Republic Of Iraq
CENTRAL BANK OF IRAQ

جمهورية العراق
البنك المركزي العراقي

البنك المركزي العراقي

دائرة الرقابة على المصارف

NO :
DATE :

العدد : ٤١/٤/٩
التاريخ : ٢٠٢٥/٤/٢٠

(تحديث سجل الناخبين واجب وطني لضمان مشاركتكم في صنع القرار)

المصارف المجازة كافة

شركات مزوّدي خدمات الدفع الالكتروني المرخصين كافة

م/ ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدّمي خدمات الدفع الالكتروني

تحية طيبة..

استنادًا إلى قرار مجلس إدارة هذا البنك المرقم (٦٣) لسنة ٢٠٢٥ نرافق ربطًا (ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدّمي خدمات الدفع الالكتروني).

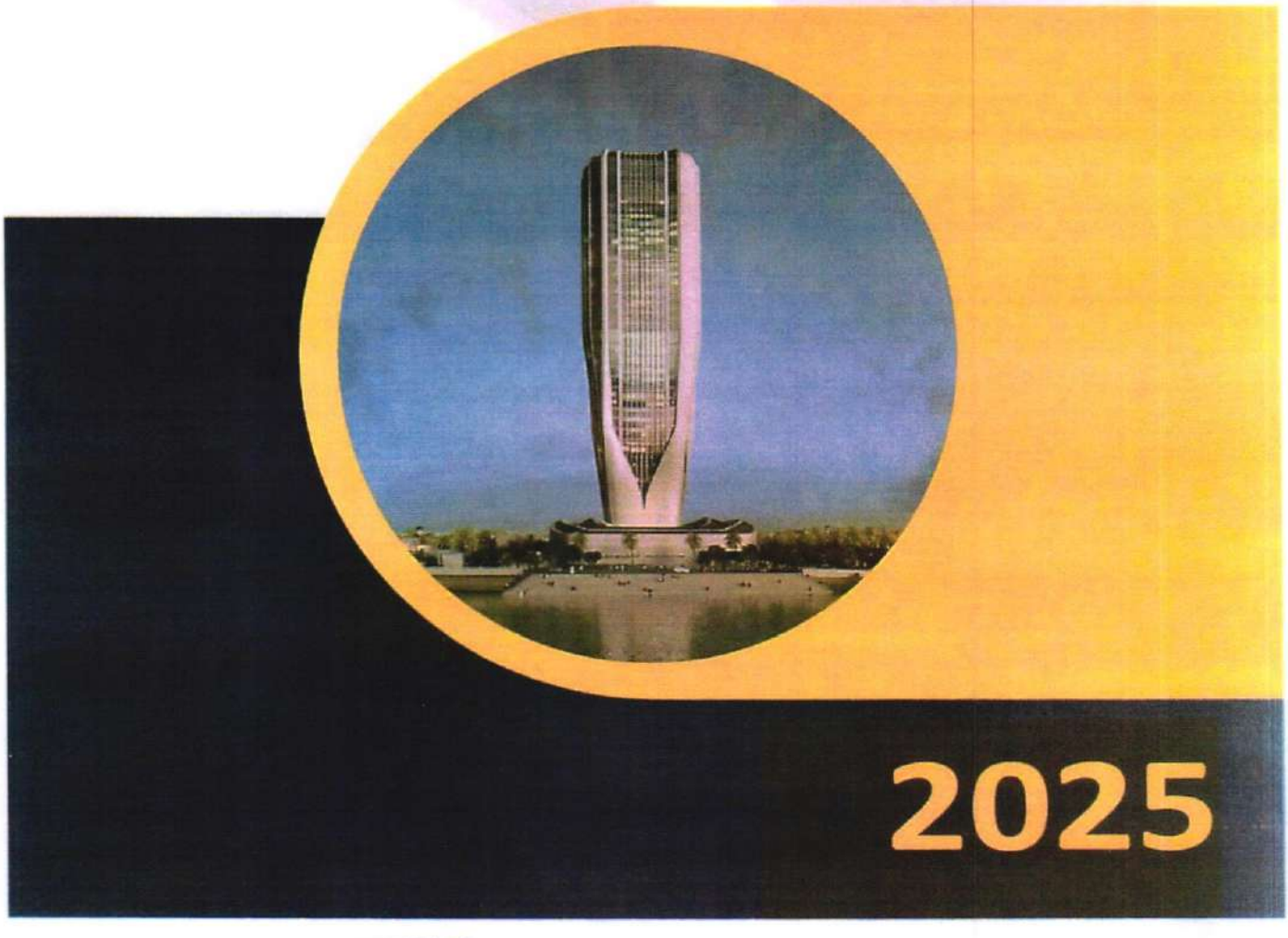
للعمل بموجبها.. مع التقدير .

المرافقات/
- ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدّمي خدمات الدفع الالكتروني.

أ.د.عمار حمد خلف
نائب المحافظ وكالة
٢٠٢٥/٤/٢٠

البنك المركزي العراقي

ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدمي خدمات الدفع الالكتروني في جمهورية العراق



2025

المحتويات

مقدّمة

تعتبر مكافحة غسل الأموال وتمويل الإرهاب من التحديات الأساسية التي تواجه النظام المالي في مختلف أنحاء العالم، ولا سيما في الدول التي تشهد تحولات اقتصادية أو بيئة مالية حديثة، وفي هذا السياق يبرز دور مقدمي خدمات الدفع الإلكتروني كأحد الأدوات المالية الحديثة التي تتيح تسهيل حركة الأموال عبر القنوات الالكترونية، ومع تزايد الاعتماد على خدمات الدفع الالكتروني في العراق، أصبح من الضروري وضع ضوابط تنظيمية تضمن حماية النظام المالي من الاستغلال في الأنشطة غير المشروعة، تواجه دول العالم تحديات متعددة تتعلق بمكافحة غسل الأموال وتمويل الإرهاب، حيث تسعى بعض الأطراف إلى استغلال النظام المالي المحلي والدولي لتمويل أنشطة تهدد الأمن الاقتصادي والاجتماعي، لذلك تبنى هذا البنك مجموعة من الضوابط التي تهدف إلى تعزيز الرقابة على مقدمي خدمات الدفع الإلكتروني، تشمل هذه الضوابط الزام مقدمي الخدمات بالتحقق من هوية العملاء، وإجراء تدقيق مستمر على المعاملات المالية، ومراقبة الأنشطة المشتبه فيها بهدف كشف أي محاولات لغسل الأموال أو تمويل الإرهاب، تشمل هذه الضوابط تكليف مقدمي خدمات الدفع الإلكتروني بتطبيق إجراءات وفق افضل الممارسات الدولية للامتثال لمتطلبات القوانين المحلية والدولية، اهمها قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015، وكذلك التعليمات و الضوابط الصادرة عن البنك المركزي العراقي، اذ يقع على عاتق مقدمي خدمات الدفع الالكتروني تطوير أنظمة متقدمة للرصد والتحليل، تعتمد على تقنيات حديثة للكشف عن العمليات المالية المشبوهة، فضلاً عن ذلك يُشترط على مقدمي خدمات الدفع الإلكتروني ضرورة تدريب الموظفين على كيفية التعرف على الأنشطة المالية غير القانونية والتعامل معها بشكل احترافي، كما يعزز التعاون مع الجهات الدولية والجهات الحكومية لضمان تطبيق أفضل الممارسات في مجال مكافحة غسل الأموال وتمويل الإرهاب، في ضوء هذه الضوابط، يسعى هذا البنك إلى بناء بيئة مالية آمنة ومستقرة، تساهم في تعزيز الثقة في النظام المالي العراقي، وتدعم النمو الاقتصادي المستدام، حيث ان التزام مقدمي خدمات الدفع الإلكتروني بتطبيق هذه الضوابط يعكس مدى أهمية تكامل جهود القطاع الخاص مع القطاع الحكومي في مكافحة الأنشطة المالية غير المشروعة، كما أن تطبيق معايير عالية من الشفافية والمراقبة يعزز من قدرة العراق على التفاعل مع المجتمع الدولي في مكافحة غسل الأموال وتمويل الإرهاب، يتطلب هذا التعاون المستمر بين الجهات الرقابية والبنوك والشركات المالية، حيث ان من خلال هذه الجهود، يهدف هذا البنك إلى بناء نظام مالي قوي وسليم يواكب المعايير العالمية، ويتيح للمؤسسات المالية العمل بأمان دون أن تشكل تهديدًا للأمن الاقتصادي.

البنك المركزي العراقي
مجلس الإدارة

المادة (1) : التعاريف

مع عدم الإخلال بالتعاريف الواردة في القانون رقم (39) لسنة 2015 بشأن مكافحة غسل الأموال وتمويل الإرهاب ونظام خدمات الدفع الالكتروني رقم (2) لسنة 2024، يقصد بالكلمات والعبارات في أدناه حيثما وردت المعاني المبينة إزاء كل منها.

1- **البنك المركزي**: البنك المركزي العراقي.

2- **القانون** : القانون رقم (39) لسنة 2015 بشأن مكافحة غسل الأموال وتمويل الإرهاب.

3- **المكتب**: مكتب مكافحة غسل الأموال وتمويل الإرهاب.

4- **الأموال** : الأُصول أو الممتلكات التي يتم الحصول عليها بأيّة وسيلة كانت كالعملة الوطنية والعملة الأجنبية والأوراق المالية والتجارية والودائع والحسابات الجارية والاستثمارات المالية والصكوك والمحررات أيًّا كان شكلها بما فيها رقمية أو ورقية والمعادن النفيسة والأحجار الكريمة والسلع وكل ذي قيمة مالية من عقار أو منقول والحقوق المتعلقة بها، وما يتأتى من تلك الأموال من فوائد أو أرباح سواء داخل العراق أم خارجه وأيّ نوع آخر من الأموال.

5- **غسل الأموال**:- كل فعل يُقصَد به إخفاء المصدر غير المشروع أو تمويهه، للأموال أو العائدات المتحصلة من جريمة أصلية أو مساعدة مرتكبها على التهرب من العقوبة.

6- **تمويل الإرهاب**: كل فعل يرتكبه أيّ شخص يقوم بأيّة وسيلة كانت مباشرة أو غير مباشرة بإرادته بتوفير الأموال أو جمعها أو الشروع في ذلك من مصدر شرعي أو غير شرعي بقصد استخدامها مع علمه أنّ تلك الأموال ستستخدم كليًا أو جزئيًا في تنفيذ عمل إرهابي أو من إرهابي أو منظمة إرهابية سواء وقعت الجريمة أم لم تقع وبصرف النظر عن الدولة التي يقع فيها هذا الفعل أو يتواجد فيها الإرهابي أو المنظمة الإرهابية.

7- **الجهات الرقابية**: الجهات المختصة بترخيص أو إجازة المؤسسات المالية والأعمال والمهن غير المالية المحدّدة، أو الإشراف عليها للتأكد من التزامها بالمتطلبات التي ستلتزمها مكافحة غسل الأموال وتمويل الإرهاب على سبيل المثال لا الحصر (البنك المركزي العراقي).

8- **المستفيد الحقيقي** :الشخص الطبيعي الذي يمتلك أو يمارس سيطرة نهائية مباشرة أو غير مباشرة على العميل أو الشخص الطبيعي الذي تتم المعاملة نيابة عنه كذلك الشخص الذي يمارس سيطرة فعلية نهائية على شخص معنوي أو ترتيب قانوني.

9- **أصحاب المناصب العليا ذوو المخاطر:**

- الأشخاص السياسيون ممثلو المخاطر الأجانب هم الأشخاص الموكلة إليهم أو الذين اوكلت إليهم مهام عامة بارزة في دولة أجنبية، كرؤساء الدول أو الحكومات والسياسيين رفيعي المستوى، والمسؤولين الحكوميين رفيعي المستوى والمسؤولين القضائيين والعسكريين، وكبار الموظفين التنفيذيين في الشركات المملوكة للدولة، ومسؤولي الأحزاب السياسيين المهمين.
- الأشخاص السياسيون ممثلو المخاطر المحليون هم الأفراد الموكلة إليهم أو الذين اوكلت إليهم مهام عامة بارزة محلية ، كرؤساء الدول أو الحكومات، والسياسيين رفيعي المستوى، والمسؤولين الحكوميين رفيعي المستوى والمسؤولين القضائيين والعسكريين، وكبار الموظفين التنفيذيين في الشركات المملوكة للدولة، ومسؤولي الأحزاب السياسية المهمين ومن في حكمهم (عائلاتهم وذوي الصلة بهم) .
- الأشخاص الموكلة إليهم مهام بارزة من منظمة دولية هم أعضاء الإدارة العليا أي المديرين ونواب المديرين وأعضاء مجلس الإدارة أو المناصب التي تعادلها، ولا ينطبق هذا التعريف على الأفراد الذين يشغلون مناسب متوسطة أو أقل في الفئات المذكورة.

10- **تدابير العناية الواجبة:** بذل الجهد للتعرف على هوية العميل والمستفيد الحقيقي والتحقق منها والمتابعة المتواصلة للعمليات التي تتم في إطار علاقة مستمرة، فضلًا عن التعرُّف على طبيعة العلاقة المستقبلية في بين المؤسسة المالية أو المؤسسة غير المالية أو المهن المعينة والعميل والغرض منها لغاية انتهاء العلاقة مع العميل .

11- **العميل:** أيُّ شخص يقوم أو يشرع بأيّة من الأعمال التالية مع إحدى المؤسسات المالية أو الأعمال والمهن غير المالية المحدّدة (ترتيب أو فتح أو تنفيذ معاملة أو علاقة عمل أو حساب له) و(المشاركة في التوقيع على معاملة أو علاقة عمل أو حساب) و(تخصيص أو تحويل حساب أو حقوق أو التزامات بموجب معاملة ما) و(الإذن بإجراء معاملة أو السيطرة على علاقة عمل أو على حساب).

12- **تحويل الأموال أو القيمة:** هي خدمة مالية تتضمن قبول النقد أو الشيكات أو غير ذلك من الأدوات النقدية أو القيم الاحتياطية ودفع مبلغ معادل نقدًا أو في أيّة صورة أُخرى لمستفيد عن طريق اتصال أو رسالة أو تحويل أو عن طريق شبكة مقاصة تنتمي إليها هذه الخدمة المختصة بتحويل الأموال أو القيمة ويمكن أن تتضمن العمليات المالية التي تقوم بها مثل هذه الخدمات وسيطًا واحدًا أو اكثر ودافعة نهائية إلى طرف ثالث، ويجوز كذلك أن تشمل أيّة طرائق دفع جديدة وغالباً ما تكون لهذه النظم صلات بمناطق جغرافية معينة.

13- **الأعمال والمهن غير المالية المحدّدة:** وتشمل هذا الأعمال والمهن على المحامين وتجار المعادن النفيسة والصاغة والوكلاء العقارين (الدلاليين) والمحاسبين والصناديق الاستئمانية.

14- **أنظمة مكافحة غسل الأموال:** مجموعة من الأنظمة التي تضع الحلول البرمجية بشأن تلقي ومعالجة وتحليل حركات وإيداعات العملاء التي تنطوي على مؤشرات اشتباه للوقوف على مدى سلامة توافق هذا الحركات والإيداعات النقدية مع تدفقاتهم ودخلهم النقدي ومراقبة وتحديث الكيانات المدرجة على قوائم العقوبات المحلية والدولية ومطابقة اسماء العملاء مع الاسماء المدرجة في قوائم الحظر المحلية والدولية و ومتابعة تحديث هذه القوائم بشكل آلي.

15- **العقوبات المحلية والدولية:** العقوبات التي تُفرَض على الأفراد أو مؤسسات معينة ويشمل كلًا من تجميد الأُصول وعمليات الحظر لمنع إتاحة الأموال أو الأُصول الأُخرى بشكل مباشر أو غير مباشر للأفراد أو الكيانات أو المجموعات أو المنظمات الخاضعة للعقوبات.

16- **نظام تلقي البلاغات الرقمية (GO AML):** هو نظام حل برمجي متكامل لمكافحة غسل الأموال وتمويل الإرهاب تمَّ تطويره من مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) ليتم استخدامه من مكتب مكافحة غسل الأموال وتمويل الإرهاب لغرض جمع البيانات وإدارتها وتحليلها وإدارة المستندات وسير العمل والاحتياجات الإحصائية الأُخرى، إذ يقوم هذا النظام بتلقي البلاغات في حالات الاشتباه بعمليات غسل الأموال وتمويل الإرهاب بصورة رقمية وآنية ليحل محل البلاغات الورقية، فضلًا عن توثيق نتائج عمليات حل حالات الاشتباه المحتملة (Fouls Matching).

17- **تحليل المخاطر:** عملية تقييم المخاطر المحتملة وتحليلها وتصنيفها وتحديد تأثيرها واحتمالية حدوثها.

18- **تقييم المخاطر:** عملية تقييم الأثر المحتمل للمخاطر واحتمالية حدوثها وتحديد مدى أهمّيتها وأولويّاتها.

19- **مزود خدمة الدفع الالكتروني:** شخص معنوي مرخص من البنك المركزي لتقديم خدمات الدفع الالكتروني .

20- **وكيل مزودي خدمات الدفع الالكتروني:** الوكيل المخول من مزود خدمات الدفع الالكتروني للعمل بالنيابة عنه وبحسب طبيعة النشاط المحدد في العقد المبرم بينهما .

21- **نظام التسوية الاجمالية الانية :** نظام تسوية اجمالي في الوقت الفعلي ، يوفر الية يتم من خلالها حصول كل من المعالجة والتسوية النهائية على أساس كل معاملة على حدا ، لأوامر الدفع الالكتروني المتبادلة بين المشاركين بالنظام .

22- **نظام المقاصة الالكترونية :** هو نظام يمكن المشاركين من تبادل أوامر الدفع الالكتروني والصكوك فيما بينهم بطريقة الكترونية

23- **يوم العمل :** أوقات الدوام الرسمي التي يحددها البنك المركزي العراقي.

24- **خدمات الدفع الإلكتروني :** مجموعة النشاطات المتعلقة بتنفيذ وإدارة المعاملات المالية المشروعة وغير المحظورة عبر وسائل إلكترونية ومنها ، التحويلات والدفعات المالية الإلكترونية المختلفة ويتم تنفيذها وإدارتها عبر استخدام أنظمة وبنى تحتية مالية وتقنية مخصصة لهذا الغرض، تتوافق مع الضوابط والمعايير التي يحددها البنك المركزي.

25- **المشغل:** الكيان المسؤول عن تشغيل نظام الدفع الالكتروني .

26- **المشارك :** شخص معنوي مجاز من قبل البنك المركزي للاشتراك بأنظمة المدفوعات العراقية ويسمح له (بشكل مباشر أو غير مباشر) بإرسال واستلام أوامر التحويل من خلال النظام .

27- **مقدم خدمة الدفع الالكتروني :** يشمل كل من مزود خدمة الدفع الالكتروني والمشغل والمشارك.

28- **تحويل الأموال الكترونياً :** اي تحويل للأموال بإيداع أو سحب من حساب محتفظ به لدى مقدم خدمة الدفع الالكتروني بوساطة اي وسائل الكترونية ويشمل نقاط البيع ، ومعاملات أجهزة الصراف الآلي ، وايداعات مباشرة أو سحوبات للأموال ، والتحويلات بوساطة الهاتف النقال ، أو الانترنت، أو البطاقة ، أو أي وسائل الكترونية أخرى.

29- **أداة الدفع الالكترونية :** أية وسيلة الكترونية معتمدة من البنك المركزي تمكن من اجراء عمليات الدفع الالكتروني أو السحب أو التحويل الالكتروني للأموال .

أ. أدوات الدفع الالكتروني الدائنة : أي وسيلة دفع إلكترونية معتمدة من البنك المركزي يصدرها المصرف أو مقدم خدمات الدفع الالكتروني المرخص دون توفر رصيد في حساب العميل .

ب. أدوات الدفع الالكتروني المدينة : أي وسيلة دفع إلكترونية مرتبطة بحساب مصرفي معتمدة من البنك المركزي يصدرها المصرف حصراً شريطة توفر رصيد في حساب العميل .

ج. أدوات مدفوعة مسبقاً : أي وسيلة دفع إلكترونية معتمدة من البنك المركزي يصدرها المصرف أو مقدم خدمات الدفع الالكتروني المرخص وتكون محملة مسبقاً بأموال العميل .

30- **قناة الدفع الالكترونية :** هي وسيلة الكترونية تمكن العميل من الوصول الى استخدام حساب الدفع الالكتروني والخدمات المرتبطة ومن خلال ادوات الدفع الالكتروني لإجراء عمليات الدفع الالكتروني ، ومنها التطبيقات الهاتفية ونقاط البيع والبوابات الالكترونية واجهزة الصراف الالي .

31- **المصدر:** الكيان المسؤول عن اصدار ادوات الدفع الالكتروني والاوراق المالية .

32- **المحصل :** الكيان المسؤول عن تزويد الأدوات اللازمة لتحصيل المدفوعات الالكترونية من الجهات المصدرة

33- **المعالج :** الكيان المسؤول عن معالجة معاملات الدفع الالكتروني .

34- **نظام الدفع الالكتروني:** مجموعة من الوسائل والاجراءات والقواعد الخاصة بعملية تحويل الاموال بين المشاركين داخل النظام على ان يكون انتقال الاموال من خلال استخدام البنية التحتية لأنظمة الدفع الالكتروني.

35- **امن المعلومات :** هي مجموعة من الاجراءات والتدابير والادوات الخاصة بحماية المعلومات واصولها وتضمن الحفاظ على سلامتها وسريتها وتوافرها ومتطلبات استخدامها والوصول اليها ، ويعد أمن البيانات والأمن السيبراني للوقاية من المخاطر الإلكترونية والاستجابة لها جزء من نطاق امن المعلومات .

المادة (2) : نطاق التطبيق واهداف الضوابط

أوّلًا: نطاق التطبيق :

تسري احكام هذه الضوابط على النطاق الاتي :

1- جميع مقدمي خدمات الدفع الالكتروني (مصارف، شركات مقدمي خدمات الدفع الالكتروني) المرخصين من قبل البنك المركزي العراقي لتقديم خدمات الدفع الالكتروني.

2- فروع المصارف وشركات مقدمي خدمات الدفع الالكتروني الأجنبية العاملة في العراق حيث يقع على عاتقها الالتزام الكامل بالقوانين والتعليمات والضوابط والمعايير المحددة من قبل البنك المركزي العراقي، مع مراعاة اعلام هذا البنك في حال كان هناك اختلاف في متطلبات مكافحة غسل الأموال وتمويل الإرهاب هذا البنك وبلد المركز الرئيسي لتلك الفروع والشركات.

3- فروع المصارف وشركات مقدمي خدمات الدفع الالكتروني العاملة خارج العراق والى المدى التي تسمح به القوانين والأنظمة السارية في الدول التي تعمل بها، واخطار هذا البنك بأية موانع او قيود يمكن ان تحد او تحول دون تطبيق احكام القوانين والتعليمات والضوابط المشرعة في العراق.

4- جميع الأنشطة والمعاملات المالية التي تتم من خلال مقدمي خدمات الدفع الالكتروني المرخصين من قبل هذا البنك.

ثانيًا: الأهداف :

1- التأكد من امتثال مقدمي خدمات الدفع الالكتروني كافة في جمهورية العراق بالالتزام بأحكام قانون مكافحة غسل الأموال وتمويل الإرهاب العراقي رقم (39) لسنة 2015 وتعليمات العناية الواجبة رقم (1) لسنة 2023 وتوصيات مجموعة العمل المالي (FATF).

2- ضمان سلامة المعاملات المالية وحماية مقدمي خدمات الدفع الالكتروني من أي تبعات قانونية دولية او محلية نتيجة القصور في إجراءات مكافحة غسل الأموال وتمويل الإرهاب.

3- ضمان خضوع كافة العمليات المالية عبر أنظمة الدفع الالكتروني إلى أعلى مستويات التدقيق والرقابة، من خلال استخدام تقنيات حديثة لتحليل الأنماط المالية غير المعتادة والتعاون مع الجهات الدولية لضمان تبادل المعلومات بشكل فعال ومواجهة التحديات العالمية المرتبطة بالجرائم المالية، وضمان الامتثال التام للقوانين والتعليمات والضوابط المحلية والدولية.

4- حماية سمعة القطاع المالي بصورة عامة والبنك المركزي العراقي بصورة خاصة والحفاظ عليه من مخاطر السمعة.

5- بيان كيفية الإبلاغ عن حالات الاشتباه المحتملة المشكوك بها لمقدمي خدمات الدفع الالكتروني بما يتوافق وآليات الإبلاغ المعتمدة لدى مكتب مكافحة غسل الأموال وتمويل الإرهاب.

6- تحديث السياسات واجراءات مقدمي خدمات الدفع الالكتروني بما يتلاءم مع السياسات والقوانين والتعليمات ذات الصلة بالامتثال ومكافحة غسل الاموال و تمويل الارهاب مع منهجية ومعايير مجموعة العمل المالي FATF.

7- تعزيز استخدام التقنيات الحديثة والتكنلوجيا المتقدمة لاجراء عمليات التحليل للعمليات المشبوة وضمان الامتثال.

المادة (3): مراحل غسل الأموال ومفهوم تمويل الإرهاب

اولاً: مراحل غسل الأموال

تمر عملية غسل الأموال بثلاث مراحل أساسية مترابطة ببعضها البعض على النحو الآتي:

1- **المرحلة الأولى: مرحلة الإيداع**

يتم في هذه المرحلة التخلص من الاموال المشبوهة أو غير المشروعة من خلال إيداعها أو توظيفها أو استثمارها في مكونات النظام المالي الرسمي بشكل مباشر من خلال مقدمي خدمات الدفع الالكتروني، أو بشكل غير مباشر من خلال الانشطة التي يمكن من خلالها استثمار أو التعامل في الاموال كالعقارات والمعادن الثمينة والاحجار الكريمة وغيرها من الأنشطة.

2- **المرحلة الثانية: مرحلة التغطية أو التمويه**

وهي مرحلة فصل العائدات غير المشروعة عن مصادرها من خلال إجراء مجموعات معقدة من المعاملات المالية لإخفاء مصدر الأموال وملكيتها إذ تتجسد هذه المرحلة في القيام بعمليات إبعاد الأموال غير المشروعة ونقلها محليًا أو خارجيًا (في الغالب إلى البلدان المتشددة في تطبيق قوانين السرية المصرفية)، وغالبًا ما تتسم هذه العمليات بالتعقيد ليصعب تتبع مصدر الأموال غير المشروعة.

3- **المرحلة الثالثة: مرحلة الدمج**

هي عملية اضفاء الصفة الشرعية على المتحصلات غير المشروعة من خلال إعادة ضخ الأموال غير المشروعة إلى الاقتصاد المحلي والعالمي كأموال مشروعة وذلك على سبيل المثال لا الحصر عبر شراء الأسهم والسندات والعقارات....الخ، وبالتالي يكون قد تم طمس القرائن كافه التي يمكن أن تدل على المصدر الحقيقي غير المشروع.

ثانياً: مفهوم تمويل الإرهاب

هي عملية استخدام الاموال بهدف تغذية هدف ارهابي او مجموعة او كيان ارهابي بصورة مباشرة او غير مباشرة لاسباب عقائدية إذ إنَّ الطرق المختلفة التي تستخدم في غسل الأموال تتفق بصورة أساسية مع تلك الأساليب والطرق المستخدمة لإخفاء مصادر تمويل الإرهاب واستخداماته حيث نجد أنّ الأموال التي تستخدم في مساندة الإرهاب يمكن أن تنشأ عن مصادر مشروعة أو أنشطة إجرامية أو كليهما إلاّ أن تمويه مصدر تمويل الإرهابي يتسم بالأهمية بغض النظر عما اذا كان مصدره من منشأ مشروع أو غير مشروع.

المادة (4): إجراءات التعرُّف على العميل و بذل العناية الواجبة

اولاً:- مبدأ اعرف عميلك (KYC)

التأكد من استيفاء العميل لنموذج اعرف عميلك (KYC) للأشخاص الذين يرغبون بالاستفادة من خدمات إصدار بطاقات دفع الكتروني/ فتح محفظة الكترونية لدى مقدم خدمة الدفع الالكتروني، والامر ذاته بالنسبة للكيانات والتجار المزمع تجهيزهم بقنوات التحصيل والجباية ومنها (POS، Payment Gateway)، كما يجب على مقدمي خدمات الدفع الالكتروني كافة التعرف على هوية العملاء المتعاملين معها سواء كانوا محليين او اجانب من خلال الحصول على المعلومات و المستندات التالية:

1 – إذا كان العميل شخصًا طبيعيًا:

أ- الاسم الكامل للعميل، جنسيته، تاريخ الولادة ومكانها، العنوان الدائم، بطاقة السكن، رقم بطاقة الهوية ومكان اصدارها وتاريخ اصدارها، رقم جواز السفر، مكان إصدار جواز السفر وتاريخه، اسم الأم، الحالة الاجتماعية.

ب- النشاط الاقتصادي للعميل وطبيعة عمله ومصادر دخله، المسمى الوظيفي، اسم صاحب العمل أو الجهة صاحبة العمل، قيمة الدخل الشهري، قيمة مصادر الدخل الأُخرى، والحصول على نسخة عن المستند الذي يثبت ذلك النشاط على وفق درجة المخاطر.

ج- معلومات الإقامة في بلدان أُخرى (**إن وجدت**).

د- معلومات الاتصال بالعميل، وتتمثّل بأرقام هواتف العميل وعنوان بريدهُ الالكتروني (**إن وجدت**).

هـ- أيّة معلومات ووثائق أُخرى يرى مقدمي خدمات الدفع الالكتروني ضرورة الحصول عليها للتعرف على هوية العميل.

و- ختم الوثائق المستحصلة من العميل بختم خاص يحمل عبارة (تستخدم هذه الوثائق لأغراض علاقة التعامل اسم مقدم خدمة الدفع الالكتروني حصرًا).

ز- يقوم (منظم الاستمارة – مدير قسم الإبلاغ أو معاونه في الفرع الرئيس – مدير الفرع) بتوقيع استمارة اعرف عميلك، ويتم تحديث بيانات الاستمارة بصورة دورية مع إبلاغ مكتب مكافحة غسل الأموال وتمويل الإرهاب في حالة وجود شبهات، مع عدم تنبيه العميل.

2- إذا كان العميل شخصًا معنوياً:

إذا كان العميل شخصًا معنوياً فيتم استيفاء البيانات والوثائق المثبتة لطبيعة الشخص، وكيانه القانوني وصحة المستندات والوثائق التي تؤيد وجود هذا الكيان، واسمه، وموطنه وتكوينه المالي وأوجه نشاطه بالتفصيل، وبيانات الأشخاص المفوضين بالتعامل على الحساب بموجب تفويض رسمي وكذلك أسماء وعناوين المساهمين الرئيسين وأعضاء مجلس الإدارة والادرة التنفيذية وذلك باتّباع الإجراءات الآتية في الأقل :

أ- التأكّد من استيفاء العميل لأُنموذج اعرف عميلك (KYC)، على أن تكون النماذج مقسّمة على مستوى المركز الرئيس والفروع وأن تتضمن تلك النماذج حدًّا أدنى من المعلومات والبيانات الواردة في الإعمامات الصادرة من هذا البنك والتوقيع عليها أمام الموظف المختص.

ب- يجب على مقدم خدمة الدفع الالكتروني استيفاء الوثائق المدرجة ادناه:

- صورة طبق الأصل من عقد التأسيس وشهادة التأسيس الصادرة عن دائرة تسجيل الشركات.
- صورة طبق الأصل من السجل التجاري.

- اسم المالك وعنوانه وأسماء الشركاء أو المساهمين الذين تزيد ملكيات كلّ منهم على (10%) فأكثر من رأسمال المنظّمة أو الشركة وعناوينهم.
- أسماء المفوضين بالتوقيع عن الشركة والمديرين التنفيذيين وعناوينهم.
- نماذج التوقيع للأشخاص المصرّح لهم بالتعامل على الحساب .
- إقرار خطي من العميل يبيّن فيه هوية المستفيد الحقيقي من الحساب أو صاحب الحق الاقتصادي للعملية التي في النية إجراؤها، ويتضمن اسمه الكامل ولقبه وشهرته ومحل إقامته، وبيانات عن وضعه المالي.

ت- يتعيّن على مقدم خدمة الدفع الالكتروني التعرف على المستفيد الحقيقي واتخاذ إجراءات مناسبة للتحقق من هويته كالاطلاع على بيانات أو معلومات يتم الحصول عليها من جهة الإصدار، بحيث تولد القناعة لدى الجهات بأنّها على علم بهوية المستفيد الحقيقي على أن يُراعَى لدى التعرف على المستفيد الحقيقي من الشخص الاعتباري وذلك عن طريق ما يأتي:

- الأشخاص الطبيعيون الذين يمتلكون حصة مسيطرة على الكيان الاعتباري.
- الأشخاص الطبيعيون الذين يسيطرون على الكيان الاعتباري أو الترتيب القانوني من خلال أيّة وسيلة أُخرى والتأكّد من أنّ المؤسس أو أي شخص آخر في هيكل الملكية والإدارة غير مدرج ضمن قوائم الحظر والعقوبات الدولية والمحلية التي تنشر على الموقع الرسمي لمكتب مكافحة غسل الأموال وتمويل الإرهاب وجميع الجهات الأُخرى ذات العلاقة.
- في حال وجود أي مؤشر اشتباه يتم التأكّد من صحة صدور الأوّليات المُقدَّمة من الكيان المعنوي.

أ- قرار رئيس مجلس إدارة الشركة بفتح الحساب ومَن له الحق في التعامل مع التعرف عليه أو عليهم.

ب- صورة من البطاقة الشخصية (الوطنية) أو جواز السفر لصاحب المنظّمة أو الشركة.

ج- المتضامنون أو الشركاء الذين تكون حصتهم في رأس مال الشركة (10%) فأكثر والمخوّلون بالتوقيع عن الشركة.

د- المستندات الدالة على وجود تخويل من المنظّمة أو الشركة للشخص أو الأشخاص الطبيعيين الذين يمثّلونها.

هـ- أية وثائق أُخرى لم يتم ذكرها التي قد يراها مقدم خدمة الدفع الالكتروني ضرورية.

و- على مقدم خدمة الدفع الالكتروني التأكّد من قيام الموظف المختص بالاطلاع على الوثائق الأصلية والتوقيع على الصور المحتفظ بها، بما يفيد أنّها صور طبق الأصل وفي حال تمّ تأشير وجود أي مؤشر اشتباه بشأن ما يُقدَّم من صحة بيانات ومعلومات أو مستندات أو وثائق يتعيّن مقدم خدمة الدفع الالكتروني اتخاذ إجراءات مناسبة للتحقق من صحتها بجميع الطرائق الممكنة بما في ذلك مفاتحة الجهات المختصة المصدّرة لها.

ز- الشركات المساهمة، فضلًا عن استيفاء الوثائق والمتطلبات الواردة آنفًا يجب استيفاء أسماء وعناوين رئيس مجلس الإدارة او الإدارة العليا والمدير العام والمدير المالي.

ح- اتخاذ الإجراءات الواردة الذكر ضمن هذه الضوابط للتأكد من أنّ العميل شخص معرض للمخاطر بحكم منصبه.

ط- يجب على مقدم خدمة الدفع الالكتروني إيلاء عناية خاصة للأشخاص الاعتباريين والتأكّد من وجودها الفعلي، وذلك عن طريق الحصول على نسخة عن آخر تقرير مالي للشركة أو بياناتها المالية، أو التأكّد من خلال أيّة مصادر أُخرى متاحة.

ي- استيفاء تعهد من العميل بتحديث بياناته فور حدوث أيّة تغيرات بها أو عند طلب مقدم خدمة الدفع ذلك.

ك- التأكّد من صحة البيانات المتوفّرة عن العميل مع الاطلاع على المستندات الأصلية المُقدَّمة منه.

ل- استيفاء أيّة بيانات أُخرى لم يتم ذكرها وقد يراها مقدم خدمة الدفع الالكتروني ضرورية.

3 المنظمات غير الهادفة للربح:

يتوجب على مقدم خدمة الدفع الالكتروني عدم التعامل مع المنظمات غير الهادفة للربح إلا بعد استيفاء الوثائق والبيانات الآتية :

أ- خطاب صادر عن الجهة المنظّمة لعمل هذه المنظمات يؤكد شخصيتها والسماح لها بفتح الحسابات المصرفية.

ب- صورة طبق الأصل من النظام الأساس.

ج- صورة طبق الأصل من قرار الترخيص.

د- اسم المنظّمة وشكلها القانوني.

هـ- عنوان المقر الرئيس والفروع.

و- رقم الهاتف مع البريد الالكتروني إن وُجدَ.

ز- يجب على مقدم خدمة الدفع الالكتروني بذل عناية خاصة فيما يتعلق بالمنظمات والجمعيات التي لا تهدف للربح والتأكّد من وجودها الفعلي ومن أنّ طالبي التعامل هم المسؤولون الحقيقيون عن المنظّمة أو الجمعية وتطبيق إجراءات العناية الواجبة المعززة تجاه المنظمات غير الهادفة للربح عند الحالات الآتية:

1- تتخذ التدابير فيما إذا كان هنالك علاقة بين المنظّمة وبين أصحاب المناصب العليا ذوي المخاطر.

2- النشاطات والأعمال التي لا يكون لها هدف اجتماعي أو سند قانوني واضح، وينبغي وضع الإجراءات الرقابية المعززة اللازمة للوقوف على خلفية الظروف المحيطة بهذا النشاط وأن تُدوَّن تلك النتائج في سجلات خاصة.

3- العمليات التي تتعامل بها المنظمات غير الهادفة للربح التي يتواجدون أو ينتمون إلى دول لا تتوفّر لديها نظم في مكافحة غسل الأموال وتمويل الإرهاب ولا سيّما إذا ما كانت هذه الدول لا تطبق الضوابط العالمية الخاصة في مكافحة غسل الأموال وتمويل الإرهاب أو تطبقها بصورة غير كافية والمنشورة على الموقع الرقمي الخاص بمجموعة العمل المالي.

4- عند وجود أي مؤشر اشتباه تجاه المنظّمة غير الهادفة للربح متعلق بعملية غسل أموال أو تمويل إرهاب أو حالة تثير الشكوك متعلقة بصحة ودقة المعلومات والبيانات التي تمّ الحصول عليها مسبقًا.

5- النشاطات والأعمال التي تمارسها المنظّمة التي يشتبه بأنّها تمويل بشكل غير قانوني سواء كانت بوسائل عينية أم رقمية أم غيرها.

6- النشاطات والأعمال التي يتم تمويلها أو دعمها من أصحاب المناصب العليا ذوي المخاطر.

ثانياً :- تدابير العناية الواجبة

1- **معايير العناية الواجبة:** يجب على مقدمي خدمات الدفع الالكتروني اتخاذ تدابير العناية الواجبة تجاه عملائها بما يتوافق و ينسجم مع المادة (10) من قانون مكافحة غسل الاموال و تمويل الارهاب رقم 39 لسنة 2015 وتعليمات العناية الواجبة رقم (1) لسنة 2023 و ذلك من خلال:-

أ- توفير سياسة مكتوبة ومعتمدة من مجلس إدارة مقدمي خدمات الدفع الالكتروني او الإدارة العليا بالنسبة للمقدمين الذين لا لايمتلكون مجلس إدارة ، في مجال مكافحة غسل الأموال وتمويل الإرهاب والامتثال تشمل تعريف هوية العملاء وتحديدها.

ب- حفظ جميع السجلات والمستندات اللازمة لإثبات الهوية الشخصية لهؤلاء العملاء لدى التعامل معهم (لفترة لا تقل عن خمسة سنوات من تاريخ انتهاء علاقة العمل مع العميل او من تاريخ تنفيذ العملية المالية) استنادًا إلى المادة (11) من القانون اعلاه.

ت- تصنيف مخاطر العملاء وعدم استبعاد اسم أيّ عميل يمثّل مخاطر مرتفعة بحكم منصبه تعامل مع مقدمي خدمات الدفع الالكتروني فور تركه منصبه والإبقاء على اسمه مدة لا تقل عن(2 سنة) كحدًّا أدنى في جميع الحالات بوصفه شخصًا يمثّل مخاطر مرتفعة.

ث- اتخاذ تدابير العناية الواجبة المعززة تجاه العملاء عالي المخاطر والاستعلام عنهم في قوائم الحظر المحلية والدولية قبل اجراء اي عملية من العمليات التي يقوم بها مقدم خدمة الدفع الالكتروني.

ج- يقع على عاتق مقدمي خدمات الدفع الالكتروني تطبيق العناية الواجبة اتجاه اصحاب المناصب العليا ذوي المخاطر بما ينسجم مع ضوابط رقم (2) لسنة 2023 الخاصة بالمؤسسات المالية والاعمال والمهن غير المالية المحددة.

2- **توقيتات العناية الواجبة:**

على مقدم خدمة الدفع الالكتروني تنفيذ تدابير العناية الواجبة في الحالات الآتية، فضلًا عن أيّة **حالة عرضية أو غير اعتيادية** ترتبط بسلوك العميل تتطلب اتخاذ إجراءات العناية الواجبة أو المعززة:

أ- قبل إقامة علاقة مع العميل وخلالها.

ب- عند إجراء عملية عارضة تفوق قيمتها ما يحدده مجلس مكافحة غسل الاموال وتمويل الارهاب سواء كانت العملية واحدة أم عمليات عدة تبدو مترابطة.

ت- عند الاشتباه في ارتكاب عملية غسل أموال أو تمويل إرهاب بصرف النظر عن أيّة إعفاءات أو حدود معينة مشار إليها في القانون أو أيّة أنظمة أو تعليمات أو بيانات أو تشريعات أُخرى.

ث- الشك في صحة البيانات التعريفية أو دقتها أو كفايتها التي حصل عليها مسبقًا عن هوية العميل.

ج- عند إجراء عملية عارضة في صورة تحويلات الكترونية حسب سقوف المبالغ التي يحددها هذا البنك.

ح- النشاطات غير الاعتياديه التي تُعدُّ مريبة وبما يتوافق والسيناريوهات الصادرة عن هذا البنك و مكتب مكافحة غسل الأموال وتمويل الإرهاب.

3- العناية الواجبة المعززة:

اضافة الى تدابير العناية الواجبة المنصوص عليها ضمن هذا الضوابط يلتزم مقدم خدمة الدفع الالكتروني باجراءات العناية الواجبة المعززة تجاه الاتي:-

أ- جميع العمليات المالية الالكترونية المعقدة والكبيرة وغير الاعتيادية وجميع الانماط غير المعتادة للعمليات المالية، التي ليس لها غرض اقتصادي او قانوني واضح وذلك لأقصى حد ممكن وبصورة معقولة.

ب- العميل غير المقيم: لكونه يُعدُّ من العملاء مرتفعي المخاطر نتيجة عدم وجود سكن محدد داخل العراق، وعلى مقدمي خدمات الدفع الالكتروني التأكّد من سريان الإقامة قبل تنفيذ بدء التعامل معهم وتشمل فئة العملاء غير المقيمين العملاء سواء كانوا أشخاصًا طبيعيين أم أشخاصًا اعتباريين الذين لا يوجد لهم محل إقامة أو عنوان دائم في العراق، ويجب مراعاة ما يأتي عند القيام بإجراءات التعرف على هؤلاء العملاء وأوضاعهم القانونية. تطبيق العناية الواجبة المعززة على العميل غير المقيم ويُراعَى عدم التعامل بأيّ شكل من الأشكال مع العميل غير المقيم ما لم يستوفِ الشروط الآتية:

- معرفة الغرض من التعامل.
- معرفة سريان الإقامة في الجمهورية العراقية عند بدء التعامل.
- الحصول على نسخة من وثيقة الهوية وجواز السفر.
- الحصول على عقد التأسيس للشخصية الاعتبارية مصدَّق عليها من السلطات المختصة في البلد الأم أو من سفارة البلد في جمهورية العراق .

ح- الأعمال والمهن غير المالية المحددة: تشمل المحامين وتجار المعادن النفيسة والصاغة والوكلاء العقارين (الدلاليين) والمحاسبين ، إذ يجب تطبيق العناية الواجبة المعززة تجاه الأعمال والمهن غير المالية المحدّدة من الجهات المختصة بترخيص أو إجازة الأعمال والمهن غير المالية المحدّدة، أو الإشراف عليها والتأكّد من التزامها بالمتطلبات التي تستلزمها على وفق قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 39 لسنة 2015، وتشمل وزارة التجارة ووزارة الصناعة والبنك المركزي العراقي وهيأة الأوراق المالية وديوان التأمين وأية جهة أُخرى يصدر قرار باختصاصها بوصفها جهة رقابية بقرار مجلس الوزراء بناءً على اقتراح المجلس وينشر في الجريدة الرسمية، وفي ما يأتي تفاصيل هذه المهن والجهات المرخصة والمنظّمة لعملهم:

- المحامين: تتولى نقابة المحامين العراقيين مهمة الترخيص للمحامين لأجل مزاولة أعمالهم وعلى مقدمي خدمات الدفع الالكتروني التأكّد من صحة رخصة العمل والانتماء إلى هذا النقابة.

- الوكلاء العقاريون (الدلالون): تتولى وزارة التجارة/غرفة التجارة مهمة إعطاء الرخص للوكلاء العقاريين .
- الصاغة وتجار المعادن النفيسة: تتولى وزارة التخطيط الجهاز المركزي للتقييس والسيطرة النوعية مهمة إعطاء الرخص للصاغة وتجار المعادن الثمينة، إذ يجب على مقدمي خدمات الدفع الالكتروني التأكّد من صحة رخصة العمل الصادرة عن وزارة التخطيط وعدم نفاذها والتأكّد من دورية تجديدها في المواعيد المحددة أو تقديم تعهد بتجديدها خلال مدّة لا تتعدى (3) أشهر من تاريخ النفاذ.
- المحاسبين: تقع على عاتق نقابة المحاسبين العراقيين مهمة إعطاء الرخص للمحاسبين بعد استيفائهم جميع الشروط الخاصة بنقابة المحاسبين ومجلس مراقبة المهنة.

إنّ الأعمال والمهن المالية غير المحددة المذكورة آنفًا لا تتساوى من حيث الأهمية النسبية ودرجة المخاطر التي تتعرّض لها، إلّا أنّها جميعًا مرتفعة المخاطر وتتطلب عناية واجبة معززة من مقدمي خدمات الدفع الالكتروني.

- كُتّاب العدل: على الرغم من اعتبار مجموعة العمل المالي مهنة كُتّاب العدل بضمن المهن المالية غير المحددة إلّا أنّها لا يمكن عَدُّها بضمن هذه المهن في العراق لكونها مهنة تابعة للدولة، إذ يتبع الكتاب العدول لـ(دائرة كتاب العدول / وزارة العدل) استنادًا إلى قانون كتاب العدول رقم (33) لسنة 1998، وعلى الرغم من ذلك يجب تطبيق العناية الواجبة المعززة تجاه كُتّاب العدل لكونهم بدرجة (مديرين عامين) استنادًا إلى القانون المذكور آنفًا وأنّ جميع المديرين العامين يتم معاملتهم على أنّهم بضمن الأشخاص المعرضين للمخاطر بحكم منصبهم.

د- أصحاب المناصب العليا ذوو المخاطر يجب استيفاء ما يأتي :

تُطبّق العناية الواجبة المعززة تجاه أصحاب المناصب العليا ذوي المخاطر والذين يشغلون أيّ من المناصب أو الوظائف الآتية، سواء كانوا محليين أم أجانب وأفراد عائلاتهم وذوي الصلة بهم:

- رئيس الجمهورية ونوابه ومستشاروه ومَن بدرجتهم.
- رئيس مجلس الوزراء ومستشاريه وأعضاء مجلس الوزراء ومَن بدرجتهم.
- رؤساء الأحزاب السياسية.
- رئيس مجلس النواب وأعضاؤه.
- رئيس مجلس القضاء الأعلى وأعضاؤه.
- رؤساء الهيئات المستقلة ومَن بدرجتهم.
- وكلاء الوزارات والمستشارون والمفتشون ومَن بدرجتهم.
- السفراء والمفوضون والمستشارون الدبلوماسيون.
- المديرون العامون ومَن بدرجتهم.
- قضاة المحاكم على اختلاف درجاتهم.
- القادة والمراتب العليا في الأجهزة الأمنية ومَن بدرجتهم.
- رؤساء المؤسسات الجمعيات الخيرية والمنظمات غير الحكومية ووكلاؤها ومديروها، وأعضاء مجلس إداراتها ومَن بدرجتهم.

هـ- يجب على مقدم خدمة الدفع الالكتروني اتخاذ الإجراءات المناسبة لبذل عناية خاصة للعمليات التي تتم مع الأشخاص الذين ينتمون إلى دول لا تطبق توصيات مجموعة العمل المالي أو لا تطبقها بالشكل المطلوب بما في ذلك الأشخاص الاعتباريون و مقدمي خدمات الدفع الالكتروني الأخرى واتخاذ إجراءات معززة حيالها، ومن أمثلة تلك الإجراءات ما يأتي :

- المراقبة الدقيقة للعمليات الخاصة بهؤلاء العملاء، والتعرف على الغرض منها، وإخطار مكتب مكافحة غسل الأموال وتمويل الإرهاب في حالة عدم توفّر غرض اقتصادي واضح أو توفّر أيّة شكوك بشأنها.
- الحد من علاقات العمل أو المعاملات المالية مع الدول المشار إليها أو الأشخاص الذين ينتمون إلى تلك الدول أو يتواجدون فيها.

و- العناية الواجبة والعناية الواجبة المعززة تجاه مشاهير السوشيال ميديا: على مقدمي خدمات الدفع الالكتروني اتخاذ أقصى درجات الحيطة والحذر على الحركات المالية التي تتم من خلال (الحسابات المصرفية والمَحافظ الالكترونية وبطاقات الدفع الالكتروني بأنواعها) الخاصة بمشاهير السوشيال ميديا، فضلًا عن تطوير سيناريوهات اكتشاف عمليات غسل الأموال الخاصة بهذه الشخصيات وبما يتناسب وهذه الحالات بالتنسيق مع مكتب مكافحة غسل الأموال وتمويل الإرهاب إن تطلب الأمر، وكذلك يجب اتخاذ إجراءات العناية الواجبة المعززة على الحركات المالية لأصحاب المتاجر الرقمية ومنها (أصحاب مواقع التسويق الرقمي والتسويق عبر وسائل التواصل الاجتماعي).

4- العناية الواجبة المبسطة:

يجوز لمقدم خدمة الدفع الالكتروني اتخاذ تدابير العناية الواجبة المبسطة كجزء من التدابير المبسطة وذلك في حال استيفاء الشروط التالية:-

أ- وجود تحليل كافي لمخاطر للعملاء الذين يتعامل معهم مقدم خدمة الدفع الالكتروني وفهم وتحليل المخاطر المحيطة بهم.

ب- عندما تكون مخاطر غسل الاموال وتمويل الارهاب المحيطة بالعميل منخفضة ولا يوجد اية مؤشرات اشتباه تجاه العميل.

ج- المبالغ النقدية التي يقوم بإيداعها العميل صغيرة ولا توجد اي مؤشرات مخاطر ريبة او شك حولها.

5- حظر التعامل:

يحظر على مقدم خدمة الدفع الالكتروني ما يأتي:

أ- التعامل مع الأشخاص مجهولي الهوية أو الأشخاص الذين يحملون أسماء صورية أو وهمية.

ب- التعامل مع أيّ شخص طبيعي أو معنوي يقدم نشاطات أو خدمات أو عمليات دون ترخيص أو تسجيل سواء كان لمصلحة عملاء أو نيابة عنهم، ويستثنى من ذلك التعامل بشكل مبدئي مع مقدمي خدمات الدفع الالكتروني قيد التأسيس أو الأعمال والمهن غير المالية المحدّدة.

ج- التعامل مع جميع الكيانات رموز فئة التاجر (MCC) التي يحددها البنك المركزي كفئات يمنع التعامل معهم.

د- جميع الكيانات والعلامات التجارية والأشخاص المدرجين على قوائم الحظر المحلية والدولية.

6- تحديد المستفيد الحقيقي:

يجب على مقدم خدمة الدفع الالكتروني اتخاذ جميع الإجراءات اللازمة والمعقولة على وفق مخاطر غسل الأموال وتمويل الإرهاب التي تنشأ عن العميل وعلاقة العمل لأجل تحديد المستفيدين الحقيقيين والتأكد من هويتهم بالاعتماد الوثائق الرسمية وبما يكوّن القناعة بعلم المؤسسة بهوية المستفيد الحقيقي وكالآتي:

أ- في حال كان العميل شخصًا طبيعيًا: يجب تحديد ما إذا كان العميل من يقوم بالمعاملات المالية الالكترونية بالأصالة عن نفسه، والتأكد من هويتهم بالاعتماد على المعلومات المثبتة في الوثائق الرسمية في حال كان العميل موجود لدى الوكلاء او مقرات مقدمي خدمات الدفع الالكتروني ، اما اذا كان العميل يرغب بأجراء التسجيل الرقمي، يقع على عاتق مقدمي خدمات الدفع الالكتروني تطبيق تقنيات التحقق الرقمي من الوثائق للتأكد من صحتها واصالتها وتحليلها لضمان ان المستفيد الحقيقي من يقوم بأجراء المعاملة الالكترونية.

ب- في حال كان العميل شخصًا معنويًا: يتم تحديد هوية المستفيد الحقيقي عن طريق هيكل الملكية، إذ يجب تحديد هوية الأشخاص الطبيعيين الذين لهم حصة ملكية مسيطرة فعلية على الشخص المعنوي سواء بشكل مباشر أم غير مباشر، وكذلك تحديد المساهم الذي يمارس السيطرة الفعلية على الشخص المعنوي بصرف النظر عن نسبة مساهمته، سواء بمفرده أم مع المساهمين الآخرين بطريقة مباشرة.

7- التحقق من صحة المستندات:

1- التحقق البصري من الوثائق الرسمية والذي يشمل التأكد من أصالتها وعدم انتهاء صلاحيتها، والتأكد من خلوها من التلاعب والتزوير، بالإضافة إلى توفر العلامات الأمنية والخصائص الأخرى.

2- التأكد من أن كافة الوثائق تحتوي على نفس المعلومات الأساسية بدقة ودون تناقضات، حيث يتضمن ذلك الاتي:

أ- التحقق من الاسم الكامل للعميل كما هو مدون في جميع الوثائق والمستمسكات الثبوتية.

ب- تاريخ الميلاد وأي معلومات أخرى مثل رقم الهوية او الجواز، فضلاً عن التأكد من أن تواريخ الوثائق مثل تواريخ الاصدار، متطابقة ولا تتعارض أو تظهر تباينات غير مفهومة.

ج- التحقق من عدم وجود أي تباينات أو اختلافات في اللغة بين الوثائق المختلفة، لضمان أنها جميعًا تعكس نفس البيانات والدقة.

3- استخدام البرمجيات الحديثة وتطبيق تقنيات متقدمة لضمان الاتي:

أ- التحليل الدقيق للصور الرقمية للوثائق، مما يسهل التعرف على العلامات الأمنية والتأكد من صحتها، حيث يتم استخدام خوارزميات الذكاء الاصطناعي للكشف عن أي تعديلات غير مشروعة أو تزوير في الصورة.

ب- مقارنة البيانات البيومترية مثل البصمات أو الصور الشمسية للوجه بين الوثائق المقدمة والمصادر الأصلية، مما يساعد في التحقق الفوري من الهوية ويقلل من الوقت المطلوب لإتمام العملية.

4- فيما يتعلق بالتطبيقات الإلكترونية لمقدمي خدمات الدفع الإلكتروني، يقع على عاتقكم اتخاذ الإجراءات الضرورية لضمان أن يُستخدم تطبيق الهاتف النقال من قبل مستخدم واحد فقط، لضمان تعزيز الأمان والحماية ضد الوصول غير المصرح به والاحتيال حيث يجب اتخاذ الإجراءات التالية بالحد الادنى :-

أ- استخدام تقنيات التحقق البايومتري (Biometric Verification) مثل التعرف على الوجه، لتأمين عملية تسجيل الدخول إلى التطبيق، يتم من خلالها مطابقة ملامح الوجه للمستخدم المسجل مسبقًا بالصورة المخزنة.

ب- التأكد من ان التطبيق يعمل بالجهاز الخاص بالعميل فقط، مثل تحديد رقم الهاتف المحمول أو رمز تعريف الجهاز.

ت- ربط كل تطبيق بحساب فريد (Unique Account) لكل مستخدم، مما يمنع أي محاولات للاستخدام المتعدد من قِبَل أشخاص غير مخولين .

ث- مراقبة وتتبع نشاطات الدخول إلى التطبيق بشكل دوري، مع إجراءات للتحقق من الأنشطة غير العادية أو المشكوك فيها التي قد تدل على استخدام غير مصرح به .

ج- توفير وسائل لإدارة الحسابات بشكل آمن، مثل تغيير كلمات المرور أو تعطيل الحسابات في حالات الشك أو الاختراق المحتمل.

5- إجراء مكالمات فيديوية مسجلة للتحقق من العميل وهويته متى ما تطلب الأمر ذلك، على ان يتم اعلام العميل بان المكالمة مسجلة وسيتم الاحتفاظ بالتسجيل .

8- طلب البيانات :

يقع على عاتق مقدم خدمة الدفع الإلكتروني مسؤولية وضع سياسات وإجراءات تتعامل مع الحالات التي تستوجب طلب تقديم وثائق إضافية غير الوثائق الأساسية المعتمدة للمعاملة من قبل العميل، لزيادة مستوى التحقق عند الضرورة، هذا يشمل تحديد السيناريوهات التي قد تستدعي هذه الخطوة، مثل التحويلات الكبيرة أو غير المعتادة او طلبات رفع السقوف الاستثنائية فيما يخص البطاقات (الدائنة والمدينة) أو النشاطات التي تثير الشكوك بشأن مصداقية المعاملة، مع مراعاة عدم تعقيد الإجراءات بالنسبة للعميل.

المادة (5): البطاقات والمحافظ الالكترونية

1- يخضع جميع العملاء الى إجراءات العناية الواجبة المنصوص عليها ضمن هذه الضوابط واية تعليمات ذات صلة.

2- يمنع استخدام البطاقات والمحافظ الالكترونية لغرض المضاربة والتداول بالعملات الرقمية بجميع أنواعها وإخضاع المتعاملين بها لأحكام قانون مكافحة غسل الأموال وتمويل الإرهاب رقم(39) لسنة 2015 والتعليمات والضوابط والتعاميم الصادرة بموجبه .

3- يكون مقدم خدمة الدفع الإلكتروني عبر الهاتف النقال مسؤولًا عن متابعة العمليات المالية التي تتم من خلال المحفظة الإلكترونية، مع اتخاذ الإجراءات اللازمة للتحقق من هوية العملاء ومراقبة الأنشطة المالية للكشف عن أي معاملات مشبوهة قد تكون مرتبطة باحتيال او غسل الأموال أو تمويل الإرهاب وفي ذات الوقت يكون مقدم خدمة الدفع المصدر للبطاقة المرتبطة بالمحفظة الإلكترونية (M-Card)مسؤولًا عن متابعة العمليات المالية التي تتم من خلال البطاقة بالتنسيق مع مقدم خدمة الدفع الالكتروني عبر الهاتف النقال.

4- يقع على عاتق مقدم خدمة الدفع الالكتروني في حال كان مصرفاً المسؤولية الكاملة بالالتزام بتحديث السقوف اليومية والشهرية المحلية والدولية المحددة من قبل البنك المركزي لجميع أنواع البطاقات التي يصدرها.

5- يقع على عاتق مقدم خدمة الدفع الالكتروني في حال كان شركة دفع الكتروني المسؤولية الكاملة بالالتزام بتحديث السقوف اليومية والشهرية المحلية والدولية المحددة من قبل البنك المركزي لجميع أنواع البطاقات التي تصدرها، فضلاً عن المسؤولية بأعلام المصارف المتعاقد معها لأغراض (الإصدار والمعالجة) لاي تحديثات للسقوف تصدر من البنك المركزي، مع الاخذ بنظر الاعتبار ان هذا الاعلام لا يقلل من المسؤولية المشار اليها في الفقرة رقم (4) اعلاه.

6- يحق لمقدم خدمة الدفع الالكتروني تحديد سقوف يومية وشهرية لبطاقاته وفقاً لسياسته الداخلية والتقييم الذاتي للمخاطر على ان لاتتجاوز الحدود والسقوف المحددة من قبل البنك المركزي، و ان يتم اتخاذ الاجراءات التي تضمن الإفصاح للعملاء عن سقوف العمليات المالية الالكترونية.

7- على مقدم خدمة الدفع الالكتروني مراقبة التحويلات بين المحافظ الالكترونية او البطاقات (P2P) لضمان عدم إساءة استخدامها، مع الأخذ بنظر الاعتبار ما يلي :

أ- الالتزام بسقوف التحويل بين المحافظ الالكترونية او البطاقات (P2P) المعتمدة من قبل البنك المركزي العراقي.

ب- اعتماد سيناريوهات ومؤشرات الاشتباه في انظمتكم تتوافق مع هذا النوع من العمليات.

ج- تحليل جميع عمليات التحويلات الالكترونية عن طريق انظمة متخصصة مرتبطة بنظام مكافحة غسل الاموال وتمويل الارهاب (AML) وقياس التكرارات والتركزات والفترات الزمنية ومدى منطقيتها، مع العرض ان يكون هذا التحليل مرتبط باستمارة (KYC) لكل عميل.

د- معرفة المعلومات الرئيسية عن التحويل على سبيل المثال لا الحصر (سبب التحويل، صلة القرابة... الخ).

هـ- يتحمل مقدم خدمة الدفع الالكتروني المسؤولية الكاملة في حال كان هناك قصور في التحليل المشار الية في الفقرة (ج) أعلاه او عدم التعامل مع نتائج التحليل بالطريقة السليمة.

8- تطبيق الإجراءات والاليات الخاصة بالتحقق من استلام الشخص المعني (صاحب البطاقة) حصراً لبطاقة الدفع الالكتروني الخاصة به وتفعيلها من قبله.

9- تخضع جميع التعاملات المالية الإلكترونية الدولية والمحلية، لمختلف أنواع البطاقات الصادرة لزبائن مقدم خدمة الدفع الإلكتروني، لعمليات المراقبة والتحليل عبر أنظمة متخصصة تهدف إلى الكشف عن أي نشاطات مشبوهة قد تكون مرتبطة بغسل الأموال أو تمويل الإرهاب، وذلك امتثالاً للأنظمة والمعايير الدولية والمحلية المعمول بها في هذا الشأن.

10- مراجعة تاريخ المعاملات وتحليل الخلفيات المالية والتجارية للزبائن بشكل شامل من خلال مراجعة أنظمة التحليل المتقدمة للكشف عن أي أنشطة غير معتادة أو مشبوهة.

11- تفرض إجراءات العناية الواجبة المعززة على العملاء الذين يتعاملون في الدول المصنفة عالية المخاطر وفقًا لتصنيف مجموعة العمل المالي(FATF) ، حيث يقع على عاتق مقدم خدمة الدفع الالكتروني تنفيذ إجراءات احترازية للكشف عن أي أنشطة مشبوهة قد تكون مرتبطة بغسل الأموال أو تمويل الإرهاب.

12- يحق لمقدم خدمة الدفع الالكتروني تحديد سقوف يومية وشهرية حسب سياسته الداخلية للحركات المالية الإلكترونية على ان لا تتجاوز الحدود العليا للسقوف المحددة من قبل هذا البنك لمختلف أنواع البطاقات في الدول المصنفة عالية المخاطر وفقًا لتصنيف مجموعة العمل المالي (FATF) على ان يتم الإعلان عن هذه السقوف والدول للعملاء قبل فرضها.

13- ضمان حماية و أمن وخصوصية وسرية بيانات العملاء لمعاملاتهم المالية.

14- تكامل النظام المصرفي الشامل او أنظمة إدارة البطاقات لدى مقدم خدمة الدفع الالكتروني مع أنظمة مكافحة غسل الأموال وتمويل الإرهاب وقوائم الحظر والعقوبات المحلية والدولية.

15- اجراء تقييم دوري لقياس مدى فعالية الأنظمة التكنولوجية المستخدمة في مكافحة غسل الأموال والتأكد من أن الأنظمة تعمل بكفاءة ودقة.

16- يجب التأكّد من أن أنظمة البحث والتحري المعتمدة تدعم عملية التحديث الدوري على قوائم الحظر والعقوبات المحلية والدولية كل (12) ساعة خلال اليوم الواحد في أقل تقدير.

17- بإمكان مقدم خدمة الدفع الالكتروني التعاون مع جهات مستقلة متخصصة ومعتمدة لإجراء تدقيق خارجي على العمليات المالية الالكترونية للحصول على تقييم موضوعي حول فعالية استراتيجيات وسياسات وخطط واجراءات مكافحة غسل الأموال وتمويل الارهاب.

18- ضمان التكامل مع المنظومات وقواعد البيانات المركزية في حال توفرها، للتحقق من معلومات العملاء وبياناتهم الاحيائية والتأكد من صحتها، مع الاخذ بنظر الاعتبار ماجاء في الفقرة (13) اعلاه.

19- تقديم دراسة تتضمن الآليات والسياسة التي سيتم اعتمادها لمكافحة غسل الأموال وتمويل الإرهاب الى البنك المركزي العراقي لاي منتج/خدمة يتم طلب ترخيصه او الموافقة عليه.

20- يقع على عاتق مؤسساتكم المراجعة المستمرة للوثائق والبيانات والمعلومات لضمان تحديثها مع الاخذ بنظر الاعتبار تاريخ انتهاء صلاحية الوثائق التي تم اعتمادها بالتسجيل، حيث يحق لمؤسساتكم اتخاذ اجراء يتناسب مع عدم استجابة العميل لتحديث الوثائق المطلوبة .

المادة (6) : أنظمة الدفع الالكتروني

تمثل أنظمة الدفع الإلكتروني المستخدمة من قبل مقدمي خدمات الدفع الالكتروني ركيزة أساسية لخدمات الدفع الالكتروني، ولكن بالمقابل برزت تحديات أمنية كبيرة، خاصة في مجالات مكافحة غسل الأموال وتمويل الإرهاب، فهذه الأنظمة قد تُستغل لتحويل الأموال لأغراض غير سليمة، مما يعرض النظام المالي للتهديد، وعليه أصبح من الضروري وجود ضوابط وأنظمة رقابة صارمة تضمن منع استخدام هذه الأنظمة لأغراض غير سليمة ، من خلال تعزيز آليات التحقق والتدقيق في المعاملات المالية، واستناداً لما جاء أعلاه نود الإشارة الى الاتي:

1- تطبيق إجراءات اعرف عميلك (KYC) وحفظ جميع بيانات ومعلومات العمليات المالية بما فيها معلومات (الشخص طالب التحويل، مبلغ التحويل والجهة المستلمة، الغرض من التحويل) كما ورد في المادة (5/اجراءات التعرف على العميل وبذل العناية الواجبة) من هذه الضوابط.

2- الالتزام بالسقوف وحدود للعمليات المالية المحددة من قبل هذا البنك، فضلاً عن اجراء عمليات تدقيق إضافية للمبالغ الكبيرة التي تدفع / تستلم من قبل كيانات والأشخاص باستثناء المبالغ الخاصة بالمؤسسات الحكومية.

3- يقع على عاتق المصارف تكامل جميع العمليات المالية الالكترونية المنفذة من قبل أنظمة الدفع الالكتروني بما فيها على سبيل المثال لا الحصر أنظمة (RTGS- ACH) مع النظام المصرفي الشامل للمصرف و نظام مكافحة غسل الأموال وتمويل الارهاب لاكتشاف أي أنماط او تعاملات مشبوهة .

4- يجب أن تكون إجراءات العناية الواجبة مستمرة طوال فترة العلاقة مع العميل، بحيث لا تقتصر فقط على مرحلة بدء العلاقة ، بل تكون عملية مراجعة وتحديث المعلومات والبيانات الخاصة بالعملاء بشكل دوري، والتحقق من مصادر الأموال والمعاملات بانتظام، خصوصًا في الحالات التي قد تطرأ فيها تغييرات على الأنشطة أو الأوضاع المالية للعميل.

5- اعتماد السيناريوهات المعدة من قبل هذا البنك ومكتب مكافحة غسل الأموال وتمويل الإرهاب فضلاً عن السيناريوهات المقترحة من قبلكم المتعلقة بعمليات وانشطة أنظمة الدفع الالكتروني.

6- المراقبة والتحليل والرصد لعمليات التجزئة في اجراء التحويلات المالية الالكترونية ومنع هذه العمليات فضلاً عن تقديم ابلاغ بهذه العمليات في ذات يوم العمل وفق السياقات المعتمدة.

7- يقع على عاتق مقدمي خدمات الدفع الالكتروني التأكد من أن العملاء الذين يتم التعامل معهم ليسوا مدرجين في قوائم الحظر و العقوبات المحلية والدولية قبل اجراء عمليات التحويل المالي، مع التأكد من نوع الادراج في القائمة ونوع العملة المستخدمة في التحويل، حيث يجب أن تكون هناك آلية فعالة للتحقق من هذه القوائم بشكل منتظم لضمان عدم التعامل مع الأشخاص أو الكيانات المرتبطة بأنشطة تمويل الإرهاب أو غسل الأموال.

المادة (7) : قنوات التحصيل والجباية

فضلاً عما جاء في فصل إجراءات التعرُّف على العميل و بذل العناية الواجبة في هذه الضوابط، يقع على عاتق مقدمي خدمات الدفع الالكتروني (المحصلين) عند تجهيز الكيان الاعتباري او التاجر بقنوات التحصيل الالكتروني ومنها (POS، Payment Gateway...الخ)الاتي:-

أ- طلب اسم الكيان الاعتباري وشكله القانوني، عنوان المقر الرئيس والفروع ان وجدت، تاريخ الترخيص ورقمه، أنواع المستندات التي تنظم عمل الشخص المعنوي، ونوع النشاط ورأس المال للكيانات التي يتطلب وجود رأس مال لها.

ب- الحصول على المعلومات اللازمة لفهم طبيعة العميل، هيكل ملكيته والسيطرة عليه، ومَن هو المستفيد الحقيقي وتحديد إن كان هيكل الملكية أو السيطرة معقد أو متعدد الطبقات.

ت- معلومات الأشخاص الطبيعيين المخولين بالتوقيع عن العميل كما هي مطلوبة للشخص الطبيعي على وفق الفقرة (1) من المادة (4) من فصل إجراءات التعرف على العميل وبذل العناية الواجبة من هذه الضوابط.

ث- وضع آلية لمراجعة المعاملات المالية التي تتم عبر قنوات التحصيل الالكتروني بشكل دوري، وتحليل أي معاملات مشبوهة أو غير معتادة.

ج- المعرفة الكاملة عن المنتجات او الخدمات التي يقدمها وهيكل التسعير لها فضلاً عن دورية المدفوعات الالكترونية لمنتجاته او خدماته، واخذ هذه المعطيات لتحليل أنماط الدفع الالكتروني لكل فئة من الكيانات والتجار.

ح- المعرفة الكاملة بنطاق عمل التاجر وفئة العملاء المستهدفين مع الاخذ بنظر الاعتبار الموقع الجغرافي للتجار (منطقة سياحية، منطقة مركز تجاري، منطقة سكنية...الخ) والتي يساعد تحديدها عملية التحليل عند تلقي حركات مالية الكترونية بمالغ عالية او تلقي مبالغ عبر بطاقات لمؤسسات مالية اجنبية.

خ- يمنع التعامل مع الكيانات مجهولي الهوية أو الذين يحملون أسماء صورية أو وهمية او الكيانات التي تعمل دون ترخيص أو تسجيل سواء كان لمصلحة عملاء أو بالنيابة عنهم.

د- يقع على مقدم خدمة الدفع الالكتروني وضع سياسات وإجراءات تحقق إضافية بناءً على تصنيف التجار على أساس المخاطر.

ذ- يقع على عاتق مقدمي خدمات الدفع الالكتروني اتخاذ الإجراءات الفنية التي تضمن عدم استخدام أجهزة السحب النقدي (POS) خارج العراق، وتفعيل الخصائص التي تسمح بمراقبة التحويلات المالية من خلالها ومراقبة مواقعها الجغرافية.

المادة (8) : أجهزة السحب النقدي (ATM- POC)

1- الالتزام بالتعليمات الصادرة من هذا البنك فيما يخص الحدود والسقوف لعميات السحب النقدي.

2- يقع على عاتق مقدمي خدمات الدفع الالكتروني متابعة وتحليل أنماط العمليات المالية الخاصة بالسحب النقدي بشكل يومي واسبوعي (بشكل مفرد وكلي) على ان تشمل عدد وحجم وتركيز عمليات السحب النقدي وبحسب نوع البطاقة والأجهزة التي تستخدم بشكل مكثف.

3- تحليل أنماط العمليات المالية على أجهزة السحب النقدي للبطاقات الصادرة من مؤسسات مالية عاملة خارج العراق وتحديد سقف سحب بما يتلائم مع التعليمات وسياسة مكافحة غسل الاموال وتمويل الارهاب والمخاطر الخاصة بكياناتكم.

4- اعتماد سيناريوهات هذا البنك و مكتب غسل الأموال فيما يتعلق بالسحب النقدي واي سيناريوهات تقترح من قبلكم حسب نتائج تحليل أنماط السلوك المشبوهة.

5- يقع على عاتق مقدمي خدمات الدفع الالكتروني اتخاذ الإجراءات الفنية التي تضمن عدم استخدام أجهزة السحب النقدي (POC) خارج العراق، وتفعيل الخصائص التي تسمح بمراقبة التحويلات المالية من خلالها ومراقبة مواقعها الجغرافية.

6- عند ملاحظة أي نمط او سلوك مشبوهة يتم ابلاغ مكتب مكافحة غسل الاموال وحسب السياقات المتبعة من قبل المكتب.

7- يقع على عاتق مقدم خدمة الدفع الالكتروني اجراء تقييم دوري لسياسات السحب النقدي وعمليات مراجعة مستمرة لمصفوفة المخاطر والتأكد من توافقها مع احدث التعليمات والضوابط المحلية والمعايير الدولية المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب.

8- وضع ضوابط إضافية على المعاملات التي تشمل أجهزة سحب نقدي تقع في دول تعتبر ذات مخاطر عالية (وفقًا لقائمة FATF أو قوائم العقوبات الدولية)، خاصةً تلك التي يتم فيها سحب أو إيداع مبالغ كبيرة.

المادة (9): الحوالات الاجنبية الالكترونية الخارجية عبر تطبيقات مقدمي خدمات الدفع الالكتروني

1- يكون مقدم خدمة الدفع الالكتروني الحاصل على وكالة خدمة حوالات اجنبية، مسؤلاً امام هذا البنك عن سياسات وإجراءات الامتثال ومكافحة غسل الأموال وتمويل الإرهاب واعتماد السيناريوهات ومؤشرات الاشتباه الصادرة عن هذا البنك ومكتب مكافحة غسل الأموال وتمويل الإرهاب فيما يتعلق بالتحويلات الخارجية لعملائه.

2- يخضع جميع العملاء الى إجراءات العناية الواجبة المنصوص عليها ضمن هذه الضوابط واية تعليمات ذات صلة.

3- يسمح لمقدمي خدمات الدفع الالكتروني الحاصلين على وكالة خدمة الحوالات الأجنبية باستخدام تطبيقاتهم الالكترونية لغرض التحويلات الخارجية لزبائنهم المسجلين في التطبيق حصراً.

4- يُمنع العملاء الذين لم يُحدّثوا بياناتهم خلال المدة المحددة من قبل مؤسساتكم من القيام بعمليات التحويل الخارجي.

5- الالتزام بسقوف التحويل الخارجي المحددة من قبل مقدم خدمة الحوالات الأجنبية او السقوف التي تحدد من قبل البنك المركزي العراقي، فضلاً عن انه يحق لمؤسساتكم تحديد السقوف وفقاً لتقيم المخاطر الذاتي وسياستكم الداخلية.

6- تحليل جميع عمليات التحويلات الخارجية عن طريق انظمة متخصصة وقياس التكرارات والتركزات والفترات الزمنية ومدى منطقيتها، مع العرض ان يكون هذا التحليل مرتبط باستمارة (KYC) لكل عميل.

7- معرفة المعلومات الرئيسية عن التحويل على سبيل المثال لا الحصر (سبب التحويل، صلة القرابة... الخ).

8- يتحمل مقدم خدمة الدفع الالكتروني المسؤولية الكاملة في حال كان هناك قصور في التحليل المشار الية في الفقرة (6) أعلاه او عدم التعامل مع نتائج التحليل بالطريقة السليمة.

المادة (10): وكلاء مقدمي خدمات الدفع الالكتروني

فضلاً عن التعليمات الصادرة عن هذا البنك لتنظيم عمل الوكلاء يقع على عاتق مؤسساتكم الالتزام بالاتي :-

1- مقدم خدمة الدفع الإلكتروني يتحمل المسؤولية عن أفعال وكلائه إذا قاموا بإخفاء الأموال أو تمويه حقيقتها أو مصادرها أو مكانها أو حالتها أو كيفية التصرف فيها أو انتقالها أو ملكيتها أو الحقوق المرتبطة بها، سواء كان الوكيل على علم بأنها ناتجة عن جريمة أو كان ينبغي عليه أن يعلم بذلك.

2- يتوجب على مقدم خدمة الدفع الإلكتروني إعداد تقارير دورية توضح تقييم امتثال وكلائه لتعليمات وضوابط مكافحة غسل الأموال وتمويل الإرهاب، على أن يتم الاحتفاظ بهذه التقارير ضمن سجلات المؤسسة لتكون خاضعة لرقابة البنك عند طلبها.

3- اتخاذ إجراءات العناية الواجبة للكيان المراد تعيينه بصفة وكيل فضلاً عن اجراء عملية التقييم الاولي على ان تتضمن هذه الاجراءات عملية البحث و التحري على قوائم الحظر و العقوبات المحلية والدولية للتحقق من ملائمته للعمل، واتخاذ إجراءات العناية المعززة بالنسبة للوكلاء في المناطق عالية المخاطر ، وذلك لضمان عدم استخدام خدمات الدفع الالكتروني لأغراض غير سليمة.

4- التأكد من هوية الوكلاء يتم من خلال تقديم وثائق رسمية، والتحقق من خلفياتهم الشخصية والمالية، وإجراء فحص شامل لضمان عدم ارتباطهم بأنشطة غير قانونية أو وجود قيد جنائي. كما يجب التحقق من عدم وجود أي مؤشرات سلبية عليهم في نظام الاستعلام الائتماني، مع مراعاة تحديث بياناتهم بشكل دوري والتأكد من صلاحية جميع الوثائق المتعلقة بنشاطهم وأوراقهم الثبوتية.

5- التأكد من أن سياساتكم الداخلية تشمل جميع جوانب العمليات المتعلقة بعمل الوكلاء، واتخاذ الإجراءات اللازمة لضمان ان الوكلاء يتبعون الإجراءات والسياسات الداخلية المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب بشكل دقيق، وإجراء مراجعات دورية لتقييم مدى التزامهم بالإجراءات والسياسات.

6- إجراء تقييم دوري للمخاطر المرتبطة بالأنشطة التي يقوم بها الوكلاء لتحديد مدى تعرضهم لمخاطر غسل الأموال وتمويل الإرهاب.

7- ضمان تدريبهم بشكل مستمر حول متطلبات مكافحة غسل الأموال وتمويل الإرهاب كون ان الوكلاء لايمتلكون الخبرة الكافية كما هو الحال في مقدمي خدمات الدفع الالكتروني.

8- عند قيام الوكيل بالعناية الواجبة للعميل عليه الامتثال لجميع التعليمات الصادرة عن هذا البنك وقوانين ومتطلبات مكافحة غسل الأموال وتمويل الإرهاب بما في ذلك تقديم ابلاغ الى مقدم خدمة الدفع بالنشاطات المشتبه بها كافة فوراً .

9- يضمن مقدم خدمة الدفع الالكتروني ان الوكيل يمتلك حساب مصرفي ويقع على عاتق المقدم اتخاذ إجراءات العناية الواجبة والمراجعات والتحليل المستمر لنمط تعاملات حسابات الوكلاء كما منصوص عليه في الضوابط الرقابية الصادرة عن هذا البنك للكشف المبكر عن أي ممارسة غير سليمة قد تؤشر عملية غسل أموال وتمويل ارهاب.

10- وضع آلية موحدة لتدفق الاموال بين المقدم والوكلاء تتوافق مع تعليمات وضوابط هذا البنك والمعايير الدولية وان يتم تثبيت هذه الآلية في سياسة وإجراءات المقدم وسيتم اعتبار أي تدفق مالي مخالف لإجراءات تدفق الأموال المثبت في السياسة مؤشر غسل أموال وتمويل إرهاب واحتيال.

11- يقع على عاتق مقدم خدمة الدفع الالكتروني الحاصل على وكالة الحوالات الاجنبية من احد مقدم خدمات الحوالات الأجنبية العالميين امتلاك سياسات وإجراءات مكافحة غسل الأموال وتمويل الإرهاب الخاصة بالحوالات الأجنبية على ان تشمل اعمال الوكيل الرئيسي والثانوي وفق تعليمات هذا البنك وافضل الممارسات الدولية بهذا الشأن.

12- وجود قاعدة بيانات للعملاء محفوظة بشكل مستقل في حال كون الوكيل متعاقداً مع أكثر من مقدم خدمة الدفع.

13- ضمان اتباع إجراءات وسياقات ونماذج الإبلاغ والتوقيتات المحددة من قبل مكتب مكافحة غسل الأموال.

المادة (11) : المو اقع الالكترونية وتطبيقات التواصل الاجتماعي

استخدام المواقع الالكترونية وتطبيقات التواصل الاجتماعي لغسل الأموال وتمويل الإرهاب من خلال أدوات وقنوات الدفع الالكتروني أصبح قضية متزايدة القلق بالنسبة للعديد من المؤسسات المالية والحكومات، تنتشر هذه الأنشطة على منصات التواصل الاجتماعي، حيث يتم استخدام (البثوث المباشرة، الدعم المالي من المتابعين، وبيع السلع غير القانونية أو جمع التبرعات بطرق غير مشروعة)، لتقليص هذه الظاهرة وحمايتها من الممارسات غير السليمة، يقع على عاتق مقدمي خدمات الدفع الالكتروني اتخاذ مجموعة من الإجراءات لضمان سلامة معاملاتهم وندرج لكم الحد الأدنى من الإجراءات وكالآتي:

1- يمنع تقديم خدمات الدفع الالكتروني في اجراء أي تبرعات الكترونية لجهات غير مرخصة للعمل كمنظمات خيرية من قبل الجهات المعنية بالترخيص.
2- تطبق مقدمي خدمات الدفع الالكتروني سياسات "اعرف عميلك (KYC) " بشكل صارم على جميع المستخدمين الذين يقومون بتحويل الأموال أو تلقي التبرعات الكبيرة عبر منصات التواصل الاجتماعي، يتضمن ذلك التحقق من الهوية الشخصية، العنوان، والمعلومات المالية.
3- يلتزم مقدم خدمة الدفع الالكتروني تحديد سقف يومي وشهري للتحويلات المالية الالكترونية والمصنفة كتبرعات مبني على أساس التقييم الذاتي للمخاطر، مع مراعاة ان يكون سقوف المعاملات المالية الالكترونية بصفة دعم مالي للبثوث اقل من المعاملات المصنفة كتبرعات لمؤسسات مرخص العمل لها بالعمل كمؤسسة خيرية.
4- يقع على عاتق مقدم الخدمة حظر التبرعات المالية الكبيرة التي تتجاوز السقف الشهري المحدد دون التحقق من هوية المانح وتسجيل تفاصيله بشكل دقيق، لضمان عدم استخدام هذه التبرعات في أنشطة غير سليمة أو مشبوهة، حيث يُطلب من المانحين تقديم الوثائق اللازمة لإثبات هويتهم قبل إتمام أي تبرع يتجاوز الحدود المالية المعتمدة.
5- تنفيذ إجراءات فحص مكثفة لجميع المعاملات المالية التي تتم عبر منصات التواصل الاجتماعي، بما في ذلك سحب الأموال، التحويلات بين الحسابات، أو شراء السلع.
6- يلتزم مقدم خدمة الدفع الالكتروني بفرض رقابة صارمة على التبرعات التي تتم بمبالغ كبيرة أو منتظمة أو تصاعدية، حيث يتوجب مراقبة الأنماط غير العادية أو المشبوهة في المعاملات المالية الالكترونية، والتأكد من أن هذه التبرعات لا تُستخدم في أنشطة غير سليمة.
7- عندما يتم التبرع عبر أدوات او قنوات الدفع الإلكتروني، يتم توثيق كل المعلومات المتعلقة بالمعاملة، على سبيل المثال لا الحصر (الشخص المرسل، الجهة المستلمة، المبلغ المتبرع به، تاريخ العملية) هذا يزيد من الشفافية والثقة بين المتبرعين والمؤسسات الخيرية، ويضمن أن الأموال تذهب إلى الغرض المقصود.

المادة (12) : الدول مرتفعة المخاطر

هي الدول التي لديها أوجه قصور كبيرة في أنظمتها الخاصة بمكافحة غسل الأموال وتمويل الإرهاب وتمويل انتشار التسلُّح وعدم الالتزام بتوصيات مجموعة العمل المالي (فاتف)، إذ تدعو (فاتف) جميع الدول الأعضاء إلى تطبيق إجراءات العناية الواجبة المعززة مع هذه الدول وتحثها على ذلك.

استنادًا إلى التوصية رقم (19/ الدول المرتفعة المخاطر) الصادرة عن مجموعة العمل المالي (FATF) وإلى قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015 على المصارف والمؤسسات المالية اتخاذ الإجراءات الآتية بشأن الدول المرتفعة المخاطر:

1- أن تكون مقدمي خدمات الدفع الالكتروني كافةً ملزمة بتطبيق إجراءات العناية الواجبة المعززة على علاقات العمل والعمليات مع الأشخاص الطبيعيين والاعتباريين و مقدمي خدمات الدفع الالكتروني من الدول التي تحددها مجموعة العمل المالي ذات المخاطر المرتفعة.
2- تطبيق عناية واجبة معززة ومطابقة بصورة فاعلة متناسبة مع المخاطر.
3- أن تتخذ تدابير مضادة وفاعلة متناسبة عند ما يتطلب الأمر ذلك أو في حال أيّة مستجدات تجاه الدول مرتفعة المخاطر التي تحددها مجموعة العمل المالي فاتف.

تقوم مجموعة العمل المالي بتقييم الدول من حيث صياغة القوانين المقبولة في مجال مكافحة غسل الأموال وتمويل الإرهاب وإنفاذها، وتضعها في إحدى القوائم الأربعة وهي:

أ - **خضراء (ليس لديها مشاكل)**: هي دول تلتزم بمعايير معموعة العمل المالي ونجاحها في الحفاظ على نظام قوي لمكافحة غسل الأموال وتمويل الإرهاب.

ب - **رمادية (متعاونة لكن لديها مشاكل)**: هي الدول التي لم تقم بتقديم إجراءات ملموسة لمعالجة أوجه القصور الاستراتيجية في مكافحة غسل الأموال وتمويل الإرهاب وتتعهد هذه الدول باتباع خطة العمل المحددة للوفاء بمعالجة أوجه القصور لديها.

ج – **حمراء (غير متعاونة)**: هي الدول التي تشكّل خطرًا على سلامة النظام المالي العالمي وتدعو مجموعة العمل المالي (فاتف) إلى تعزيز الإجراءات عند التعامل معها وتفرض عليها مجموعة متطلبات لاتخاذها بأسرع وقت ممكن.

د - **سوداء (غير متعاونة وتخضع لتدابير مضادة)**: هي دول غير ملتزمة بتوصيات مجموعة العمل المالي ولا تخضع لرقابتها فتصبح تلك الدول ضمن الدول المحظور التعامل معها ويفرض عليها مجلس الأمن التابع للأمم المتحدة عقوبات مالية واقتصادية على وفق قرارات تصدر عنه، يتم من خلالها فرض قيود على النشاطات والعمليات وعلاقات العمل التي تتم من الأشخاص الطبيعين والاعتباريين لهذه الدول.

يجب على جميع مقدمي خدمات الدفع الالكتروني الاخذ بنظر الاعتبار المخاوف المتعلقة بأوجه القصور وعدم الالتزام بأيٍّ من إجراءات أنظمة مكافحة غسل الأموال وتمويل الإرهاب في الدول الواردة ضمن الفئات المذكورة آنفًا، بشأن علاقات العمل وجميع العمليات التي تتم مع أشخاص طبيعيين أو اعتباريين وأن تتخذ الإجراءات اللازمة التي تتناسب ودرجة المخاطر، على النحو الآتي:

1- إيلاء عناية خاصة بعلاقات العمل والمعاملات الواردة من تلك الدول وبالعكس.
2- طلب معلومات إضافية عن العميل والمعاملات المرتبطة به.
3- مراجعة علاقات العمل مع البنوك المراسلة في تلك الدول (عالية المخاطر).
4- التحقق من طبيعة العمل والهدف منها.
5- الوقوف على مصادر أموال العميل وأصوله.
6- تحديث بيانات العملاء (الأجانب) من خلال استمارة اعرف عميلك (KYC) بشكل دوري للوقوف على المتغيرات التي قد تطرأ عليهم.
7- الحصول على موافقة الإدارة العليا لاستمرار علاقة العمل من عدمها.
8- تعزيز مراقبة المعاملات.

المادة (13) : مبدأ النهج المستند على المخاطر

هو إطار يركّز على تحديد وإدارة المخاطر المحتملة المتعلقة بغسل الأموال وتمويل الإرهاب، وتقييمها، التي تتعرض لها المؤسسة، وإنّ هذا النهج يعتمد على تخصيص الموارد والجهود على وفق مستوى المخاطر المرتبطة، ويعمل النهج القائم على المخاطر أيضًا على تقييم المخاطر التي تواجهها البلاد في مجال مكافحة غسل الأموال وتمويل الإرهاب وتحديدها، يتسم بمرونة وفاعلية وتناسب عالٍ، وبناءً على ذلك على مقدم خدمة الدفع الالكتروني تصميم تدابير مناسبة وتطبيقها للحد من المخاطر، إذ يجب اتباع ما يأتي:

أوّلًا: تقييم المخاطر:

1- تطوير أسلوب مرتكز على المخاطر لعملية المراقبة بما يتناسب عدد وعمل العملاء وتصنيفهم وأنواع المعاملات، والمنتجات والخدمات المقدمة لهم بحسب درجة مخاطر غسل الأموال وتمويل الإرهاب.
2- بذل عناية خاصة في التعامل مع الحالات التي تمثّل درجة مخاطر مرتفعة .
3- تصنيف درجات المخاطر إلى (مرتفعة ومتوسطة ومنخفضة) في أقل تقدير ويمكن تصنيفهم إلى خمس مستويات من المخاطر.
4- وضع الإجراءات اللازمة للتعامل مع هذه المخاطر بما يتناسب مع كل درجة من الدرجات المشار اليها في الفقرة رقم (3) اعلاه.

ثانيًا: تحديد المخاطر:

1- يقع على عاتق مقدم خدمة الدفع مراجعة تصنيف العملاء وفقاً لدرجات المخاطر "الخاصة بغسل الأموال وتمويل الإرهاب" بشكل دوري أو في حالة حدوث تغيرات لاحقه.
2- يقع على عاتق مقدم خدمات الدفع اعتماد أنظمة خاصة بمكافحة غسل الأموال و تمويل الإرهاب (AML) يتكامل مع نظام إدارة البطاقات بالنسبة لشركات مقدمي خدمات الدفع الالكتروني اما المصارف يجب ان يتكامل النظام أعلاه مع النظام المصرفي الشامل، لاجل قياس و تحديد المخاطر المتعلقة بـ (العملاء و المنتج و قنوات تقديم الخدمات و المخاطر المتعلقة بالمنطقة الجغرافية).

3- اعداد مصفوفة تفصيلية يعتمد عليها النظام اعلاه تاخذ بنظر الاعتبار المخاطر المتعلقة بالعملاء مرتفعي المخاطر على سبيل المثال (العملاء غير المقيمين، الاشخاص المعرضين للمخاطر بحكم منصبهم و المنظمات الخيرية،.. الخ).

4- اعتماد السيناريوهات المعدة من قبل هذا البنك ومكتب مكافحة غسل الاموال و تمويل الارهاب ضمن نظام مكافحة غسل الاموال (AML) و العمل على تحديث هذا النظام بأية سيناريوهات يصدرها المكتب من خلال المتابعة الدورية كحد ادنى بالاضافة الى السيناريوهات المقترحة من قبلكم فضلاً عن السيناريوهات المعتمدة دولياً .

5- انشاء آلية لاعادة تقييم تصنيف المخاطر بشكل دوري (ربع سنوي على الاقل) لمواكبة التغيرات.

ثالثًا: تطبيق التدابير:

1- على مقدم خدمة الدفع الالكتروني عند تصنيف المخاطر في علاقة العمل التي تربط المقدم بالعميل أن يتحقق من إن النظام الموضوع لإدارة المخاطر يتضمن سياسات وإجراءات تقوم على تحديد المخاطر وتقييمها والرقابة عليها والإبلاغ عنها، على أن يتناول ذلك النظام مجالات المخاطر كافة.

2- عند وصف المخاطر في علاقة العمل التي تربط المقدم بالعميل يتم النظر في عناصر المخاطر الأربعة الآتية كحد أدنى (مخاطر العملاء، مخاطر المنتج، مخاطر تقديم قنوات الخدمة، المخاطر المتعلقة بالمناطق الجغرافية).

- على مقدم خدمة الدفع الالكتروني العمل على اعداد تقرير تقييم ذاتي لمخاطر غسل الاموال وتمويل الارهاب بصورة سنوية يتضمن المخاطر الكامنة للمقدم ومخففات المخاطر ونسبة المخاطر المتبقية، يتم ارسال هذا التقرير الى البنك المركزي العراقي كما يجب على الادارة العليا العمل على تخفيف نسبة المخاطر المتبقية في السنوات التالية.
- يقع على عاتق الإدارة العليا لمقدم خدمة الدفع الالكتروني ضمان الالتزام بالمسؤوليات الرئيسية الاتية:

1- توفير الميزانية والموارد الكافية بما في ذلك توفير موظفين مناسبين ومؤهلين، و أنظمة وأدوات ملائمة، لضمان التطبيق الفعال للسياسات والإجراءات والضوابط الداخلية بما يتناسب مع المخاطر المحددة لمكافحة غسل الأموال وتمويل الإرهاب.

2- ضمان عدم السماح بأي انتهاكات عندما لا يتمكن فرع او وكيل في بلد ما من تنفيذ متطلبات مكافحة غسل الأموال وتمويل الإرهاب حسب ما هو وارد في نظام مكافحة غسل الأموال ولائحته التنفيذية ونظام مكافحة جرائم الإرهاب وتمويله ولائحته التنفيذية كون القوانين واللوائح أو غيرها من التدابير المحلية في ذلك البلد ضعيفة أو لا تسمح بتطبيق الإجراءات المناسبة بمكافحة غسل الأموال، وينبغي على الإدارة اتخاذ الإجراءات المناسبة بشكل عاجل.

3- متابعة تنفيذ برامج التدريب المستمر والسنوي في مجال مكافحة غسل الأموال وتمويل الإرهاب لجميع الموظفين.

4- ضمان أن يتم تقييم مخاطر غسل الأموال وتمويل الإرهاب في مقدمي خدمات الدفع الالكتروني بشكل دقيق وشامل لجميع المخاطر التي تواجه مقدمي خدمات الدفع الالكتروني لوضع السياسات المناسبة لإدارة المخاطر التي تتعرض لها.

5- اعتماد السياسة الداخلية للتخفيف من مخاطر غسل الأموال وتمويل الإرهاب وضمان فاعلية تطبيقها.

6- ضمان استلام تقارير منتظمة وشاملة عن مخاطر غسل الأموال وتمويل الإرهاب التي تواجه مقدمي خدمات الدفع الالكتروني ، بما في ذلك على سبيل المثال لا الحصر:

أ- خطط العمل التصحيحية، إن وجدت، لمعالجة نتائج عمليات المراجعة المستقلة سواءالداخلية أوالخارجية .

ب- التطورات والتحديثات في أنظمة ولوائح مكافحة غسل الأموال وتمويل الإرهاب، وانعكاساتها، إن وجدت، على مقدمي خدمات الدفع الالكتروني.

ج- تفاصيل مخاطر غسل الأموال وتمويل الارهاب العالية والتأثيرات المحتملة على مقدمي خدمات الدفع الالكتروني.

د- تفاصيل خاصة عن تطبيق وتنفيذ إجراءات العقوبات المالية المتعلقة بقرارات مجلس الأمن الخاصة بالمدرجين على قوائم الإرهاب، أو المتعلقة بمكافحة انتشار التسليح والجهات ذات الاختصاص.

المادة (14) : أنظمة مكافحة غسل الأموال وتمويل الإرهاب وقوائم الحظروالعقوبات

أوّلًا – نظام مكافحة غسل الأموال وتمويل الإرهاب (AML/CFT System): يجب على جميع مقدمي خدمات الدفع الالكتروني المرخّصين من قبل هذا البنك اقتناء نظام مكافحة غسل الأموال وتمويل الإرهاب والعمل عليه، على أن يكون هذا النظام في أقل تقدير كما يلي:

1- النظام مرخّص من شركة مجهزة رصينة وعالمية.

2- متابعة آنية وفورية لجميع الحركات التي تحدث من العملاء وقياس المبالغ التي يتم سحبها أو إيداعها او تحويلها مع التدفقات النقدية المحدّدة من العميل وتحليلها، على وفق مبدأ اعرف عميلك واستماره فتح الحساب (KYC) والسيناريوهات المتعلقة بغسل الأموال وتمويل الإرهاب المعتمدة من مكتب مكافحة غسل الأموال والبنك المركزي العراقي ورفع تنبيهات فيها أوّلًا بأول.

3- يقوم النظام بتصنيف مخاطر العملاء على أساس التدفقات النقدية لكل عميل وطبيعة عمله والموقع الجغرافي للعمل وطبيعة المنتجات وقنوات تقديم المنتجات التي يتعامل بها كل عميل ليتم تحديد هذه المخاطر وتصنيفها إلى (عالية – متوسطة – منخفضة) في أقل تقدير، ويمكن أن يكون قياس مخاطر العملاء بدرجة تصنيف خماسية.

4- أن يكون هذا النظام متكامل بشكل مباشر مع النظام المصرفي الشامل في حال كان مقدم الخدمة مصرفاً ومع نظام إدارة البطاقات في حال كان مقدم خدمة الدفع الالكتروني شركة من جهة وبمنصة البحث والتحري عن المدرجين في قوائم الحظر والعقوبات المحلية والدولية من جهة أُخرى (Automatic Integration).

5- يفضل استخدام النظام آنفًا الذكاء الاصطناعي وخوارزميات التعلم الآلي لتحليل البيانات وتحديد المعاملات التي قد تكون مشبوهة، وبناءً على ذلك يُرسل مسؤول قسم الإبلاغ عن غسل الأموال وتمويل الإرهاب تقارير عن المعاملات المشبوهة إلى مكتب مكافحة غسل الأموال وتمويل الإرهاب عن طريق نظام (GO AML).

6- تحليل أنماط العمليات المالية المنفذة من عملاء المقدم ومقارنة حجم التعاملات المالية المُنفذة منهم مع المعلومات التي تمّ الإفصاح عنها.

7- إيقاف أيّ معاملة تتطابق بالمواصفات مع سيناريو أو أكثر من سيناريوهات الاشتباه الاسترشادية إلى حين إجراء عملية التحقق من سلامتها من مسؤو ل قسم الابلاغ عن غسل الاموال وتمويل الارهاب في مقدم خدمة الدفع الالكتروني.

8- تشخيص العملاء المعرّضين للمخاطر بحكم مناصبهم (PEPs) لضمان التعامل معهم على وفق لمخاطر المرتبطة بهم واستحصال الموافقات الضرورية قبل بدء علاقة العمل معهم.

9- إصدار التقارير اليومية بشأن المعاملات التي تمّت مراجعتها مع ذكر حالة كل عملية ونتائج تحليلها.

10- إمكانية الرجوع إلى التقارير السابقة التي تمت مراجعتها من النظام.

ثانيًا – أنظمة البحث والتحري على قوائم الحظر والعقوبات المحلية والدولية:

1 – على جميع مقدمي خدمات الدفع الالكتروني المرخصين من هذا البنك القيام بالبحث والتحري عن جميع العملاء المعنويين والاعتباريين الذين يتعاملون معهم على قوائم الحظر والعقوبات المحلية والدولة الآتية:

أ- قائمة العقوبات المفروضة من مجلس الأمن التابع للأمم المتحدة (UN) .

ب- قائمة العقوبات المفروضة من وزارة الخزانة الأمريكية (OFAC) .

ج- قائمة العقوبات المفروضة من الاتحاد الأوروبي (EU) .

د- قائمة العقوبات المفروضة من المملكة المتحدة (UK) .

هـ- لجنة تجميد أموال الإرهابين: هي لجنة مشكّلة من الأمانة العامة لمجلس الوزراء تتولى تجميد أموال الإرهابين أو غيرها من الأُصول التي حدّدتها لجنة مجلس الأمن التابع للأمم المتحدة.

و- قوائم داخلية تتضمن الاسماء المحظورة من التعامل محلياً والصادرة من هذا البنك ومكتب مكافحة غسل الاموال و تمويل الارهاب.

2 – تكون إجراءات عمليات البحث والتحري عن طريق نظام البحث والتحري الخاص بمقدم خدمة الدفع الالكتروني والمجهز من شركة عالمية رصينة لتشمل عملية البحث جميع الأفراد والمؤسسات الراغبة في التعامل مع المقدم، ويجب أن تشمل عملية البحث والتحري جميع الأطراف المتعامل معهم سواء بطريقة مباشرة أم غير مباشرة وتحديد المستفيدين النهائيين من الكيانات التي يتعامل معها المقدم.

3 – يجب التأكد من أنّ أنظمة البحث والتحري المعتمدة يدعم عملية التحديث الدورية على قوائم الحظر والعقوبات المحلية والدولية كل (12) ساعة خلال اليوم الواحد في أقل تقدير.

المادة (15): المؤشرات الاسترشادية للتعرف على العمليات التي يشتبه في أنها غسل أموال أو تمويل إرهاب

يعتمد التعرُّف على العمليات التي يشتبه في أنها تتضمن مؤشرات غسل أموال أو تمويل إرهاب، على مدى إرساء ثقافة الامتثال في المؤسسة المالية، فضلًا عن آلمام الموظفين بأحكام قانون غسل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 النافذ والتعليمات الصادرة بموجبه، فضلًا عن الخبرة المكتسبة من الممارسة العملية والتدريب النوعي في مجال مكافحة غسل الأموال وتمويل الإرهاب. وفي ما يأتي بعض الأمثلة والسيناريوهات للعمليات التي تُعدُّ أحدث ما تمَّ التطرق إليه من البنك المركزي العراقي ومكتب مكافحة غسل الأموال وتمويل الإرهاب ولمختلف العمليات التي تتطلب المزيد من العناية الواجبة والمراجعة للتعرف على مدى تأكد الاشتباه في غسل الأموال ، إذ من الجدير بالذكر السيناريوهات الآتية هي الحد الأدنى التي يجب أن تتضمنها أنظمة مقدم خدمة

الدفع الالكتروني، إذ يجب اعتماد جميع السيناريوهات الصادرة عن هذا البنك ومكتب مكافحة غسل الأموال وتمويل الإرهاب مع الالتزام باي تحديث يصدر من قبل الجهات الاشرافية والرقابية المعنية جنبًا إلى جنب السيناريوهات الآتية:

1- حوالات صادرة أو واردة بفترات متقاربة ولنفس المستفيدين دون وجود علاقة واضحة بين الطرفين.
2- حوالات صادرة أو واردة إلى دول ومواقع جغرافية مصنفة على أنّها مرتفعة المخاطر حسب مجموعة العمل المالي (FATF) أو المدرجة على قوائم العقوبات المحلية (قوائم تجميد الأموال) أو قوائم الحظر والعقوبات الدولية (OFAC,UN,EU,UK).
3- حوالات واردة ثم يتم تحويلها بالمدّة نفس أو بعد مدّة قصيرة.
4- حوالات صادرة أو واردة من الأشخاص أصحاب المناصب العليا ذوي المخاطر.
5- تشابه المعلومات الشخصية لأشخاص عدّة من دون مبرر (العنوان، رقم الهاتف، التولد، رقم الجواز،إلخ).
6- اختلاف الوثائق المقدّمة في كل عملية تحويل (واردة أو صادرة) وبحسب قواعد البيانات المتوافرة لديكم.
7- الامتناع عن تقديم جواز السفر للمرسل والمتسلّم الذي يُعتمَد في تدقيق الأسماء في قوائم المدرجين على القوائم المحلية والدولية.
8- تحويلات بمبالغ صغيرة وكبيرة بصورة متكررة من دول تعاني من اضطرابات سياسية أو أمنية، وإليها.
9- اصدار او استلام حوالات بمبالغ نقدية على مراحل متعددة بحيث تكون قيمة المبلغ المودع في كل مرة اقل من الحد الوارد ضمن التعليمات الصادرة من قبل هذا البنك ولكن في مجموعها مبالغ تزيد عن ذلك.
10- تلقي تحويلات بمبالغ كبيرة للعميل وعلى وجه الخصوص التي تسحب نقداً بما لا يتناسب مع نشاط العميل.
11- تحويلات بمبالغ كبيرة بصفة منتظمة من مناطق تشتهر بجرائم معينة مثل تجارة أو زراعة المخدرات أو دول ليست لديها نظم لمكافحة غسل الأموال أو تمويل الارهاب.
12- تكرار ورود تحويلات خارجية للعميل من دول تعتمد نظام السرية المطلقة.
13- التحويلات المتكررة التي لا يتناسب مجموعها خلال فترة معينة مع نشاط العميل.
14- معاملات كبيرة متكررة مع الشركات المنشأة حديثاً و/أو التي لا تتوافق أنشطتها الرئيسية مع الأنشطة التي يقوم بها المستفيد أو لها غرض عام.
15- حسابات متعلقة بكياناتٍ يتُوقَّع أنها لم تعد نشطة (ومثال ذلك حساب الطلاب الأجانب بعد انتهاء السنة الدراسية).
16- قيام العميل بعمليات تحويل نقدي خارجي عدّة بمبالغ مرتفعة.
17- تلقي العميل حوالات نقدية خارجية بمبالغ مرتفعة.
18- الدخل الشهري للعميل تجاوز الحد المتوقع للدخل المصرّح به بضمن استمارة اعرف عميلك (KYC).

❖ ندرج في ادناه مؤشرات الأنماط والأساليب المختلفة التي تهدف إلى تعزيز الكشف عن الأنماط غير الاعتيادية في التعاملات المالية الالكترونية، وهي مستمدةٌ من تبادل الخبرات والتجارب دولياً، مع الاخذ بنظر الاعتبار إن وجود مؤشر واحد متعلّق بعميل أو معاملة قد لا يضمن وحده الاشتباه، كما أن مؤشرًا واحدًا لا يدلّ بالضرورة دلالةً واضحةً على مثل هذا النشاط، ولكنه يمكن أن يقود إلى مزيدٍ من الرصد والفحص على حسب الاقتضاء، مع العرض انه بالإمكان ان يشترك مؤشر واحد من المؤشرات مع عده محاور من المحاور ادناه، ونستعرض فيما يلي عدد من هذه الأنماط و الأساليب والمؤشرات :-

1- بطاقات الدفع الإلكترونية (الدائنة والمدينة والمسبقة الدفع)

أ- معاملات سريعة أو فورية متكررة، ذات مبالغ عالية عند اصدار البطاقة بفترة قصيرة.

ب- عمليات سحبٍ نقديّ أو تحويلات نقدية سريعة أو فورية لمبالغ كبيرة بعد استلام تحويل مالي بهدف إفراغ البطاقة.

ج- معاملات متكررة وكبيرة، لا تتّفق مع الملف الاقتصادي لصاحب الحساب (ومثال ذلك: التحويلات الدولية المفاجئة، أو عمليات سحب الأموال النقدية التي تجري ببطاقات الدفع في أجهزة الصراف الآلي الأجنبية، أو المشتريات الكبيرة من البضائع، أو الدفعات لصالح شركات أجنبية غير مرخصة إلى خدمات تحويل القيمة المالية).

د- قيام العملاء باستخدام كافة رصيد بطاقة الائتمان ومن ثم قيامه بالسداد الكامل للرصيد المدين.

هـ- عمليات تسديد مفاجئة للتمويلات أو التسهيلات المالية التي قام العميل بالحصول عليها من خلال طرف أو أطراف أخرى دون وجود علاقة واضحة.

و- استخدام البطاقات الالكترونية في شراء الممتلكات والأصول مرتفعة القيمة والسلع الثمينة مثل المجوهرات والمعادن النفيسة في دول / أقاليم مرتفعة المخاطر من حيث غسل الأموال.

ز- استخدام البطاقات الالكترونية لعمل سحوبات يومية متكررة وبقيم متساوية ومن اماكن مختلفة وبعيدة عن عنوان اقامة العميل أو مكان عمله ودون مبرر واضح.

ح- الحصول على خدمات مختلفة في أماكن متعددة في مناطق جغرافية مختلفة وبعملات مختلفة.

ط- دفعة صغيرة للمستفيد، بمجرد إتمامها بنجاح تتبعُها بسرعة دفعات ذات قيمة أكبر لنفس المستفيد.

ي- عمليات شراء ذات قيمة صحيحة بلا فواصل عشرية متكررة و/أو مبالغها كبيرة.

ك- شركات مستفيدة تُدير مواقع إنترنت مزوّدة لخدمات التداول والاستثمار، تكون في كثير من الحالات غير مرخّصة أو مُدرجَة في قائمة العقوبات.

ل- تحديث معلومات الاتصال بشكل متكرر دون مبرر.

م- استخدام البطاقة لإجراء تحويلات مالية إلى دول تُعرف بكونها ملاذات ضريبية أو ذات أنظمة مالية غير شفافة.

ن- إجراء عمليات إرجاع سلع بشكل متكرر، مما يشير إلى سلوك مريب.

2- الخدمات المصرفية الإلكترونية

والتي تشمل على سبيل المثال لا الحصر(Mobile banking ،Electronic applications)

أ- تلقي العميل عدة تحويلات مالية صغيرة بطريقة الكترونية وبعد ذلك اجراء تحويلات كبيرة بنفس الطريقة الى بلد اخر.

ب- ايداع دفعات كبيرة وبشكل منتظم بمختلف وسائل الايداع الالكتروني او تلقي دفعات كبيرة وبشكل منتظم من بلدان اخرى تعتبر مرتفعة المخاطر.

ج- قيام العميل بطلب فتح حساب او محفظة الكترونية او تسجيل او اصدار بطاقة عبر التطبيق الالكتروني ورفض تقديم المعلومات اللازمة لاستكمال الإجراءات او تبين عدم صحة المعلومات.

د- قيام العميل باستخدام التطبيق الالكتروني للتحويل بين حساباته او بطاقاته لمرات عديدة ودون وجود اسباب واضحة لذلك.

هـ- استخدام القنوات البنكية الإلكترونية لإجراء تحويلات صادرة متكررة لأشخاص مختلفين دون وجود مبرر واضح.

و- استخدام التطبيق من مناطق مرتفعة المخاطر بمجال غسل الاموال، وتنفيذ حركات مالية بمبالغ كبيرة وتكرارات كثيرة.

ز- استخدام وسائل تكنولوجية مختلفة لإجراء التحويلات المالية وتغيير عناوين الدخول(IP Address) لإخفاء معالم التتبع.

ح- أمور غير طبيعية حُدِّدت من خلال السلوك عبر الإنترنت، كالتردُّد في إدخال البيانات، وتأخير ضغطات المفاتيح، وعلامات الأتمتة، وتعدّد محاولات تسجيل الدخول الفاشلة...إلخ

ط- استخدام الشبكات الخاصة الافتراضية، والأجهزة المخترقة، والشركات المُضيفة التي قد تخفي عنوان بروتوكول الإنترنت الخاص بالمستخدم.

ي- عناوين بروتوكول الإنترنت متعدّدة أو أجهزة إلكترونية مرتبطة بحساب واحد عبر الانترنت.

ك- عنوان بروتوكول الإنترنت ثابت واحد أو جهاز إلكتروني مرتبط بحسابات متعدّدة لأصحاب حسابات مختلفة.

ل- عناوين بريد إلكتروني لا تبدو متوافقة مع اسم صاحب الحساب/ المحفظة الالكترونية ، أو نمط من عناوين البريد الإلكتروني المتشابهة تَظهَر عبر حسابات متعدّدة.

م- وجود مخالفات في تفاصيل الملف الشخصي للعميل، مثل بيانات تسجيل الدخول المشتركة (ومثال ذلك أن تكون مشتركة بين مستخدمين أو أكثر) مع حسابات أخرى.

3- مؤشرات المخاطر الهيكلية

أ- يبدو الهيكل المؤسسي للكيان التجاري معقدًا بشكل غير عادي وغير منطقي، مثل الاشتراك مع شركات وهمية أو مع شركات مسجلة في دولة ذات مخاطر عالية .

ب- كيان تجاري مسجل أو لديه مكاتب في دول ذات التزام ضعيف في مكافحة غسل الأموال وتمول الإرهاب.

ج- كيان تجاري مسجل في عنوان من المحتمل أن يكون عنوان تسجيل جماعي، على سبيل المثال المباني السكنية عالية الكثافة، وعناوين البريد، والمباني التجارية أو المجمعات الصناعية.

د- لا يبدو أن النشاط التجاري لكيان تجاري مناسب للعنوان المذكور، على سبيل المثال يبدو أن كياناً تجارياً يستخدم العقارات السكنية، دون وجود مساحة تجارية أو صناعية، وعدم وجود تفسير معقول لذلك.

هـ- يفتقر الكيان التجاري إلى التواجد ع الإنترنت أو يشير التواجد على الإنترنت إلى وجود نشاط تجاري غير متوافق مع نوع الأعمال المحدد، على سبيل المثال الموقع الإلكتروني لكيان تجاري يحتوي بشكل أساسي على مواد مأخوذة من مواقع الكترونية أخرى أو يشير الموقع إلى نقص المعرفة فيما يتعلق بالمنتج أو الصناعة المعينة التي يتداول فيها الكيان .

و- يعرض الكيان التجاري نقصاً ملحوظاً في الأنشطة التجارية النموذجية، على سبيل المثال تفتقر إلى معاملات كشوفات الرواتب المنتظمة بما يتماشى مع عدد الموظفن المعلنين والمعاملات المتعلقة بتكاليف التشغيل والتحويلات الضريبية .

ز- مالكي أو مديري الكيان التجاري يفتقرون إلى الخبرة في إدارة الأعمال أو يفتقرون الى معرفة تفاصيل المعاملات، أو يديرون شركات متعددة.

ح- يظهر كيان تجاري أو مالكوه أو كبار المديرين في الأخبار السلبية، ع سبيل المثال المخططات السابقة لغسل الأموال، أو الاحتيال، التهرب الضريبي، الأنشطة الإجرامية الأخرى، الأنشطة الجارية، التحقيقات، أو الإدانات السابقة .

ط- يتواجد لدى الكيان التجاري عدد أدنى من الموظفين العاملين، بما لايتسق مع حجم السلع المتداولة.

ي- الكيان التجاري يحمل نسخة مشابهة لاسم شركة معروفة أو مشابه جداً لها، في محاولة للظهور كجزء من الشركة، على الرغم من أنها غير مرتبطة بها في الواقع.

ك- يمتلك الكيان التجاري فترات سكون غير مبررة .

ل- التجار الموجودين في مناطق غير مستقرة امنياً حسب تصنيف الجهات الأمنية المسؤولة.

4- مؤشرات مخاطر نشاط التجارة

أ- لا يمتثل الكيان لالتزامات العمل العادية، مثل تقديم إقرارات الضريبة.

ب- نشاط تجاري غير متسق مع نوع الأعمال المعلن.

ج- ممارسة الكيان التجاري صفقات تجارية معقدة تشمل العديد من الوسطاء الخارجين في خطوط أعمال غير متوافقة مع كيانه.

د- يعرض الكيان التجاري باستمرار هوامش ربح منخفضة بشكل غير معقول في معاملاته التجارة، على سبيل المثال بيع السلع بذات قيمة الاستيراد او اقل من قيمة الاستيراد.

هـ- يقوم الكيان التجاري بعمليات شراء لسلع تفوق قدرته الاقتصادية بشكل كبير.

و- كيان تجاري تم شكيله حديثاً يشارك في نشاط تجاري كبير الحجم والقيمة .

ز- حجم كبير من العوائد أو الإلغاءات.

ح- الكيانات التي تتلقى مدفوعات دولية.

ط-الكيانات والتجار الذين لايملكون نموذج تسعير واضح لمنتجاتهم او خدماتهم.

5- مؤشرات مخاطر نشاط الحساب والمعاملات التجارية

أ- يقوم الكيان التجاري بإجراء تغييرات متأخرة جداً على ترتيبات الدفع للمعاملة، على سبيل المثال يقوم الكيان بإعادة توجيه الدفع إلى كيان غير معروف سابقاً في آخر لحظة، أو يطلب الكيان التغييرات في تاريخ الدفع المجدول أو مبلغ الدفع.

ب- عرض الحساب عدداً أو قيمة عالية غير متوقعة للمعاملات التي لا تتوافق مع النشاط التجاري المعلن للعميل.

ج- عمليات الدفع الالكترونية الخاصة بكيان تجاري تكون باستمرار أقل بقليل من السقوف المحددة او حدود الإبلاغ.

د- يزداد نشاط المعاملات المرتبطة بالكيان التجاري في الحجم بسرعة وبشكل ملحوظ، ثم يصبح راكداً بعد فترة قصيرة من الزمن.

هـ- يتم إرسال المدفوعات أو استلامها بمبالغ حركة كبيرة بغرض التجارة في قطاعات تعتبر فيها هذه الحركة غير معتادة.

و- يتم توجيه المدفوعات في حلقة يتم إرسال الأموال من دولة ما واستلامها مرة أخرى في نفس الدولة، بعد المرور عبر دولة أو دول أخرى.

6- نظام التسوية الآنية الاجمالية وبيع الاوراق المالية ونظام المقاصة

أ- فتح عدد من الحسابات أو التفويض عن عدة حسابات دون القيام بأجراء تعاملات على تلك الحسابات.

ب- القيام بإيداع مبلغ كبير وبعد ذلك بفترة قصيرة يتم تحويل المبلغ الى جهة دون وجود مبرر واضح.

ج- التعامل بمبالغ ضخمة دون توفر الحد الادنى من المعرفة بطبيعة الاستثمار بالاوراق المالية ومخاطرها.

د- القيام بإيداع مبلغ نقدي لشراء الاوراق المالية لغايات الاستثمار طويل الاجل وبعد ذلك بفترة قصيرة يقوم بيع تلك الاوراق المالية وسحب الأموال.

هـ- تغذية الحساب دائماً وعدم القيام بأي تعامل او القيام بتعاملات قليلة ثم سحب تلك الاموال.

و- القيام بطلب إجراء مناقلات بين حسابات العميل او مع اشخاص اخرين مفوض بالتعامل عنهم دون مبرر.

ز- إظهار العميل أنه ليس لديه معرفة كافية بطبيعة المعاملة/المعاملات أو موضوعها أو مبلغها أو غرضها أوالعلاقة بين الحسابين، أو تقديمه تفسيرات غير واقعية أو مربكة أو غير متّسقة.

ح- محاولة المستخدم إخفاء هويته باستخدام هوية مزورة أو مسروقة أو معدلة (العنوان، ورقم الهاتف، والبريد الإلكتروني).

ط- تغييرات متكررة في تفاصيل الاتصال وأرقام الهواتف وعناوين البريد الإلكتروني بعد فتح الحساب.

ي- تنفيذ تحويلات متكررة بمبالغ متطابقة من وإلى حسابات مختلفة في فترات زمنية قصيرة.

ك- تحويلات مفاجئة وكبيرة إلى حسابات جديدة أو غير معروفة.

ل- تقديم العميل لمعلومات متناقضة حول أهداف التحويلات.

م- تزايد النشاط المالي بشكل كبير وغير مبرر في حسابات كانت ذات نشاط قليل سابقًا.

ن- تنفيذ عمليات سحب نقدي ضخمة بعد فترة من النشاط المالي المحدود.

س- استخدام حسابات لشركات صغيرة أو غير نشطة للتحويلات المالية الكبيرة.

ع- فتح حسابات لشركات تحمل أسماء مشابهة لشركات معروفة لتضليل الجهات الرقابية.

ف- استخدام الأموال المحولة لشراء أصول أو استثمارات في فترة قصيرة بعد الإيداع.

المادة (16): سلوكيات الموظف وسياسة اعرف موظفك

اولاً: تطبيق مبدأ اعرف موظفك (KYE):

يجب على مقدمي خدمات الدفع الالكتروني كافةً بذل العناية الواجبه تجاه الموظفين لأجل منع أيّة حالات مشبوهة وغير مشروعة وذلك عن طريق الآتي:

1- على مقدم خدمة الدفع الالكتروني تطبيق مبدأ اعرف موظفك (KYE) بما يساعد في تشخيص أيّة حالات تواطؤ داخلي ممكن قد تحدث.

2- تنظيم استمارة اعرف موظفك (KYE) ويتولى قسم الامتثال متابعة التزام المؤسسة وتضمين النتائج الخاصة به ضمن التقارير التي ترسل دورياً إلى البنك المركزي العراقي.

3- يتحمل مقدم خدمة الدفع الإلكتروني المسؤولية الكاملة عن جميع الأفعال والسلوكيات التي تصدر من موظفيه أو أي من موظفي فروعه او وكلائه ، ويجب عليه ضمان امتثالهم التام للقوانين والسياسات المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب، ويُعد مقدم الخدمة مسؤولًا أمام البنك المركزي عن ضمان تنفيذ كافة الإجراءات الوقائية والتدابير الاحترازية لمنع استخدام خدمات الدفع في الأنشطة غير القانونية أو المشبوهة.

4- يلتزم مقدم خدمة الدفع الالكتروني بتنفيذ إجراءات التحقق من موظفيه و موظفي وكلائه و القيام بفحوصات شاملة للمؤهلات والسجل الجنائي والتاريخ المالي للموظفين المحتملين لضمان أنهم لا يتورطون في أي نشاطات غير قانونية أو مشبوهة، تشمل هذه الإجراءات أيضًا التحقق من الوضع في قوائم العقوبات المحلية والدولية، بالإضافة إلى التدقيق في علاقاتهم التجارية لضمان الامتثال للمعايير العالمية لمكافحة غسل الأموال وتمويل الإرهاب.

5- يقع على عاتق مقدم خدمة الدفع الالكتروني التحقق من المؤهلات العلمية والمهنية لجميع الموظفين لضمان امتلاكهم الكفاءات اللازمة لأداء وظائفهم بشكل قانوني وأخلاقي، يشمل هذا التحقق من صحة الشهادات الاكاديمية والتراخيص المهنية المقدمة من قبل الموظف، مع التأكد من أنها صادرة من جهات معترف بها، كما يتم فحص تاريخ الموظف المهني لضمان عدم ارتباطه بأي أنشطة قد تهدد الامتثال للوائح مكافحة غسل الأموال وتمويل الإرهاب.

6- يلتزم مقدم خدمة الدفع الالكتروني بتطبيق سياسات وإجراءات فعّالة لضمان عدم وجود تضارب في المصالح بين الموظفين والأطراف الأخرى، يتم التأكد من أن الموظفين لا يشاركون في أي أنشطة قد تؤدي إلى تضارب في المصالح أو تُستغل لغسل الأموال أو تمويل الإرهاب، حيث يحتوي ذلك الكشف عن أي علاقة مالية أو تجارية قد تكون لها تأثيرات سلبية على نزاهة العمل، ومراجعة التصريحات المالية والتجارية للموظفين بانتظام، كما يتم تعزيز الوعي بتأثيرات تضارب المصالح في سياق مكافحة غسل الأموال وتمويل الإرهاب لضمان امتثال كامل للمعايير القانونية والأخلاقية.

7- منح إجازة إلزامية مدّة (اسبوعين) متواصلة ولجميع الموظفين لدى مقدم خدمة الدفع الالكتروني خلال السنة على أن تشمل تلك الإجازات المديرين وموظفي الأقسام الرقابية من دون أن تُقابَل بأيّ استقطاع من مستحقاته مهما كان نوعها، تهدف هذه الإجازات إلى ضمان عدم وجود أي تضارب في المصالح وتعزيز الشفافية داخل المؤسسة، بما يساهم في الوقاية من أي ممارسات غير قانونية أو مشبوهة قد تؤثر على نزاهة العمل.

8- إدخال مديري المؤسسات المالية وموظفيها دورات تدريبية مختصة في مجال الامتثال ومكافحة غسل الأموال ومكافحة الفساد والاحتيال مع مراعاة عمليات التدريب الدورية لضمان المتابعة المستمرة ومواكبة أحدث الأساليب والمستجدات على أن تشمل جميع الموظفين ولا تقتصر على المديرين وألّا تُستقطَع من رواتبهم أية أُجور لقاء هذه الدورات.

9- ضرورة تدوير مديري الفروع كل (5) سنوات حدًّا أقصى.

ثانياً: سلوكيات الموظف

تُعدُّ بعض السلوكيات للموظف مؤشرًا على تورطه بعمليات غير مشروعة مع الاخذ بنظر الاعتبار إن وجود مؤشر واحد قد لا يضمن وحده الاشتباه، كما أن مؤشرًا واحدًا لا يدلّ بالضرورة دلالةً واضحةً على وجود نشاط غير مشروع، ولكنه يمكن أن يقود إلى مزيدٍ من الرصد والفحص والتحري على حسب الاقتضاء، وندرج في ادناه بعض السلوكيات التي قد تعد مؤشر على ماجاء في أعلاه وكما يأتي:

1- ارتفاع مستوى معيشة الموظف ومستوى إنفاقه بشكل ملحوظ ومفاجئ بما لا يتناسب ودخله الشهري.
2- قيام الموظف بتجاوز الإجراءات الرقابية واتباع سياسة المراوغة أثناء تأديته لعمله.
3- قيام الموظف بالمساعدة في تنفيذ عمليات تتميز بعدم وضوح كامل لهوية المستفيد أو الطرف المقابل.
4- قيام الموظف بالمبالغة في مصداقية العميل وأخلاقياته وقدرته ومصادره المالية، وذلك ضمن تقاريره المرفوعة للادارة.
5- بقاء الموظف بعد انتهاء الوقت الرسمي للدوام من دون وجود مبرر على بقائه.
6- الإهمال الواضح لواجباته الوظيفية وبشكل ملحوظ غير مشفوع بأيّة مبررات.
7- امتلاك أُصول أو ممتلكات لا تتناسب تمامًا وراتبه ومستوى دخله الشهري.
8- التعامل مع أشخاص وجهات مشبوهة ومعروفة بعدم نزاهتها.
9- عدم المحافظة على السرية للمؤسسة وإفشاء الوثائق السرية والمهمة وإخراجها.
10- اظهار الموظف مستوى غير مبرر من السرية أو مقاومة للتدقيق في الأنشطة التي يقوم بها، أو رفض توفير مستندات ضرورية لإتمام المعاملات.

11- إظهار الموظف سلوكًا غير معتاد أو مريب في بيئة العمل، مثل عدم التعاون مع التحقيقات الداخلية أو إخفاء معلومات تتعلق بالمعاملات.

12- القيام بتعديل أو تلاعب في السجلات المالية أو بيانات المعاملات بهدف إخفاء أنشطة مشبوهة أو غير قانونية.

13- محاولة الموظف الضغط على زملائه أو المعنيين لتجاوز الإجراءات الرقابية أو أي قيود قانونية أو داخلية.

المادة (17) : التدريب المستمر للموظفين

يُعد التدريب من أهم الوسائل للتأكيد على أهمية جهود مكافحة غسل الأموال وتمويل الإرهاب، فضلًا عن تثقيف الموظفين بشأن ما يجب فعله حين مواجهة مؤشر غسل أموال أو تمويل إرهاب، إذ يقع على عاتق مقدم خدمة الدفع الالكتروني وضع إجراءات لضمان ارتفاع معايير الكفاءة عند تعيين أو توظيف المسؤولين أو الموظفين، فضلًا عن وضع برنامج مستمر لتدريب المسؤولين والموظفين لدى المؤسس مقدمي خدمات الدفع الالكتروني المالية على أساليب مكافحة غسل الأموال وتمويل الإرهاب بما ينسجم ومضمون المادة (12) الفقرة (أوّلًا / د) التي تنص على (**تلتزم المؤسسات المالية وأصحاب الأعمال والمهن غير المالية المحدّدة بالتدريب المستمر للمسؤولين والعاملين بما يكفل رفع قدراتهم في فهم مخاطر غسل الأموال وتمويل الإرهاب والتعرُّف على العمليات والتصرّفات غير الاعتيادية أو المشبوهة وكيفية التعامل معها وتطبيق التدابير الواجب اتباعها بفاعلية**)، كما يأتي:

1- يجب على مقدمي خدمات الدفع الالكتروني وضع خطط وبرامج تدريبية مستمرة وملائمة سنويًا في الأقل لتدريب المسؤولين والعاملين (موظفي خط الدفاع الأوّل) فيها على مكافحة غسل الأموال وتمويل الإرهاب.

2- يجب أن يشمل برنامج التدريب الخاص بمقدمي خدمات الدفع الالكتروني تدريبًا مستمرًا لضمان محافظة المسؤولين والموظفين على مهاراتهم وقدراتهم بهدف زيادة كفاءتهم في الامتثال الدقيق بالقواعد والنظم المقررة لمكافحة غسل الأموال وتمويل الإرهاب، وضمان اطلاعهم على التطورات الجديدة المتعلقة بالأساليب والاتجاهات العامة لعمليات غسل الأموال وتمويل الإرهاب ونظم مكافحتها، والمستجدات المحلية والإقليمية والعالمية في هذا الشأن.

3- إجراء مراجعة دورية لحاجات التدريب بانتظام ودراسة هذه الاحتياجات على وفق اتجاهات التدريب العالمية والنظر في مسائل الخبرات والمهارات والقدرات القائمة، والوظائف والأدوار المطلوبة، وحجم أعمال مقدم خدمة الدفع وتصنيف مخاطره ونتيجة التدريب المسبق والحاجات المتصورة، ويجب على الادارة العليا أن تأخذ بالحسبان نتيجة كل مراجعة.

4- التخطيط لهذه البرامج وتنفيذها بالتنسيق بين مقدمي خدمات الدفع الالكتروني وبين البنك المركزي العراقي و مكتب مكافحة غسل الأموال والبنك المركزي العراقي، على أن يُراعَى ما يأتي:

أ- أن يكون التدريب شاملًا لجميع اقسام والمسؤولين والموظفين.

ب- الاستعانة في تنفيذ البرامج التدريبية بالمعاهد المختصة التي تنشأ لهذا الغرض أو يكون التدريب في مجال مكافحة غسل الأموال وتمويل الإرهاب من بين أغراضها، محلية كانت أم خارجية، مع الإفادة بالخبرات المحلية والدولية في هذا الشأن.

ج- أن يتم التنسيق مع مسؤول الامتثال و قسم الابلاغ عن غسل الاموال وتمويل الارهاب فيما يتعلق باختيار الموظفين الذين يتم ترشيحهم لحضور برامج تدريبية في هذا المجال.

د- الالتزام بفقرات الشهادات والدورات الصادرة بموجب ضوابط المناصب القيادية الصادرة عن هذا البنك.

المادة (18): مسؤولية الإدارة العليا وتعزيز الأنظمة الداخلية

أوّلًا: مسؤولية الإدارة العليا:

تقع على عاتق الإدارة العليا لمقدمي خدمات الدفع الالكتروني مسؤولية مكافحة غسل الأموال وتمويل الإرهاب التي من الممكن أن يتعرضو لها، إذ يجب على الإدارة العليا لأجل الحد من هذه الجرائم العمل على إعداد برامج لمنع غسل الأموال وتمويل الإرهاب وتنفيذها، تتضمن بالحد الأدنى الآتي:

أ – إجراء تقييم لمخاطر غسل الأموال وتمويل الإرهاب التي من الممكن ان تتعرض لها، يتضمن تحديد هذه المخاطر وتقييمها وفهمها، واتخاذ إجراءات فاعلة للحد منها وتوفير هذا التقييم للجهات الرقابية بشكل دوري.

ب – اعتماد سياسات وإجراءات وضوابط داخلية تتناسب مع الالتزامات المفروضة في مجال مكافحة غسل الأموال وتمويل الإرهاب مما يؤدي إلى الحد من المخاطر التي جرى تقييمها.

ج_ تطبيق معايير نزاهة ملائمة عند اختيار الموظفين.

د- التدريب المستمر للمسؤولين والعاملين في مجال مكافحة غسل الأموال وتمويل الإرهاب ورصد الموارد المادية والمالية اللازمة لهم بما يكفل رفع قدراتهم في فهم مخاطر غسل الأموال وتمويل الإرهاب والتعرُّف على العمليات والتصرّفات غير الاعتيادية أو المشبوهة وكيفية التعامل معها وتطبيق التدابير الواجب اتباعها بفاعلية.

هـ- التدقيق المستقل لاختبار مدى فاعلية السياسات والإجراءات ومدى تطبيقها.

و – يحتوي النظام على الكفاءة والفاعلية اللازمة لقياس المخاطر المتعلقة بالعملاء وطبيعة الأعمال التي يمارسونها والموقع الجغرافي للعميل بأحدث الأساليب المعتمدة في هذا المجال.

أ- ضمان وجود وصف وظيفي وسلم صلاحيات لكافة العاملين في المؤسسة المالية .

ثانيًا: مهام مسؤولي وظفية الامتثال والإبلاغ عن غسل الأموال وتمويل الإرهاب.

❖ **مهام مراقب الامتثال:**

من الضروري تحديد مهام ومسؤولية مراقب الامتثال ولا بُدّ للإدارة العليا أن توضح ذلك بشكل كامل ومكتوب، فضلًا عن توضيح علاقة مراقب الامتثال بالإدارة العليا والإدارات المختلفة لدى مقدم خدمة الدفع الالكتروني، وتتضمن وظيفة مراقب الامتثال بشكل عام المهام الآتية:

1- مراجعة السياسات والإجراءات والقرارات الصادرة من ادارة مقدم خدمة الدفع الالكتروني للتأكد من مدى توافقها مع القوانين و الانظمة والتعليمات والاعمامات الصادرة من قبل البنك المركزي العراقي او ايّة قوانين وتعليمات صادرة بهذا الشأن ومناقشة امتثالها مع الادارة.

2- اقتراح السياسات والاجراءات اللازمة للخدمات الجديدة او تحديث السياسات والاجراءات السابقة بناءً على تطور اعمال مقدمي خدمات الدفع الالكتروني ومتابعة مدى امتثال هذه النشاطات والخدمات الجديدة للقوانين والانظمة والتعليمات الصادرة بشأنها.

3- اعداد تقرير مراقب الامتثال وارساله الى البنك المركزي العراقي ونسخة منه الى الادارة العليا.

4- مراجعة الاجراءات التي تتبعها الاقسام و الشعب في المؤسسة للتأكد من مدى انسجامها مع القوانين والانظمة والتعليمات الخاصة بها.

5- تحديد و تقييم وتحديث مخاطر الامتثال بشكل سنوي او حسب مقتضيات العمل ووضع الاجراءات المناسبة للتخفيف من تلك المخاطر للوصول الى تحديد مستوى المخاطر المرتبطة بعد الامتثال وادارتها و معالجتها.

6- اعداد قائمة بالخدمات و المنتجات التي يقدمها مقدم خدمات الدفع الالكتروني بالتعاون مع الاقسام الاخرى التي تبين نوع الخدمات المقدمة من قبل المؤسسة للجهات الرقابية.

7- مراجعة إجراءات ملئ استمارة اعرف عميلك (KYC) واتخاذ اجراءات العناية الواجبة تجاه العملاء.

8- ان يكون لدى مراقب الامتثال الاطلاع التام والفهم الكامل لجميع القوانين والانظمة والتعليمات الخاصة بعمل مقدم خدمات الدفع الالكتروني الصادرة من قبل البنك المركزي العراقي او أية جهة اخرى.

9- رفع تقارير شهرية الى الادارة العليا تتضمن الانحرافات المكتشفة ان وجدت والاقتراحات اللازمة لتلافيها ومتابعة مدى تطبيق جميع القوانين و التعليمات و الاعمامات الصادرة من قبل البنك المركزي العراقي من خلال الاعمال اليومية لجميع الاقسام، والاحتفاظ بنسخة من هذه التقارير في سجلاته لغرض مراجعتها من قبل اللجان التفتيشية الميدانية الخاصة بالبنك المركزي العراقي عند الطلب.

10- يتولى مراقب الامتثال مسؤولية التزام المؤسسة بقرارات الادارة العليا والسياسات الداخلية اضافة الى الاجراءات المقررة بموجب القوانين والتعليمات التي يصدرها البنك المركزي العراقي.

11- انشاء مصفوفة امتثال لتدقيق ومراقبة اعمال المؤسسة للتأكد من ان تكون جميع الاقسام ممتثلة لتعليمات ومتطلبات البنك المركزي العراقي ، اضافة الى انشاء مكتبة امتثال تضم جميع القوانين والانظمة والتعليمات ذات الصلة بعمل مقدم خدمة الدفع الالكتروني.

12- بيان الرأي بخصوص الخطط الاستراتجية وتقديم الملاحظات والاقتراحات التي من شأنها تطوير الية العمل داخل المؤسسة وبما يتناسب مع القوانين والتعليمات والضوابط الصادرة عن البنك المركزي العراقي.

13- اعداد خطة سنوية لمراجعة امتثال الفروع الخاصة بالمؤسسة.

14- العمل على اجراء دراسة تفصيلية لجميع المنتجات و الخدمات فضلاً عن المنتجات والخدمات التي في النية اطلاقها المؤسسة ومخاطر غسل الاموال و تمويل الارهاب المتعلقة بها والدور الذي تلعبه الادارة العليا في الرقابة على انظمة مكافحة غسل الاموال و تمويل الارهاب ومعالجة ما بها من اوجه قصور ان وجدت.

15- اقتراح دورات تدريبية حول السياسات والاجراءات الموضوعة التي يجب ان تتبع والتأكد من ضرورة الالتزام بها من الموظفين الموجودين بشكل عام والموظفين الجدد بشكل خاص.

16- تنسيق عمليات التدقيق الحاصلة على اعمال مقدم خدمة الدفع الالكتروني من قبل الجهات التدقيقية والرقابية المعتمدة.

17- يتولى مراقب الامتثال مسؤولية التنسيق المستمر مع البنك المركزي العراقي لضمان توافق سياسات مؤسسته مع خطط وتعليمات البنك المركزي المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب، حيث يشمل ذلك مراجعة وتطبيق التعليمات الصادرة عن البنك المركزي بشكل دوري، والتأكد من أن جميع الإجراءات والسياسات المعتمدة تلتزم بالمعايير القانونية والتنظيمية، كما يُعنى مراقب الامتثال بمتابعة التحديثات المستمرة في سياسات البنك المركزي لضمان التكيف الفوري مع أي تغييرات أو متطلبات جديدة.

18- التنسيق المستمر مع المؤسسات المالية الأخرى لضمان الامتثال الكامل للقوانين واللوائح المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب، يتضمن ذلك تبادل المعلومات المتعلقة بالمعاملات المشبوهة، التعاون في التحقيقات المشتركة، والالتزام بالمعايير الدولية المتعلقة بالرقابة المالية مع مراعاة عدم الاخلال بقوانين السرية المعمول بها.

❖ **مهام مدير قسم الإبلاغ عن غسل الأموال / تمويل الإرهاب**

تتحدّد مهام مدير قسم الإبلاغ عن غسل الأموال وتمويل الإرهاب في كل مؤسسة على وفق حجم مقدم خدمة الدفع الالكتروني وموارده والنظم المطبقة فيه، وبصفة عامة يتعين أن توكل إليه المهام الآتية:

1- التعرف و التحقق من هوية العميل والمستفيد الحقيقي عن طريق بيانات و معلومات من مصادر موثوقة ومستقلة.

2- التحقق من اسم العميل على قوائم الحظر والعقوبات المحلية والدولية قبل البدء بعلاقة العمل والموافقة على استمارة اعرف عميلك (KYC) والمتابعة والتحديث المستمر.

3- ابلاغ مكتب مكافحة غسل الاموال وتمويل الارهاب بالعمليات التي تتضمن شبهة غسل اموال او تمويل ارهاب وفقاً للآليات المعمول بها بهذا الشأن.

4- اتخاذ القرار بشأن حفظ العمليات التي يتبين فيها عدم وجود شبهة غسل اموال أو تمويل ارهاب او التي لا ترتقي لمستوى الابلاغ ويجب ان تتضمن الاسباب التي استندت اليها في الحفظ والتي يتوجب ان يتم أرشفتها مع أوليات العملية .

5- المتابعة المستمرة في كل ما يتعلق بعلاقة العمل وفحص المعاملات التي تجري لضمان توافقها مع ما يتوفر عن العميل من معلومات وانشطة تجارية ونمط مخاطر ومصادر امواله عند اللزوم.

6- اتخاذ و تنفيذ تدابير العناية الواجبة قبل وخلال اقامة علاقة العمل مع العميل لغرض التعرف على المستفيد الحقيقي.

7- فهم الغرض وطبيعة العلاقة والاطراف المتوقع التعامل معهم وحجم المبالغ المتوقع التعامل بها مع ضرورة الحصول على المعززات التي من شأنها اثبات العملية.

8- المشاركة في اعداد وتنفيذ خطة الرقابة على فروع مقدم خدمة الدفع الالكتروني.

9- تصنيف كافة العملاء حسب درجة المخاطر المتعلقة بغسل الاموال و تمويل الارهاب ، وتنفيذ تدابير العناية الواجبة المعززة بحق العملاء الذين يتم تصنيفهم كعملاء عاليين المخاطر.

10- العمل على تطبيق السيناريوهات المعممة من قبل البنك المركزي العراقي ومكتب مكافحة غسل الأموال وتمويل الإرهاب في انظمة مكافحة غسل الاموال و تمويل الارهاب الخاصة بالمؤسسات المالية كحد ادنى ومتابعة تحديثها بشكل مستمر.

11- التواصل بشكل مباشر مع العملاء الذي يتم الشك في تعاملاتهم لغرض التأكد من سلامة تلك العمليات.

12- تقديم الدورات و الورش التدريبية بشكل دوري لجميع موظفين مقدم خدمة الدفع الالكتروني لغرض التوعية بمخاطر غسل الاموال و تمويل الارهاب.

13- العمل على انشاء النهج القائم على المخاطر بالتنسيق مع الاقسام و الوحدات المعنية لدى مقدم خدمة الدفع الالكتروني لتحديد نوعية ودرجة الرقابة والضبط الداخلي استناداً الى تصنيف مخاطر غسل الاموال وتمويل الارهاب المتعلقة بالعملاء والمنتجات و الخدمات.

14- اجراء تقييم ذاتي لمخاطر غسل الاموال و تمويل الارهاب لمقدم خدمة الدفع الالكتروني و بالتنسيق مع الاقسام و الوحدات المعنية على ان يتضمن مخاطر العملاء والدول والخدمات والمنتجات وقنوات التوصيل وتطوير تطبيق سياسات وبرامج لمكافحة هذه المخاطر وآلية تخفيفها وعلى شكل تقرير سنوي يقدّم الى البنك المركزي العراقي.

15- اعداد سياسات واجراءات خاصة بالقسم وانشاء الهيكل التنظيمي لتوزيع المهام و المسؤوليات.

16- الاحتفاظ بقاعدة بيانات تضم اسماء الافراد و الكيانات التي يتم حرمانها من التعامل من قبل البنك المركزي العراقي، وقاعدة اخرى تخص المحظورين من التعامل محلياً ودولياً.

17- إعداد تقرير شهري عن نشاط مكافحة غسل الأموال وتمويل الإرهاب بالمؤسسة، وعرضه على الإدارة العليا لإبداء ما تراه من ملحوظات، واتخاذ ما تقرره من إجراءات بشأنه، وحفظ نسخة من هذا التقرير ضمن سجلات مقدم خدمة الدفع الالكتروني، يكون مشفوعًا بملحوظات وقرارات الإدارة، ويُراعَى أن يتضمن هذا التقرير – حدًّا أدنى - ما يأتي:

أ- الجهود التي تمت خلال المدة التي يتناولها التقرير بشأن العمليات غير الاعتيادية والعمليات المشتبه فيها، وما اتخذ بشأنها.

ب- ما تسفر عنه المراجعة الدورية لنظم مكافحة غسل الأموال وتمويل الإرهاب وإجراءاتها المتبعة في مقدم خدمة الدفع الالكتروني من نقاط ضعف ومقترحات تلافيها، بما في ذلك التقارير التي تتيحها الأنظمة الداخلية عن العمليات غير الاعتيادية.

ج- عدد التنبيهات على أنظمة مكافحة غسل الأموال وتمويل الإرهاب المعتمدة داخل المؤسسة المالية التي تمَّت متابعتها وهل كانت ستوجب الإبلاغ أو عدم الابلاغ والسبب وراء ذلك.

د- ما تمَّ إجراؤه من تعديلات على السياسات أو النظم الداخلية أو الإجراءات في شأن مكافحة غسل الأموال وتمويل الإرهاب خلال المدة التي يتناولها التقرير.

هـ- بيان مدى الالتزام بتنفيذ الخطط الموضوعة خلال مدة التقرير للإشراف العام مكتبيًا وميدانيًا على مختلف فروع المؤسسة للتحقق من التزامها بتطبيق أحكام القوانين والضوابط الرقابية والنظم الداخلية بشأن مكافحة غسل الأموال وتمويل الإرهاب.

و- عرض اجراءات الخطة الموضوعة للإشراف العام مكتبيًا وميدانيًا على الفروع خلال المدة الآتية للتقرير.

ز- بيان تفصيلي بالبرامج التدريبية التي تمَّ عقدها للعاملين في مجال مكافحة غسل الأموال وتمويل الإرهاب خلال المدة المشار إليها.

المادة (19) : آلية الإبلاغ

اولاً: استنادا إلى الفقرة (خامسًا/أ) للمادة (12) والفقرة (أوّلًا /و) للمادة (26) من قانون مكافحة غسل الأموال وتمويل الإرهاب، يلتزم مقدمي خدمات الدفع الالكتروني وأصحاب المهن غير المالية المحدّدة فيها بإبلاغ مكتب مكافحة غسل الأموال وتمويل الإرهاب فورًا بأيّة عملية يشتبه بأنّها تتضمن غسل أموال أو تمويل إرهاب، سواء تمت هذه العملية أم لم تتم، وعلى وفق أُنموذج الإبلاغ المعتمد لدى مكتب مكافحة غسل الأموال وتمويل الإرهاب، وكما في الحالات الآتية:

1- إذا تمَّ الاشتباه أو توافرت أسس معقولة للاشتباه في أنّ هذه المعاملات تتم من خلال أموال تشكّل متحصلات جريمة غسل أموال أو تمويل إرهاب.
2- للأموال صلة أو ارتباط بعمليات غسل أموال أو يعتزم استخدامها في ارتكاب أفعال إرهابية من منظمات إرهابية أو أشخاص يموّلون الإرهاب.
3- وجود شك أو ريبة في سلوكيات العميل توحي باشتباه في عمليات غسل أموال أو تمويل إرهاب.
4- وجود تطابق مع أيّ من سيناريوهات غسل الأموال أو تمويل الإرهاب الصادرة عن البنك المركزي اومكتب مكافحة غسل الأموال وتمويل الإرهاب.

وبخلافه يحق للبنك المركزي العراقي أن يفرض عقوبات وتدابير إضافية بحق المؤسسات المالية المخالفة لإجراءات الإبلاغ عن حالات الاشتباه، تشتمل على:

1- فرض غرامات مالية أو إدارية.
2- تعليق الترخيص أو سحب أيّ نوع آخر من التصاريح أو تقييده.
3- حظر استمرار العمل أو مزاولة المهنة أو النشاط.

ثانياً: النتائج المترتبة على العمليات التي تمَّ الإبلاغ عنها:

يتضمن القانون أحكامًا تلزم الجهات التي تقوم بالإبلاغ عن العمليات المشبوهة، على النحو الآتي:

1- يجب إيقاف العملية المالية القائمة بينها وبين الشخص المبلَّغ عنه مدة لا تزيد على (7) أيّام عمل بحسب ما ورد في الفقرة (أوّلًا/ ج) من المادة (9)، إذ يجب على الجهات المبلّغة أن تدرك أنّ قرار الاستمرار بعلاقة العمل بعد الإبلاغ عن العمليات المشبوهة يجب أن يضمن تجنّب المخاطر المترتبة على استمرار هذه العلاقة.
2- أن يُشترَط في حالات الإبلاغ عدم الإفصاح للعميل أو المستفيد أو مجلس الادارة ، الادارة التنفيذية او أيّ شخص آخر غير السلطات المختصة بتطبيق أحكام هذا القانون عن الإجراءات القانونية التي تُتخَذ في شأن المعاملات أو العمليات المشتبه فيها، وذلك عملًا بأحكام المادة (12/ رابعًا) من قانون مكافحة غسل الأموال وتمويل الإرهاب، وفي حال طلب اي جهة رقابية داخلية او خارجية نسخة او تقرير عن حالات الاشتباه التي تم تزويد المكتب بها يتم تزويدهم بعدد تقارير الاشتباه فقط بدون اي تفاصيل.
3- فضلًا عن القيام بحجز المبلّغ المشتبه به بصفة دليل ملموس بشأن عملية الاشتباه.

4- في الحالات التي تقرّر فيها الجهات المبلّغة إنهاء علاقة العمل، يجب القيام بالتنسيق مباشرة مع مكتب مكافحة غسل الأموال وتمويل الإرهاب لضمان عدم تنبيه الكيان أو الشخص المشتبه فيه بعملية الإبلاغ نتيجة هذا الإنهاء، وعدم عرقلة التحريات بأيّة صورة كانت.

ثالثاً: الحماية التي يوفرها القانون للمبلّغ:

تتم حماية المبلّغ استنادًا إلى المادة (48) من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015، المتضمنة لا يُسأل جزائيًا أو انضباطيًا مَنْ قام بالإبلاغ عن أيّ من العمليات المشتبه بها الخاضعة لأحكام قانون مكافحة غسل الأموال وتمويل الإرهاب أو تقديم معلومات أو بيانات عنها، وإن ثبت أنّها غير صحيحة.

رابعاً: الإبلاغ عن حالات الاشتباه :

يتم ملء أُنموذج المعاملة المشبوهة وإرساله إلى مكتب مكافحة غسل الأموال وتمويل الإرهاب مع مراعاة السرية التامة ويكون تسليم الإبلاغ عن طريق الوسائل الآتية:

أ- التسليم باليد من مسؤول الإبلاغ عن غسل الأموال وتمويل الإرهاب أو معاونه حصرًا.

ب- البريد الرقمي الخاص بمكتب مكافحة غسل الأموال وتمويل الإرهاب (iq.aml@info).

ت- عن طريق نظام تلقي الإبلاغات الرقمية (GO AML).

ويجب أيضًا على مسؤولي قسم الإبلاغ عن غسل الأموال وتمويل الإرهاب تثقيف جميع العاملين في المؤسسة المالية وفروعها ووكلائها وتوعيتهم بكل ما يتعلق بالإبلاغ عن العمليات التي يشتبه بأنّها تحتوي على عملية غسل الأموال وتمويل إرهاب والقيام بالتوضيح لهم بأنّ كل شخص يقوم بالإبلاغ عن هذه المعاملات محمي ولا يترتب عليه أيّة إجراءات قانونية استنادًا إلى أحكام المادة (48)من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39 لسنة 2015) التي نصت على أنّه لا يُسأل جزائيًا أو انضباطيًا كل مَنْ قام بحسن نية بالإبلاغ عن أيّ من العمليات المشتبه بها الخاضعة لأحكام هذا القانون أو بتقديم معلومات أو بيانات عنها، وإن ثبت أنّها غير صحيحة.

المادة (20) الاحتفاظ بالسجلات والمستندات

قدر تعلق الامر باجراءات مكافحة غسل الأموال وتمويل الإرهاب يقع على عاتق مقدمي خدمات الدفع الالكتروني حفظ بيانات العملاء على وفق قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015 والمدة المحدّدة فيه.

1- أنواع السجلات والمستندات الواجب الاحتفاظ بها:

يتعين على مقدم خدمة الدفع الالكتروني الاحتفاظ بما يأتي:

أ- سجلات العملاء والمستفيدين الحقيقيين ومستنداهم، على أن تتضمن صور مستندات تحقيق الشخصية الخاصة بهم سواء كانوا أشخاصًا طبيعيين أم اعتباريين.

ب- السجلات والمستندات المتعلقة بالعمليات التي تتم مع العملاء، على أن تتضمن بيانات كافية للتعرف على تفاصيل كل عملية على حدة.

ج- تقارير العمليات غير الاعتيادية، وما يفيد مراجعة هذه التقارير.

د- السجلات الخاصة بالعمليات المشتبه بها، على أن تتضمن صور الإخطارات عن العمليات التي تمَّ إرسالها إلى قسم مكافحة غسل الأموال والبيانات والمستندات المتعلقة بها.

هـ- سجلات ومستندات التقارير التي تمَّ اتخاذ قرار بحفظها من مدير قسم مكافحة غسل الأموال وتمويل الإرهاب.

و- السجلات الخاصة بالبرامج التدريبية، على أن تشمل بيانات البرامج جميع التي يحصل عليها العاملون لدى مقدمي خدمات الدفع الالكتروني في مجال مكافحة غسل الأموال وتمويل الإرهاب، وأسماء المتدربين، والأقسام / الإدارات التي يعملون فيها، ومحتوى البرنامج التدريبي، ومدته، والجهة التي قامت بالتدريب سواء في الداخل أم في الخارج.

2- **الشروط الواجب اتباعها لدى الاحتفاظ بالسجلات**

يتعيّن على مقدم خدمة الدفع الالكتروني مراعاة الشروط الآتية لدى الاحتفاظ بالسجلات والمستندات المنصوص عليها في البند السابق:

أ- الاحتفاظ بالسجلات والمستندات والتقارير كافة بطريقة آمنة، والاحتفاظ بنسخ احتياطية منها في مكان آخر.

ب- أن تتسم طريقة الحفظ بسهولة وسرعة استرجاع السجلات والمستندات المحتفظ بها، بحيث يتم توفير أيّة بيانات أو معلومات يتم طلبها بشكل وافٍ، وبلا تأخير.

ج- حفظ سجلات الكترونية للعمليات اضافة الى حفظها ورقياً.

3- **مدة الاحتفاظ**

يكون الاحتفاظ بالسجلات والمستندات مدّة (5) خمس سنوات في الأقل، ويختلف تاريخ حساب بدء مدة الاحتفاظ بها بحسب أنواعها على وفق ما يأتي:

أ- سجلات العملاء والمستفيدين الحقيقيين ومستنداتهم.

ب- السجلات والمستندات المتعلقة بالعمليات التي تتم مع العملاء بصورة مستمرة.

ج- تقارير العمليات غير الاعتيادية وذلك من تاريخ صدور التقرير.

د- السجلات الخاصة بالعمليات المشتبه بها التي تمَّ إرسالها إلى قسم مكافحة غسل الأموال وذلك من تاريخ إرسالها، أو إلى حين صدور قرار أو حكم نهائي بشأن العملية، أيُّهما أطول.

هـ- سجلات ومستندات تقارير الاشتباه التي تمَّ اتخاذ قرار بحفظها من مدير قسم مكافحة غسل الأموال وتمويل الإرهاب، وذلك من تاريخ اتخاذ القرار بحفظها.

و- السجلات الخاصة بالبرامج التدريبية، وذلك من تاريخ انتهاء البرنامج التدريبي.

المادة (21) : وظيفة إدارة المخاطر

تتضمن هذه المادة الحد الأدنى من مهام إدارة المخاطر في اطار مكافحة غسل الأموال وتمويل الإرهاب وهي كالآتي:-

أولًا: أهمّ الإجراءات الواجب على مقدم خدمة الدفع الالكتروني الالتزام بها في مجال إدارة المخاطر:

1- إعداد سياسة عامة تتضمن في الأقل تحديد سقوف للمخاطر المرتبطة بعدم الامتثال ومكافحة غسل الأموال وتمويل الارهاب.

2- تحديد الإجراءات الخاصة بإدارة المخاطر بشكل واضح وتتفق وحجم تعقيد عملياته ودرجته.

3- تحديد أنواع المنتجات والخدمات والعمليات المسموح التعامل بها وتحديد مستوى المخاطر بشكل دقيق لها.

4- المراجعة الدورية للسياسات والإجراءات المُتبَعة والعمل على تعديلها بما يتناسب ونشاط مقدم خدمة الدفع ومخاطره.

5- تحديد المخاطر الناتجة عن المنتجات والخدمات الجديدة وقبل التعامل بها.

6- التوصية بالتخلي عن النشاطات التي تسبب مخاطر لمقدم خدمة الدفع الالكتروني والتي ليس له القدرة على مواجهتها.

7- تحديد حدود للمخاطر التي يمكن لمؤسسته المالية تحملها.

8- إعداد التقارير عن الخطر وتقديمها للإدارة العليا.

9- بناء الوعي الثقافي للخطر داخل المؤسسة ويشمل التعليم الملائم والتدريب المستمر.

ثانيًا: خطوات إدارة المخاطر:

1- تحديد المخاطر:

لكي يتمكن مقدم خدمة الدفع الالكتروني من إدارة المخاطر لا بدّ عليه أوّلًا أن يحددها فكل منتج أو خدمة يقدّمها.

2- قياس الخطر:

إن العملية الثانية بعد تحديد المخاطر هي قياسها، إذ إنّ كل نوع من المخاطر يجب أن ينظر إليه بثلاثة أبعاد (حجمه، مدته، احتمالية الحدوث لهذه المخاطر) ويُعدُّ الوقت ذا أهمية بالغة الأثر على القرارات لإدارة المخاطر.

3- ضبط المخاطر:

هناك ثلاث أساليب أساسة لضبط المخاطر وهي (تجنب بعض النشاطات، تقليل المخاطر، إلغاء أثر هذه المخاطر).

المادة (22) : أحكام عامة

1- مراجعة دورية للسياسات والإجراءات المصادق عليها من قبل الادارة العليا المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب لتواكب مع المعايير الدولية مثل توصيات مجموعة العمل المالي (FATF) التطورات القانونية والتقنية في هذا المجال.

2- مخاطبة هذا البنك بالفقرات أو الإجراءات ضمن هذه الضوابط التي يتعذر عليكم تنفيذها وتوضيح الأسباب وراء عدم التنفيذ ووضع خطة زمنية لتطبيقها، وبخلافه تتحمل مؤسساتكم تبعات القصور في الإجراءات.

3- يجب على مقدمي خدمات الدفع الإلكتروني ضمان أن تكون اجراءاتهم في سياساتهم المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب واضحة، شاملة، مرنة، ومتناسبة مع حجم ونوعية النشاط التجاري.

4- تصميم سياسات بطريقة لا تفرض تعقيداً أو قيوداً غير مبررة تؤثر على الابتكار أو تقديم الخدمات والمنتجات، ووضع إجراءات مخففة للعملاء منخفضي المخاطر مع ضمان عدم التنازل عن مستوى العناية الواجبة، وبما يراعي خططكم ومبادراتكم للشمول المالي.

5- يقع على عاتق مقدمي خدمات الدفع الإلكتروني التعاون والتنسيق فيما بينهم في مجال مكافحة غسل الأموال وتمويل الإرهاب لتبادل المعلومات والبيانات اللازمة.

6- اتخاذ تدابير فعالة لحماية البيانات والمعلومات الشخصية للعملاء، وضمان سرية المعلومات المتعلقة بالمعاملات المالية وفقاً لأفضل الممارسات الدولية.

7- تحديد وتوضيح المسؤوليات داخل المؤسسة بشكل دقيق، خاصة فيما يتعلق بالإجراءات الرقابية وفق ماجاء في هذه الضوابط.

8- تسري العقوبات والغرامات الواردة في قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015 ودليل الغرامات والعقوبات الصادر عن هذا البنك على أوجه القصور وعدم الامتثال الى هذه الضوابط.

المادة (23) : الضوابط المتجانسة والدخول حيز النفاذ

تأتي هذه الضوابط مكملة لجميع الضوابط والتعليمات الصادرة عن هذا البنك في إطار مكافحة غسل الأموال وتمويل الإرهاب، وتدخل حيز التنفيذ اعتبارًا من تاريخ صدورها، حيث يتوجب على مؤسساتكم عند صدورها الاتي:

1- اجراء عملية تقييم اولي وتحليل فجوات لسياساتكم واجراءاتكم الخاصة بمكافحة غسل الأموال وتمويل الإرهاب.
2- بعد تشخيص الفجوات ونقاط الضعف، يتم تبني وتعديل سياسات واجراءت تتلائم اجراءات مكافحة غسل الاموال وتمويل الارهاب.
3- الاعتماد على الأنظمة الالكترونية في مراقبة وتحليل واجراء أنشطة مؤسساتكم في اطار مكافحة غسل الأموال وتمويل الإرهاب.
4- يتوجب عليكم اجراء مراجعة وتقييم نهائي بعد تنفيذ الفقرات أعلاه لقياس أوجه التحسين والمعالجات المتخذة من قبلكم.
5- توثيق جميع اجراءاتكم المتخذة بناءً على الفقرات (4،3،2،1) أعلاه وضمان توفيرها للجهات الرقابية متى ما تطلب الامر.

البنك المركزي العراقي
مجلس الادارة

علي محسن إسماعيل
محافظ البنك المركزي العراقي