - أدلة داعمة معقولة تثبت امتلاكه للأسهم.
2- فيما يتعلق بالشخص الاعتباري الذي يملك أسهماً لحاملها صادرة عن شركة أخرى:
   - قائمة مفصلة بجميع الأسهم التي يملكها هذا الشخص الاعتباري.
   - ترخيص مزاولة المهنة من جهات الاختصاص.
   - أدلة داعمة معقولة تثبت أن الشخص الاعتباري يمتلك الأسهم لحاملها.
3- فيما يتعلق بالشخص الاعتباري الذي أصدر أسهماً لحاملها:
   - قائمة مفصلة بجميع الأشخاص التي اصدرت الأسهم لصالحهم، بما في ذلك عناوين أصحابها ووثائق الهوية المطلوبة.
4- يجب على كل بنك او شركة/منشاة الصرافة أن تطلب من أي شخص طبيعي أو اعتباري تزويدها بالمعلومات بموجب الفقرة السابقة وتحديث تلك المعلومات مرة واحدة على الأقل كل سنة وكلما طرأ أي تغيير يجعل المعلومات المقدمة سابقا غير دقيقة.
5- يحظر على جميع البنوك وشركات/منشآت الصرافة أن يكون لديها عميل أو ان تشرع بأي عمل مع أي شخص طبيعي أو اعتباري يحتفظ أو يصدر أسهما لحاملها قبل تقديم المعلومات المطلوبة بموجب الفقرات 1 و2 و3 أعلاه.

سادساً: المخاطر المتعلقة بالجرائم عبر الوسائل الإلكترونية:

على البنوك ومنشآت الصرافة، كلاً فيما يخصه، ان تقوم بإعداد سياسات واتخاذ تدابير واجراءات وقائية للتخفيف من الجرائم عبر الوسائل الالكترونية وان تقوم وعلى مسؤوليتها باتخاذ الاجراءات الادارية والتقنية

والقضائية المناسبة للتنبه ورصد ومكافحة الجرائم المالية عبر الوسائل الالكترونية وعلى ان تتضمن السياسات التالية كحد أدنى:

1- سياسات عامة:

1.1 تقييم مخاطر الجرائم عبر الوسائل الالكترونية المحتملة والاطلاع المستمر على آخر المستجدات في مجال تكنولوجيا امن المعلومات.

1.2 توعية الموظفين والعملاء حول الوقاية من الجرائم المالية عبر الوسائل الالكترونية.

1.3 تنظيم عقود تأمين تغطي مخاطر الجرائم المالية عبر الوسائل الالكترونية.

1.4 مراقبة اي تغييرات في عادات وسلوك الموظفين، لاسيما الذين يتمتعون بامتيازات هامة للدخول على الانظمة المعلوماتية.

1.5 وضع الخطط اللازمة للوقاية من الجرائم المالية عبر الوسائل الالكترونية وتحديثها باستمرار (مثل خطة الاستجابة للحوادث، خطة استمرار التشغيل اثناء وبعد حدوث كارثة، خطة التدريب على التدخل الفوري).

1.6 تخصيص المبالغ اللازمة لإرساء وتطبيق سياسة ونظم وقواعد أمان تكنولوجيا المعلومات.

1.7 انشاء فريق عمل مخصص للوقاية من الجرائم المالية عبر الوسائل الالكترونية.

1.8 تبادل المعلومات المتعلقة بالجرائم المالية عبر الوسائل الالكترونية، مع الجهات المعنية داخل أو خارج المصرف أو المؤسسة المالية.

1.9 التيقّظ والحذر لدى التعاقد مع جهات خارجية لتكليفها بمهام تتعلق بالأنظمة الالكترونية والتأكد من ان هذه الجهات لا تقوم بالتعاقد مع كيانات من الباطن أقل موثوقية.

1.10 تضمين العقد الموقع مع العميل" اتفاقية فتح الحساب" احكاماً خاصة تتعلق بتحديد وسائل اخرى غير البريد الالكتروني للاتصال بالعميل (كالاتصال الهاتفي مثلاً) لتأكيد صحة طلبات التحاويل المرسلة الكترونيًا على ان لا يتم تغيير هذه الوسائل الا بالاتفاق الخطي بين الطرفين والاحتفاظ بالمعلومات والمراسلات والأدلة التي تثبت الاتصال وحفظها في مكان آمن.

1.11 ابلاغ العميل عن المخاطر الناتجة عن استخدام البريد الالكتروني لطلب اجراء تحويلات مالية وتوجيهه لاستعمال وسائل اخرى أكثر امانًا والحصول على موافقته الخطية على تحمل هذه المخاطر.

1.12 تزويد العميل بإرشادات التنبه من الجرائم المالية عبر الوسائل الالكترونية.

1.13 الطلب من عملائها الابلاغ عن أي جرائم مالية عبر الوسائل الالكترونية قد تعرضوا لها فور علمهم أو اكتشافهم أو تبليغهم انهم وقعوا أو كادوا ان يقعوا ضحية لها.

1.14 مراقبة موضوع التحويل ووجهته لجهة الدول المُرسل اليها والوسطاء الماليين أو المصرفيين المعتمدين ومراجعة اسماء المستفيدين النهائيين وارقام حساباتهم مقارنة مع تعاملات العميل السابقة.

1.15 التنبه الى اي طلب تحويل مشبوه عبر البريد الالكتروني خاصة إذا تبين انه لا يتلاءم مع النشاط الاعتيادي للعميل أو مع العمليات التي تجري عادةً على حساب العميل من ناحية قيمتها وموضوعها ووجهتها.

2-سياسات تقنية:

2.1 وضع انظمة واجراء ات داخلية مخصصة لتنفيذ طلبات تحويل الاموال الواردة اليها الكترونيًا عبر البريد الالكتروني، خدمة العمليات المصرفية الالكترونية Electronic Banking .

2.2 اعتماد وسيلة تحقيق مزدوجة على الأقل للتأكد من هوية المستخدِمين من خارج المصرف أو المؤسسة المالية عند دخولهم الى النظام.

2.3 استخدام تقنية ترميز متطورة وآمنة للبيانات الهامة منعًا لفقدانها أو التلاعب بها.

2.4 اعتماد قواعد واضحة عند تفحص البريد الإلكتروني الوارد (Filtering) وضبط الوصول إلى البريد الإلكتروني من خارج المصرف أو المؤسسة المالية.

2.5 تحديث انظمة اجهزة الكمبيوتر كافة والتحقق من امان الأجهزة الموضوعة بتصرف الموظفين لاستخدامها خارج المصرف او المؤسسة المالية.

2.6 عمل اختبار دوري لإمكانية الاختراق، لكشف أي نقاط ضعف محتملة في الشبكة.

2.7 مراقبة الحركة على الشبكة لكشف أي سلوك غير اعتيادي، سواء من خلال نوعية المعلومات المرسلة أو عددها او اتجاهاتها.

2.8 التحقق من سلامة البيانات ومراقبتها بهدف كشف أي تلاعب غير مشروع بها، وتعقّب مصدر الوصول غير المشروع إليها.

3- إجراءات الإبلاغ عن الجرائم المالية عبر الوسائل الالكترونية:

على البنوك وشركات/منشآت الصرافة، عند اكتشافها أو علمها أو تبلغها بأن أي من عملائها قد وقع ضحية افعال جرمية عبر الوسائل الالكترونية ذات طابع مالي، اتخاذ اجراء ات سريعة وفعالة تشمل على الاقل الاجراءات التصحيحية التالية:

3.1 تزويد كل من البنك المراسل والبنك المستفيد أو المؤسسة المالية المستفيدة بكافة المعلومات ذات الصلة وطلب الغاء عملية التحويل واعادة قيمتها للعميل.

3.2 ابلاغ وحدة جمع المعلومات المالية بالمعلومات والمراسلات التقنية ذات الصلة وكحد أدني المعلومات التالية:

- مصدر البريد الالكتروني المنسوب للعميل أو العنوان (IP Address) الذي تم عبره ارسال طلبات التحاويل المشبوهة.
- اسم الشركة مقدمة خدمة الانترنت التي تم عبرها ارسال طلبات التحاويل المشبوهة
- اسم الشركة مقدمة خدمة الانترنت المستخدمة للولوج غير المصرح به الى حساب العميل عن طريق خدمة العمليات المصرفية الالكترونية Electronic Banking.

3.3 توجيه العميل لتقديم ابلاغ أو شكوى قضائية الى الجهات المختصة.

يعتبر هذا المنشور ملحق للمنشور الدوري رقم (1) لسنة 2012م والمنشور رقم (1) لسنة 2013م والمنشور رقم (8) لسنة 2014م وتعديلاً لبعض بنودهما.

يتم العمل بموجبه

صادر بتاريخ / /1442هـ

الموافق / /2021م

حسين المحضار

وكيل قطاع الرقابة على البنوك

الجمهورية اليمنية REPUBLIC OF YEMEN البنك المركزي اليمني Central Bank Of Yemen Head Office - Aden