Republic Of Iraq
AML/CFT office

جمهورية العراق
مكتب مكافحة غسل الأموال وتمويل الإرهاب

NO :
Date :

العـدد : ٧/١/ب د/ اعمام (١٧)
التاريخ : ٢٠٢٠/٩/١٧

إلى/ المصارف المجازة كافة

م/ اعمام

تحية طيبة ....

نرسل ربطاً ورقة ارشادية بخصوص (مخاطر غسل الأموال وتمويل الإرهاب المرتبطة بانتشار فيروس كورونا)، وتأتي هذه الورقة الارشادية في ظل حرص مكتب مكافحة غسل الأموال وتمويل الإرهاب على متابعة ورصد مخاطر غسل الأموال وتمويل الإرهاب الناشئة عن اساءة استغلال التدابير الاحترازية المطبقة لمواجهة انتشار جائحة فيروس كورونا ، على المستويات المحلية والاقليمية والدولية والتعاون والتنسيق مع الجهت المعنية في التعرف على تلك المخاطر واتخاذ اللازم للحد منها.

للتفضل بالاطلاع واتخاذ مايلزم.... مع التقدير

المرافقات:

- ورقة ارشادية.

المـدير العـام
٢٠٢٠/٩/١٧

جمهورية العراق
مكتب مكافحة غسل الأموال وتمويل الإرهاب

مكتب مكافحة غسل الاموال وتمويل الارهاب

ورقة ارشادية

مخاطر غسل الاموال وتمويل الارهاب المرتبطة بانتشار فيروس كورونا المستجد(COVEID١٩)

المقدمة

تشكل جائحة فيروس كورونا صدمة اقتصادية واجتماعية شديدة على جميع البلدان على حد سواء ومن التحديات العالمية غير مسبوقة ومعاناة بشرية واضطراب الاقتصاد وبالتالي ادت إلى أحداث تغييرات كبيرة على النواحي الاجتماعية والاقتصادية وكذلك معدلات الإنتاج والعمل نتيجة التدابير الاحترزية التي اتخذتها الدول في مواجهة هذه الجائحة. من ناحية أخرى فقد وفرت هذه التدابير فرصاً جديدة للمجرمين لتحقيق مكاسب غير مشروعة وكذلك لتمويل الإرهابيين والمنظمات الارهابية والأعمال الارهابية، مما يزيد من معدل ارتكاب الجرائم، وفى الوقت ذاته يزيد من مخاطر غسل الأموال وتمويل الإرهاب التي تواجهها دول العالم.

وفي هذا الصدد، ونظراً للتعليمات الحكومية التي ترتب عليها خفض مستوى القوى العاملة التي تباشر أعمالها من مقرات العمل بصفة عامة في القطاعين العام والخاص لأغراض التباعد الاجتماعي، فأن مكتب مكافحة غسل الأموال وتمويل الإرهاب يؤكد على أهمية استمرار الجهات الملزمة بالإبلاغ بتطبيق نظم مكافحة غسل الأموال وتمويل الإرهاب لديها والتعرف على المعاملات التي يجب الإبلاغ عنها والقيام بذلك وفقاً للتعليمات السارية بقدر الإمكان. وفي حالة وجود أي تحديات قد تعوق الجهة المبلغة عن القيام بواجب الإبلاغ في الوقت المناسب يجب أن يتم إشعار المكتب بذلك حتى يتمكن المكتب من الحصول على المعلومات التي تمكنه من القيام بأداء مهامه التي أناطه بها القانون.

كما نؤكد على الجهات المبلغة على اشعار هذا المكتب بأي مستجدات غير مبررة يتم ملاحظتها فيما يتعلق بسلوكيات فئات معينة من عملائها في كيفية تنفيذ معاملاتهم أو الدول والأطراف المرتبطة بهذه المعاملات.

وتأتي هذه الورقة الارشادية في ظل حرص مكتب مكافحة غسل الاموال وتمويل الارهاب على متابعة ورصد مخاطر غسل الاموال وتمويل الارهاب الناشئة عن اساءة استغلال التدابير الاحترازية المطبقة لمواجهة انتشار جائحة فايروس كورونا ، على المستويات المحلية والاقليمية والدولية والتعاون والتنسيق مع الجهات المعنية في التعرف على تلك المخاطر واتخاذ اللازم للحد منها.

أولا : تهديدات غسل الأموال وتمويل الارهاب

أ- **تهديدات غسل الأموال:** لقد ولّدت جائحة فايروس كورونا استجابات حكومية مختلفة تتراوح بين المساعدة الاجتماعية ومبادرات الإعفاء الضريبي ،وهذا قد يوفر فرصاً جديدة للمجرمين والإرهابيين لتوليد وغسل العائدات غير المشروعة ونورد فيما يلى أهم تهديدات غسل الأموال الجديدة الناجمة عن الجرائم المرتبطة بستغلال انتشار فيروس كورونا المستجد(COVID ١٩):

١- تزايد الانشطة الاحتيالية من خلال بعض الممارسات أهمها:

- **بيع سلع مقلدة أو مزورة** تفاقم غش المنتجات الطبية وتقليدها عالميا، في ظل أزمة تفشي فيروس كورونا، إذ استغل المجرمون الجائحة للتربح عبر بيع مستلزمات مغشوشة لا تقي من الفيروس، وأدوية مقلدة ومزورة، في مثل هذه الحالات، يعرض المجرمون على الانترنت بيع أدوية أو مستلزمات أو أجهزة طبية ترتبط بمعالجة الفيروس أو الوقاية منه منسوبة إلى شركات عالمية أو منظمات صبية دولية، ويتم طلب معلومات بطاقات ائتمان الضحايا أو يتم طلب دفع رسوم شحن، ولكن لا يتم تسليم البضاعة أو يتم ارسال سلع مزيفة أو مقلدة أو غير فعالة، وفي بعض الاحيان يقوم المجرمون بخداع المنتجين والموزعين لتلك الأدوية والمستلزمات ويتم دفعهم للتعامل معهم من خلال تقديم وثائق مزورة، أو إنشاء شركات أو مواقع الكترونية وهمية من أجل كسب ثقتهم.

- **انتحال هوية المسئولين الحكوميين** :في مثل هذه الحالات، يتواصل بالافراد سواء شخصياً او بالبريد الإلكتروني أو عبر الهاتف وينتحلون هوية مسؤولين حكوميين بقصد الحصول على معلومات عن بطاقات أو حسابات مصرفية شخصية أو حصولهم على النقود بشكل مادي تحت عدة ادعاءات، منها أنها لأغراض تخفيض الضرائب في ظل الأزمة أو لصرف إ عانات مالية، أو ينتحل المجرمون صفة مسؤولين بأحد المراكز الطبية بقصد الحصول على أموال بزعم أنها مقابل علاج المصابين والمخالطين وتوفير مستلزمات طبية.

٢- زيادة وتيرة الانشطة الاحتيالية و الجرائم الإلكترونية:

- **التصيد عبر البريد الإلكتروني والرسائل النصية القصيرة** هي رسائل إلكترونية يُفترض أنها صادرة عن أجهزة وطنية أو هيئات صحية عالمية من أجل خداع الضحايا وحملهم على توفير معلومات شخصية عنهم

أو تفاصيل الدفع، أو أيضا فتح ملف مرفق يحتوي على برمجية خبيثة ويدعي المجرمون بأنهم ينتمون مثلا لمنظمة الصحة العالمية(WHO) عبر إرسال رسائل بريد إلكتروني أو رسائل هاتف محمول لاغراء الافراد للدخول على روابط أو فتح مرفقات تكشف لاحقًا عن اسم المستخدم وكلمة المرور أو تطلب معلومات عن البطاقة الائتمانية أو الحساب المصرفي.

- **عمليات الاحتيال باستخدام البريد الإلكتروني للشركات:** من ضمن عمليات الاحتيال الشائعة المتعلقة بالبريد الإلكتروني للشركات هي الفواتير المزيفة، وغالبًا ما يتم استهداف الشركات المزودة بموردين أجانب بهذه الطريقة، حيث يتظاهر المهاجمون بأنهم المورّدون الذين يطلبون تحويل الأموال إلى حساب يمتلكه المحتالون، ومن ضمن اساليب الاحتيال بأن يقوم المهاجمون بالتظاهر بأنهم أحد كبار المديرين التنفيذيين للشركات وإرسال بريد إلكتروني إلى العاملين في الشؤون المالية بالشركة يطلبون منهم تحويل الأموال إلى الحساب الذي يسيطرون عليه، وأيضا تسوية الحساب حيث يتم اختراق حساب البريد الإلكتروني الخاص بالمسؤولين التنفيذيين أو الموظفين ويستخدم في طلب دفع الفواتير إلى البائعين المدرجين في جهات اتصال البريد الإلكتروني الخاصة بهم ثم يتم إرسال المدفوعات إلى حسابات مصرفية حتيالية. كما يتم سرقة البيانات من موظفي إدارة الموارد البشرية والمالية في الشركات للحصول على معلومات شخصية عن الموظفين والمديرين التنفيذيين، حتى يتمكن المنتحل من استخدام هذه البيانات للهجمات المستقبلية على المؤسسة.

- **الفساد المالي و الإداري** : يحاول بعض اصحاب السلطة الاستفادة غير المشروعة مس الوضع الحالي وبطرق مختلفة ومنها:
  - استخدام اسماء وهمية للحصول على الاعانات الاجتماعية.
  - اساءة استخدام المساعدات المالية الدولية.
  - استخدام عقود حكومية لشراء كميات كبيرة من المستلزمات الطبية توفر فرصآ لآختلاس الأموال العامة أو ارساء مناقصات طبية أو تعليمية على جهات محددة.

-**الابتزاز عن طريق برامج الفدية:** بالتزامن مع انتشار **جائحة كورونا** الذي أجبر الشركات والمؤسسات على تفعيل العمل من المنزل لحماية موظفيها. ومعها نشُطت عمليات القرصنة ونشر البرمجيات الخبيثة

وبالتحديد **برامج الفدية ransomware** التي تلوث أجهزة الكمبيوتر والهاتف الذكي أو الكمبيوتر اللوحي وتشفر الملفات أو تتلف نظام التشغيل، فيصبح عصيا على صاحب الجهاز استخدامه. لاستعادة السيطرة على الجهاز وعلى معطياته التي تم تشفيرُها، عليه دفع فدية مالية، ولا يقتصر استهداف ضحايا الابتزاز فقط على المؤسسات والمستشفيات، بل يطال بشكل كبير **الأفراد**، اللذين غالبا ما يجهلون كيفية التعامل مع هذا النوع من القرصنة ويلجأون إلى حلول تُقتَرح عبر مواقع على الإنترنت.

- **استغلال العمال وتجنيدهم كحاملي الأموال** :الانتشار الواسع لكورونا أدى إلى غلق المطاعم والمقاهي والمراكز التجارية مما أدى ذلك إلى زيادة البطالة مع قلة المساعدات المادية والاجتماعية وبرامج التوعية المقدمة لتلك الفئات يمكن ان يتم استغلال العمالة المتضررة من انتشار جائحة كورونا في تجنيد بعضهم من خلال فتح حسابات الشخصية لهم لتمرير الأموال من خلالها، وقد يكون في كثير من الأحيان بطرق احتيالية، وكذلك يمكن خلال نشر إعلانات عن وظائف مزيفة لمنظمات رعاية صحية مزيفة ومنظمات غير حكومية مزيفة ويُطلب ممن تم تجنيدهم تمرير أموال إلى المجرمين من خلال حساباتهم المصرفية بزعم أنها أموال موجهة إلى مستحقي التبرعات، حيث يمكن أن تتضمن هذه الأموال تبرعات بالفعل تم جمعها من الضحايا عن طريق التحايل أو أموالاً غير مشروعة يتم محاولة إضفاء صفة الشرعية عليها من خلال تلك العمليات، وغالباً ما يتم اغراء من تم تجنيدهم على القيام بذلك عن طريق السماح لهم بالاحتفاظ بجزء من المبالغ كعمولة.

ب - **تهديدات تمويل الإرهاب** : تشمل تهديدات تمويل الارهاب الاشخاص او الانشطة ذات احتمالية لإحداث خطر على الدولة او المجتمع او الاقتصاد او غيرها يتعلق بتقديم الدعم للعمليات الارهابية ويتضمن ذلك الارهابين والمجموعات الارهابية ومعاونيهم واموالهم وكذلك انشطة تمويل الارهاب. وتتمثل التهديدات الناشئة عن استغلال انتشار فيروس كورونا في استخدام الجماعات الارهابية للأزمة لجمع الاموال وتحريكها لتمويل اعمالها الارهابية مستغلة انشغال الحكومة بمكافحة انتشار الفيروس وتزايد الحاجة الى المساعدة وجمع التبرعات ومن ضمن اهم صور هذه التهديدات جمع الاموال من قبل ممولي الارهاب من خلال رسائل الكترونية او التواصل المباشر او الرسائل النصية عبر وسائل التواصل الاجتماعي لطلب تبرعات انسانية لمصابي او اسر ضحايا الفيروس او العمالة المتضرر بزعم انهم يمثلون منظمات دولية او جمعيات خيرية ،

وتوجيه الضحايا لتقديم معلومات بطاقات الائتمانية الخاصة بهم او اجراء المدفوعات باستخدام المحافظ الرقمية او الحصول على الاموال نقداً.

كما يمكن استغلال المؤسسات المالية في تمويل الإرهاب، عبر استغلال الأوضاع العالمية لجمع الأموال لتمويل الإرهاب واستغلال الحالات الإنسانية الناتجة عن تلك الأزمة، بالإضافة إلى إساءة استخدام الخدمات التي تقدمها الجهات غير الهادفة للربح لأغراض إنسانية وخيرية وطبية، علاوة على إمكانية زيادة المعاملات مع الدول غير الملتزمة بشكل كامل بتعليمات مجموعة العمل المالي والتي قد تكون مناطق صراع من خلال حوالات مالية.

ثانياً / بعض نقاط الضعف في المؤسسات المالية التي يمكن أن تستغل في ظل انتشار جائحة كورونا:

- انخفاض أعداد الموظفين وخاصة الذين يتعاملون بشكل مباشر مع الزبائن مما يؤثر سلباً على تطبيق متطلبات مكافحة غسل الأموال وتمويل الإرهاب وخاصة اكتشاف العمليات المشتبه فيها.
- عدم التركيز على متابعة العمليات لاكتشاف العمليات غير العادية والمشتبه فيها والرقابة على مدى الالتزام بمتطلبات مكافحة غسل الأموال وتمويل الإرهاب نظراً لإعطاء الاولوية لوضع وتنفيذ خطط استمرارية العمل.
- انخفاض أو وقف الزيارات الميدانية من قبل الجهات الرقابية قد يؤثر على الالتزام بمتطلبات مكافحة غسل الأموال وتمويل الإرهاب.

ثالثاً/بعض المؤشرات الاسترشادية للعمليات المشتبه فيها

في ضوء ما سبق، وعملا على مساعدة المؤسسات المالية والجهات الأخرى في تحديد العمليت المشتبه فيها ذات العلاقة بانتشار الفيروس، فيما يلي بعض المؤشرات الاسترشادية ذات الصلة:

١- إيداعات متكررة أو ضخمة من أنشطة تجارية غير أساسية أو ضرورية بما لا يتناسب مع طبيعة هذه الأنشطة أو حاجة المواطنين إليها في وقت الأزمة.

٢- تلقى إيداعات ضخمة أو متكررة يبدو أنها بغرض تبرعات أواعانات لمصابي الفيروس أو أسر ضحاياه.

٣- وجود مدفوعات مقابل شحنات أدوية أو أجهزة طبية أو مستلزمات حماية شخصية تبدو وهمية.

٤- وجود شبهة تلاعب في فواتير تتعلق بشحنات أدوية أو أجهزة طبية أو مستلزمات حماية شخصية لتبدو بقيمة أكبر أو أقل.

٥- تسييل لمحافظ اوراق مالية ضخمة بصورة مفاجئة دون مبرر واضح.

٦- تلقي إيداعات أو تحويلات بمبالغ ضخمة خلال فترة سريان التدابير الاحترازية الخاصة بمواجهة انتشار الفيروس رغم حداثة فتح الحساب، أو عدم وجود ما يشير إلى نشاط كبير أو تاريخ طويل للعميل في مجال النشاط المعلن له.

٧- زيادة التعامل على الحساب بصورة مفاجئة دون وجود مبرر اقتصادي واضح.

٨- وجود تحويلات للأموال من وإلى دول مرتفعة المخاطر.

٩- التغييرات المتكررة في هيكل الملكية أو السيطرة الخاص بعميل من الأشخاص الاعتبارية.

١٠- تلقى أموال تتعلق بحصيلة بيع أدوية أو أجهزة طبية أو مستلزمات حماية شخصية خاصة بالفيروس، على الرغم من عدم وجود تعاملات سابقة بهذا النشاط.

١١- وجود مؤشرات بأن العميل أو المستفيد الحقيقي يتعامل مع شركة وهمية أو لا تمارس أية أعمال بشكل فعلي.

رابعآ / بعض التوصيات والاجراءات المقترحة للحد من مخاطر غسل الأموال وتمويل الإرهاب المرتبطة بانتشار فيروس كورونا

وهنا نؤكد على أهمية قيام المؤسسات المالية بتنفيذ تدابير واجراءات في ضوء تلك المخاطر

١- تطبيق إجراءات العناية الواجبة المناسبة والمراقبة الفعالة للمعاملات الإلكترونية مع إيلاء عناية خاصة بالمعاملات الإلكترونية التي قد لا تتماشى مع النمط الطبيعي للعملاء وكذلك المعاملات الخاصة بالشرائح الجديدة من العملاء.

٢- تطبيق تدابير العناية الواجبة للمعاملات التي تتم باستخدام المنتجات والخدمات التجارية كخطابات الضمان والاعتمادات المستندية وخاصة تلك المرتبطة بشراء معدات وأجهزة طبية للعملاء الذين قد لا تكون طبيعة عملهم مرتبطة بتلك الأنشطة.

٣- فهم المخاطر الجديدة المرتبطة بانتشار فيروس كورونا وتقييم هذه المخاطر على مستوى المؤسسة.

٤- الاعتماد على المنهج القائم على المخاطر بصورة أكبر في الرقابة على المؤسسات الخاضعة للرقابة.

٥- تطوير سيناريوهات اكتشاف العمليات غير العادية والمشبوهة في ضوء المخاطر المحددة.

٦- زيادة التركيز على متابعة العمليات لاكتشاف العمليات غير العادية والمشتبه فيها.

٧- زيادة التركيز على متابعة الجرائم مثل (الغش وتقليد المنتجات , جمع التبرعات لمؤسسات وهمية أو بدون ترخيص ,القرصنة الالكترونية , هدر المال العام) من قبل جهات انفاذ القانون.

٨- التأكد من إيلاء عناية واجبة مشددة للحوالات والمعاملات الإلكترونية التي تتم مع الدول التي بها نقص استراتيجي في أنظمة مكافحة غسل الأموال وتمويل الإرهاب أو مناطق الصراع.

٩- تطبيق تدابير العناية الواجبة المشددة للتبرعات التي تتم من خلال الجمعيات والمنظمات غير الهادفة للربح والتحقق من وجهات صرفها.

١٠- تطبيق إجراءات العناية الواجبة المبسطة في حالات المخاطر المنخفضة مثل تسهيل المدفوعات الحكومية للأفراد والشركات لدعمهم في أزمة فيروس كورونا المستجد.

١١- لتأكد من أن حالات عدم تطبيق إجراءات العناية الواجبة هي لأسباب قهرية وأنه سيتم معالجتها بشكل فوري بعد انتهاء أزمة فيروس كورونا المستجد.

١٢- التنبه لكافة أنواع المخاطر الجديدة خاصة المرتبطة منها بأنماط وأشكال قد ترى المؤسسة المالية أنها تمثل خطر على أنظمتها وإجراءاتها الرامية للحد من مخاطر غسل الأموال وتمويل الإرهاب

١٣- ضرورة التنبه لأي مخاطر أو تهديدات قد تواجهها المؤسسة المالية مرتبطة بغسل الأموال أو تمويل الإرهاب قد تكون مرتبطة بإنشاء علاقات عمل جديدة مع فئة معينة من العملاء أو توفير الخدمات عن بعد.

١٤- زيادة الاهتمام بتدريب الموظفين على كيفية تطبيق اجراءات العناية الواجبة في ظل الظرف الحالي.