القاهرة في: ٤ نوفمبر ٢٠٢١

السيد الأستاذ /
بنك

تحية طيبة وبعد،

في إطار توجهات البنك المركزي المصري نحو المساهمة في التحول إلى مجتمع أقل اعتماداً على أوراق النقد، والاسهام في رفع مستوى فاعلية وكفاءة البنية التحية لنظم وخدمات الدفع للقطاع المصرفي وذلك بهدف إتاحة إتمام المعاملات المالية للعملاء بصورة لحظية على مدار الساعة.

وفي هذا الصدد، أرجو التكرم بالإحاطة باعتماد مجلس إدارة البنـك المركزي المصري بجلسته المنعقدة في ٢٦ أكتوبر ٢٠٢١ القواعد المنظمة لخدمات شبكة المدفوعات اللحظية داخل جمهورية مصر العربية (مرفق).

كما يرجى التكرم بالتوجيه نحو ما يلي:

- ضرورة قيام مصرفكم الموقر الالتزام بإنهاء كافة الاختبارات الخاصة باشتراك مصرفكم الموقر في شبكة المدفوعات اللحظية في موعد أقصاه ٦ أشهر اعتبارا من تاريخه.
- تفعيل خدمات التحويلات لشبكة المدفوعات اللحظية من خلال خدمة الأنترنت البنكي والهاتف المحمول البنكي في موعد أقصاه ١٢ شهر اعتبارا من تاريخه.

برجاء التفضل بالتنبيه باتخاذ ما يلزم نحو الالتزام بالقواعد المشار إليها.

وتفضلوا بقبول فائق الاحترام،،،

طارق عامر

البنك المركزي المصري
CENTRAL BANK OF EGYPT

القواعد المنظمة لخدمات

شبكة المدفوعات اللحظية

داخل جمهورية مصر العربية

Instant Payment Network (IPN)

أكتوبر 2021

البنك المركزي المصري

CENTRAL BANK OF EGYPT

المحتويات

مقدمة

في إطار خطة البنك المركزي المصري لتحقيق الشمول المالي ووصول الخدمات المصرفية لكل افراد المجتمع، وفي ضوء خطة البنك المركزي للتحول الرقمي والحاجة إلي زيادة أعداد المعاملات الالكترونية واتاحة وسائل السداد والتحصيل المختلفة لتلبية احتياجات العملاء، تهدف هذه القواعد إلى تحديد إطار عمل البنوك وتطبيقات الهاتف المحمول لمقدمي الخدمات على شبكة المدفوعات اللحظية بما يتيح للعملاء والبنوك القيام بعمليات التحويل اللحظية من خلال أدوات الدفع الالكترونية وتقديم الخدمات المصرفية الملائمة لكافة فئات المجتمع.

تعريفات عامة

يكون لكل من الكلمات والعبارات الآتية المعنى المبين لها أدناه أينما وردت في هذه القواعد:

الدفع اللحظي	هي إتمام عملية الخصم من حسابات العميل المرسل وإضافتها لحسابات العميل المستفيد لحظياً.
أدوات الدفع الإلكترونية	هي الأدوات المصرفية الإلكترونية التي تتم إتاحتها من قبل البنوك المصدرة لاستخدامها من خلال شبكة المدفوعات اللحظية.
شبكة المدفوعات اللحظية (IPN)	هي شبكة التشغيل البيني بين مختلف البنوك والتي تتيح إتمام عمليات التحويل اللحظي والعديد من الخدمات الإضافية الأخرى المشار اليها بالقواعد وذلك للبنوك وعملائها على مدار الساعة وطوال أيام الأسبوع
البنك المصدر (Issuer Bank)	البنك المسؤول عن إدارة حسابات العملاء والتصديق على معاملاتهم المالية من خلال أدوات الدفع الإلكترونية الصادرة من خلاله ووفقاً لإجراءات العمل المعتمدة من شبكة المدفوعات اللحظية.
البنك مقدم خدمات الدفع (PSP Bank)	هو البنك المسؤول عن التعاقد مع وتشغيل مقدمي خدمات الدفع وإتاحة خدماتهم لعملاء شبكة المدفوعات اللحظية بالإضافة إلى تفعيل قنوات التوزيع الإلكترونية الخاصة به والتي تشمل على سبيل المثال لا الحصر الإنترنت البنكي والهاتف المحمول البنكي.
البنك القابل (Acquirer Bank)	هو البنك المسؤول عن التعاقد مع وتشغيل الشركات/التجار من خلال شبكة المدفوعات اللحظية وذلك لتمكين الشركات/التجار من قبول المدفوعات الخاصة بعملاء شبكة المدفوعات اللحظية من خلال وسائل قبول المدفوعات المعتمدة من قبل الشبكة.

مقدم خدمات الدفع لشبكة المدفوعات اللحظية Instant Payment) Network Service (Provider	هو شركة مرخص لها بالعمل مع البنك مقدم خدمات الدفع لتقديم خدمات الدفع من خلال تطبيقات الهاتف المحمول الخاصة بها وفقاً لقواعد شبكة المدفوعات اللحظية وذلك لعملائها من الأفراد والتجار بعد الحصول على موافقة البنك المركزي المصري.
مقدم الخدمات التكنولوجية لشبكة المدفوعات اللحظية Technology) (Service Provider	هو شركة لتقديم الخدمات التكنولوجية المختلفة بالنيابة عن البنك وذلك فيما يخص خدمات شبكة المدفوعات اللحظية بعد الحصول على موافقة البنك المركزي المصري.
مكتبة الواجهة الآمنة (“Secure library” SL)	هي تطبيق آمن خاص بشبكة المدفوعات اللحظية وهي المسؤولة عن تشفير البيانات الحساسة الخاصة بعملاء شبكة المدفوعات اللحظية.
عنوان الدفع اللحظي Instant Payment) (“Address “IPA	هو عنوان يتم إنشاءه بواسطة العميل لكل حساب مصرفي ويتم تعريفه على شبكة المدفوعات اللحظية من خلال مقدم خدمات الدفع لتمكين العملاء من استقبال المعاملات المالية بدلالة عنوان الدفع اللحظي.
القوائم السلبية	القوائم السلبية: تشمل قوائم الكيانات الإرهابية والإرهابيين المنظمة بموجب القانون رقم ٨ لسنة ٢٠١٥ وتعديلاته، والقوائم الصادرة عن مجلس الأمن التابع للأمم المتحدة ذات الصلة بالإرهاب وتمويله وتمويل انتشار أسلحة الدمار الشامل، وأية قوائم أخرى يعدها البنك أو يرى ضرورة الرجوع إليها.

١. نطاق القواعد

١-١ تسري هذه القواعد على كافة البنوك العاملة في جمهورية مصر العربية وتعتبر هذه القواعد والضوابط هي الحد الأدنى اللازم لتقديم البنوك ومقدمي خدمات الدفع المصرح لهم من قبل البنك المركزي المصري للخدمات المختلفة من خلال شبكة المدفوعات اللحظية وعلى كافة البنوك ألا تكتفى بذلك وأن تتأكد من اتخاذ كافة ما يلزم نحو إدارة المخاطر المرتبطة بتقديم هذا النوع من الخدمات.

١-٢ تتضمن هذه القواعد بعض الضوابط والأهداف الرقابية العامة الواجب التوافق معها لتقديم خدمات شبكة المدفوعات اللحظية

١-٣ تسري هذه القواعد فيما يتعلق بتقديم خدمات شبكة المدفوعات اللحظية وذلك دون الإخلال بالضوابط الرقابية للعمليات المصرفية الإلكترونية السابق صدورها عن البنك المركزي المصري وكذلك التعليمات والقواعد الخاصة بتنفيذ العمليات المصرفية وضوابط مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري، وإجراءات العناية الواجبة بعملاء البنوك الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.

٢. إدارة مخاطر خدمات شبكة المدفوعات اللحظية

٢-١ المخاطر المرتبطة بخدمات تنفيذ العمليات المصرفية اللحظية من خلال القنوات الإلكترونية

يقترن تقديم خدمات تنفيذ العمليات المصرفية اللحظية من خلال القنوات الإلكترونية بالعديد من المخاطر، وبينما لا تعتبر تلك المخاطر جديدة على البنوك إلا أن خصائص خدمات المدفوعات اللحظية قد تزيد من درجات المخاطر بالإضافة إلى خلق تحديات جديدة لإدارة تلك المخاطر والتي يتعين على كافة الجهات المعنية بتقديم تلك الخدمات وضع الأطر والضوابط اللازمة لإدارة والحد من تلك المخاطر وتتمثل هذه المخاطر فيما يلي وذلك على سبيل المثال لا الحصر:

٢-١-١ المخاطر الاستراتيجية

تتمثل في قرار تقديم العمليات المصرفية اللحظية ونوع الخدمات المقدمة واختيار الوقت المناسب لتقديمها، ويقصد بذلك على وجه التحديد مدى الجدوى الاقتصادية لتقديم هذه الخدمات أو استمرارها وما إذا كانت نسبة العائد على الاستثمار سوف تفوق الاستثمارات الأولية ومصروفات استمرار تقديم هذه الخدمات، كما أن سوء تنفيذ العمليات المصرفية اللحظية والقرارات الاستثمارية غير المدروسة يمكنها أن تزيد المخاطر الاستراتيجية التي تتعرض لها البنوك.

٢-١-٢ مخاطر التشغيل / مخاطر المعاملات

تتمثل في المخاطر الناجمة عن الاحتيال أو الأخطاء في تنفيذ المعاملات، أو غيرها من الأحداث غير المتوقعة التي قد تؤدى إلى عدم قدرة البنك والشركة على تقديم الخدمات أو تعرض البنك أو عملائه لخسائر مالية. وبينما تكمن المخاطر في كل المنتجات والخدمات المقدمة، إلا أن مستوى المخاطر الخاصة بالمعاملات اللحظية يتأثر بهيكل الإجراءات والمعاملات البنكية ويتضمن ذلك أنواع الخدمات المقدمة ودرجة تعقيد العمليات والوسائل التكنولوجية المساعدة.

٢-١-٣ مخاطر الالتزام / المخاطر القانونية

تنشأ هذه المخاطر نتيجة تفعيل خدمات الدفع من خلال شبكة المدفوعات اللحظية، وقد تتضمن التحديات التنظيمية / القانونية الخاصة ما يلي:

- **بالنسبة للبنك المصدر لأدوات الدفع الإلكترونية:**
  - الأساليب التي يستخدمها البنك للتحقق من هوية العملاء حائزي أدوات الدفع الإلكترونية المصدرة من قبل البنك.
  - عملية التصديق على المعاملات المالية.
  - الاحتفاظ بالسجلات وكشوف الحسابات.
  - الالتزام بالقوانين السارية والخاصة بسرية الحسابات وحقوق العملاء وحماية البيانات الشخصية بالإضافة إلى المسؤولية القانونية للبنوك تجاه العملاء نتيجة احتمالات حدوث أية اختراقات لخصوصية البيانات، القرصنة أو الاحتيالات والإخفاقات التكنولوجية.
- **بالنسبة للبنك مقدم خدمات الدفع:**
  - تفعيل قنوات الدفع الخاصة بالبنك (eChannel's) لاستخدامها من قبل عملاء البنك لتنفيذ المعاملات المالية من خلال شبكة المدفوعات اللحظية.
  - إبرام التعاقدات مع مقدمي خدمات الدفع (PSPs) لاستخدام شبكة المدفوعات اللحظية.
  - مسئولية البنوك القانونية تجاه مقدمي خدمات الدفع لضمان آمن وسرية البيانات والعمل على حماية تلك البيانات، أو أي من الإخفاقات التكنولوجية الأخرى.
  - مخاطر الالتزام الناشئة عن الطبيعة المتغيرة للتكنولوجيا والتعديلات الرقابية التي تهدف إلى التعامل مع المشاكل الخاصة بتقديم هذا النوع من الخدمات.
- **بالنسبة للبنك القابل:**
  - إبرام التعاقدات مع الشركات والتجار.
  - الالتزامات القانونية والتنظيمية الناشئة عن التعاملات مع الشركات والتجار.

٢-١-٤ مخاطر السمعة

يتزايد مستوى المخاطر المتعلقة بالسمعة وذلك نتيجة تطور النظم وزيادة عدد المستخدمين، وفيما يلي بعض المخاطر التي قد تؤثر على سمعة البنك:

- انعدام الثقة نتيجة وجود معاملات غير مصرح بها على حسابات العملاء.

الفشل في تقديم خدمات يمكن الاعتماد عليها نتيجة لتكرار تعطل الخدمة أو طول مدة توقفها.

- شكاوى العملاء من صعوبة استخدام الخدمات أو عدم قدرة موظفي خدمة العملاء على حل هذه المشكلات.
- استغلال خدمات التحويل اللحظي عبر البنوك في عمليات غسل الأموال أو تمويل الإرهاب.

٢-١-٥ مخاطر أمن المعلومات والأمن السيبراني:

ينشأ هذا النوع من المخاطر نتيجة احتمال استغلال إحدى الجهات غير المشروعة لنقاط الضعف بأنظمة البنك مما ينتج عنه آثار تتعلق بمستوى سلامة وإتاحة وسرية البيانات.

٢-٢ مسئوليات والتزامات مجلس الإدارة والإدارة العليا

٢-٢-١ يتولى مجلس الإدارة بالبنك مسئولية الإشراف على إعداد استراتيجية العمل الخاصة وكذا اتخاذ قرار استراتيجي واضح بشأن الخدمات التي سوف يقوم البنك بتقديمها، وعلى الأخص يجب على مجلس الإدارة التأكد مما يأتي:

٢-٢-١-١ توافق خطط تطوير خدمات المدفوعات اللحظية المختلفة مع الأهداف الاستراتيجية للبنك.

٢-٢-١-٢ تحديد مدى قدرة البنك على تقبل المخاطر (Risk Appetite) وذلك فيما يتعلق بالخدمات المصرفية اللحظية مع ضمان إدراج عمليات إدارة المخاطر المتعلقة بهذه الخدمات في المنهجية العامة للبنك لإدارة المخاطر كما يجب أن تتم مراجعة السياسات والعمليات الحالية والخاصة بإدارة المخاطر وذلك للتأكد من كفايتها لتغطية المخاطر الجديدة التي قد تنتج عن خدمات المدفوعات اللحظية.

٢-٢-١-٣ وضع أطر الرقابة الفعالة على المخاطر المرتبطة بتقديم تلك الخدمات بما في ذلك تحديد المسؤوليات والسياسات والضوابط الرقابية لإدارة هذه المخاطر.

٢-٢-١-٤ وضع سياسة واضحة للحد من المخاطر المصاحبة للمعاملات الناشئة عن شبكة المدفوعات اللحظية على أن يتم تقييم تلك السياسة بصورة سنوية على أن تشمل تلك السياسة علي الأخص النقاط الأتية:

- التصديق على المعاملات.
- التسويات.
- عمليات الاعتراض (Disputes).
- رد العمليات (Refunds).
- الاحتيال (Fraud).

- الإفلاس للتجار والشركات المشتركة بالخدمة.
- مستوي الخدمة وكفاءتها.

٢-٢-٢ يجب على الإدارة العليا ضمان تحليل المخاطر المرتبطة بالمدفوعات اللحظية حال قيام البنك بتقديم هذه الخدمة والحد منها بالطرق الملائمة، وذلك وفقا لما يأتي:

٢-٢-٢-١ تحليل المخاطر الخاصة بتنفيذ المعاملات اللحظية قبل إطلاقها.

٢-٢-٢-٢ إعداد إجراءات مناسبة لمراقبة المخاطر التي يتم تحديدها والحد منها.

٢-٢-٢-٣ المراجعة المستمرة لتقييم نتائج الخدمات المقدمة من خلال شبكة المدفوعات اللحظية وفقا للخطط والأهداف المحددة.

٢-٢-٢-٤ الإشراف على التطوير والصيانة المستمرة للبنية التحتية للرقابة الأمنية التي توفر الحماية المناسبة لنظم وبيانات المعاملات التي يتم تنفيذها من خلال شبكة المدفوعات اللحظية من أي تهديدات داخلية أو خارجية، ومن أجل ضمان فعالية عملية المعاملات المالية، يجب على الإدارة العليا التأكد من اتخاذ الإجراءات الآتية:

٢-٢-٢-٤-١ تحديد مسئوليات واضحة خاصة بالإشراف على وضع وإدارة السياسات الأمنية الخاصة بالبنك.

٢-٢-٢-٤-٢ توفير الحماية اللازمة لمنع دخول الأشخاص غير المصرح لهم إلى بيئة الحاسب الآلي، والتي تتضمن كافة الأنظمة الحيوية وخوادم الشبكة وقواعد البيانات والتطبيقات والاتصالات، والأنظمة الأمنية الخاصة بشبكة المدفوعات اللحظية.

٢-٢-٢-٤-٣ توفير الضوابط الإلكترونية اللازمة والتي من شأنها منع أي أطراف داخلية أو خارجية غير مصرح لها من الوصول إلى التطبيقات وقواعد البيانات الخاصة بخدمات شبكة المدفوعات اللحظية ووضع أسس لتحديد حق الاطلاع على البيانات والذي بدوره يتطلب قيام البنك بتصنيف البيانات وتحديد صلاحيات الوصول إليها.

٢-٢-٢-٥ ضمان عدم تقديم البنك خدمات جديدة بالتعاون مع مقدمي خدمات الدفع أو تبنى وسائل تكنولوجية جديدة إلا إذا توافرت لدي البنك الخبرات اللازمة التي تمكن من إدارة المخاطر بكفاءة وينبغي ان تتناسب خبرات الموظفين والإدارة مع الطبيعة الفنية ودرجة تعقيد التطبيقات والتقنيات الخاصة بخدمات المدفوعات اللحظية.

٢-٢-٢-٦ قيام إدارتي المراجعة الداخلية والالتزام تقديم تقييم مستقل وموضوعي لمجلس الإدارة ولجنة المراجعة والإدارة العليا عن مدى فعالية الضوابط الداخلية التي يتم تطبيقها للحد من المخاطر الناتجة عن تقديم المدفوعات اللحظية بما في ذلك مخاطر التكنولوجيا ومخاطر غسل الأموال وتمويل الإرهاب.

٢-٢-٢-٧ مراجعة واعتماد الجوانب الرئيسية لعملية الرقابة الأمنية الخاصة بالبنك بما يشمل المراجعة الدورية لعمليات اختبار الإجراءات والنظم الأمنية - على سبيل المثال إجراء اختبار الاختراق دوريًا كما هو موضح في البند (٧-٣) بما في ذلك المتابعة المستمرة للتطورات في النظم الأمنية في هذا المجال، وتحميل وإعداد التحديثات الخاصة بالبرامج وحزم الخدمات المناسبة والتدابير اللازمة وذلك بعد إجراء الاختبارات المطلوبة.

٢-٢-٢-٨ إعداد آلية شاملة ومستمرة لإجراء الأبحاث النافية للجهالة Due Diligence والرقابة على عمليات التعهيد وعلاقات المتعهد بالأطراف الخارجية الأخرى التي يتم الاعتماد عليهم لتقديم تلك الخدمات مع تركيز الإدارة العليا على الأخص بالنقاط الآتية:

٢-٢-٢-٨-١ الإلمام الكامل بالمخاطر المترتبة على إبرام أي ترتيبات خاصة بالإسناد أو الشراكة أو الوكالة فيما يتعلق بالنظم الخاصة بشبكة المدفوعات اللحظية بالإضافة إلى توفير الموارد اللازمة للإشراف على هذه الترتيبات والحصول على موافقة البنك المركزي المصري قبل الشروع في إسناد الخدمات الخارجية.

٢-٢-٢-٨-٢ إجراء الأبحاث النافية للجهالة اللازمة فيما يتعلق بالكفاءة والبنية التحتية للنظام والقدرة المالية للشريك أو الطرف الخارجي وذلك قبل إبرام أي اتفاقيات خاصة بالإسناد أو الشراكة أو الوكالة.

٢-٢-٢-٨-٣ تحديد المسؤوليات التعاقدية لكافة الأطراف الخاصة باتفاقيات الإسناد أو الشراكة أو الوكالة بشكل واضح على سبيل المثال، يتم تحديد مسئوليات توفير المعلومات إلى مقدم خدمات الدفع وتلقيها منه بشكل واضح وضرورة قيام البنك بتحديد المعايير التنظيمية مع ضمان الالتزام بكافة القواعد والقوانين السارية في هذا الشأن.

٢-٢-٢-٨-٤ تتضمن تعاقدات خدمات الإسناد أو الوكالة اتفاقية لعدم الإفصاح عن المعلومات السرية لأطراف خارجية واتفاقية مستوى الخدمة والتي تشمل على سبيل المثال لا الحصر: تحديد الأدوار والمسؤوليات والوقت المطلوب لتنفيذ الخدمة وإجراءات وبيانات التصعيد والعقوبات في حال عدم الالتزام، هذا بالإضافة إلى البنود التي تحفظ حق البنك في التدقيق على المتعهد أو الاعتماد على تقارير التدقيق المعتمدة (الصادرة عن جهات تدقيق معتمدة).

٢-٢-٢-٨-٥ خضوع كافة النظم والعمليات الخاصة بخدمات شبكة المدفوعات اللحظية التي تتم من خلال عملية الإسناد أو الوكالة لنظام إدارة المخاطر وسياسات الخصوصية وأمن المعلومات التي تتفق مع المعايير الخاصة بالبنك.

٢-٢-٢-٨-٦ إجراء التدقيق الداخلي و/أو الخارجي بصفة دورية على العمليات التي تتم عن طريق الإسناد أو الوكالة، وينبغي ألا يقل نطاق

تغطية أعمال التدقيق عن مثيلتها التي يتم تطبيقها على المستوى الداخلي في البنك.

٢-٢-٢-٨-٧ توفير كافة تقارير التدقيق والتقييم لمفتشي قطاع الرقابة والإشراف بالبنك المركزي المصري.

٢-٢-٢-٨-٨ وضع خطط طوارئ مناسبة لخدمات شبكة المدفوعات اللحظية التي تتم عن طريق الإسناد أو الوكالة والتأكد من اختبارها بشكل دوري.

٢-٢-٢-٨-٩ أن تتسم إجراءات فسخ/إنهاء التعاقد بالفاعلية، كما يجب أن تضمن هذه الإجراءات الحفاظ على استمرارية العمل وسلامة البيانات وكذلك نقلها والتخلص منها.

٢-٢-٢-٨-١٠ وبالرغم من قيام البنك بإسناد بعض الخدمات لأطراف خارجية، فإن البنك يظل مسئولاً مسئولية كاملة تجاه مستخدمي النظام وتجاه التزام الأطراف الخارجية بهذه القواعد، والتأكد مما يأتي:

- الاحتفاظ بسجل محدث يشتمل على جميع اتفاقات وتعاقدات الإسناد والاستعانة بالأطراف الخارجية.
- وضع حدود لإسناد أكثر من وظيفة إلى مقدم خدمة واحد للحد من مخاطر التركز والتشغيل.

٢-٢-٢-٨-١١ يجب على الإدارة العليا التأكد من أن سياسة أمن المعلومات المُطبَّقة بالبنك - والمُعتمدة من مجلس الإدارة ويتم تحديثها بشكل دوري وإنها تراعي الخدمات المقدمة من خلال شبكة المدفوعات اللحظية، ويسهم ذلك في تحديد السياسات والإجراءات والضوابط الرقابية اللازمة لحماية العمليات البنكية من الاختراقات والانتهاكات الأمنية، كما يحدد المسؤوليات الفردية وكذا يوضح آليات التنفيذ والإجراءات التي يجب اتخاذها في حال مخالفة هذه السياسات والإجراءات.

٢-٢-٢-٨-١٢ تتولى الإدارة العليا تعزيز ونشر الثقافة الأمنية على كافة مستويات البنك عن طريق التأكيد على التزامهم بالمعايير العالية لأمن المعلومات، ونشر هذه الثقافة على كافة العاملين بالبنك.

٢-٢-٢-٨-١٣ ضرورة أن تكون منهجية التأمين قائمة على تحليل المخاطر والتهديدات الخاصة، مع الأخذ في الاعتبار المخاطر المتأصلة (Inherent Risk) والضوابط الرقابية التعويضية (Compensating Controls) من أجل الوصول لمستوى من المخاطر المتبقية (Residual Risk) التي تقع ضمن مستويات المخاطر المقبولة.

٢-٣ ضوابط مكافحة غسل الأموال وتمويل الإرهاب

٢-٣-١ يجب على البنوك المشتركة بشبكة المدفوعات اللحظية الالتزام بما يلي:

- الالتزام بقانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢ وتعديلاته ولائحته التنفيذية وتعديلاتها والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري، وإجراءات العناية الواجبة بالعملاء السارية الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.
- اتباع الارشادات الصادرة للبنوك في شأن تنفيذ آليات تنفيذ العقوبات المالية المستهدفة وكذا إرشادات المعنيين بالتنفيذ في شأن قوائم الكيانات الإرهابية والإرهابيين بشأن الوصول إلى القوائم المحدثة (المنشورة على موقع وحدة مكافحة غسل الأموال وتمويل الإرهاب www.mlcu.org.eg تحت بند القوائم السلبية).
- ايلاء عناية كافية لما يتفق مع طبيعة الخدمة من المؤشرات الاسترشادية الواردة بالبند السابع (المؤشرات الاسترشادية للتعرف على العمليات التي يشتبه في أنها تتضمن غسل أموال أو تمويل إرهاب) من الضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري.
- في حالة الاشتباه في أية عمليات تتم من خلال شبكة المدفوعات اللحظية وتتضمن غسل أموال أو متحصلات جريمة أصلية أو تمويل إرهاب القيام على الفور بإخطار وحدة مكافحة غسل الأموال وتمويل الإرهاب بشأنها، وذلك وفقا لأحكام قانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢ وكافة تعديلاتها.
- تطبيق إجراءات فعالة تشمل استخدام النظم الآلية للكشف عن مدى إدراج العميل والمستفيد الحقيقي (وفقاً للتعريف الوارد بإجراءات العناية الواجبة بعملاء البنوك الصادرة عن الوحدة وتعديلاتها) على القوائم السلبية قبل التعامل بما يشمل قيام بنك مرسل التحويل بالكشف عن مدي ادراج طالب التحويل على القوائم السلبية قبل تنفيذ التحويل وقيام بنك متلقي التحويل بالكشف عن مدي ادراج المستفيد على القوائم السلبية قبل الصرف له أو الإضافة لحسابه.
- متابعة موقع الوحدة بشكل يومي للتعرف على التحديثات على القوائم السلبية سواء بالحذف أو الإضافة أو التعديل.
- الاحتفاظ بالسجلات والمستندات الخاصة بالعملاء والعمليات وفقاً لما ورد بكل من قانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢ وتعديلاته ولائحته التنفيذية وتعديلاتها والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري

٣. القواعد العامة المنظمة للبنوك المشاركة في شبكة المدفوعات اللحظية

يتعين على البنك الراغب في الحصول على ترخيص للاشتراك في شبكة المدفوعات اللحظية التقدم للحصول على الموافقات اللازمة من البنك المركزي المصري ومراعاة ما يلي:

- الالتزام بالقواعد الصادرة عن البنك المركزي المصري وتحديثاتها.
- الالتزام بالقواعد الصادرة عن شبكة المدفوعات اللحظية وتحديثاتها.
- الالتزام بالمواصفات الفنية للربط الفني وقواعد تشغيل شبكة المدفوعات اللحظية وتحديثاتها.

٣-١ التزامات البنك المصدر (Issuer Bank) لأدوات الدفع الإلكترونية

٣-١-١ البنك المصدر هو المسؤول عن توثيق ومصادقة بيانات أدوات الدفع الإلكترونية الخاصة بعملائه للاشتراك في شبكة المدفوعات اللحظية من خلال أي من تطبيقات مقدمي خدمات الدفع (PSPs) وفق الضوابط والإجراءات المعتمدة من قبل البنك المركزي المصري.

٣-١-٢ عدم قيام البنك المصدر بإتاحة أي بيانات تخص حسابات العملاء قبل نجاح عملية المصادقة الإلكترونية لعملائه.

٣-١-٣ البنك المصدر هو المسؤول الرئيسي عن التصديق على أي معاملات لعملائه المتعاملين على شبكة المدفوعات اللحظية سواء من خلال تطبيقات مقدمي خدمات الدفع او من خلال قنوات البنك الإلكترونية.

٣-١-٤ يتعين على البنك في ضوء تقييمه للمخاطر المرتبطة بالخدمة قيام البنك بوضع الحدود المناسبة لقيم وعدد العمليات الشهرية وفقا ورؤية إدارة المخاطر لدي البنك وبما لا يتجاوز الحدود التالية في حال قيام العميل باستخدام تطبيقات مقدمي الخدمة المعتمدين:

- **الحد الأقصى** لقيمة المعاملة: **٥٠,٠٠٠** (خمسون ألف) جنيها مصريا.
- **الحد الأقصى** اليومي لقيمة المعاملات: **٦٠,٠٠٠** (ستون ألف) جنيها مصريا.
- **الحد الأقصى** الشهري لقيمة المعاملات: **٢٠٠,٠٠٠** (مائتان ألف) جنيها مصريا.

ولمحافظ البنك المركزي المصري أن يعدل تلك الحدود القصوى.

٣-١-٥ يمكن للبنك زيادة تلك الحدود في حال قيام البنك باستخدام وسائل تصديق إضافية من خلال قنوات البنك الإلكترونية وذلك بناءاً على ترخيص البنك كبنك مقدم خدمات دفع من خلال قنوات البنك الإلكترونية (Pre-authorized PSP Bank).

٣-١-٦ إتاحة استخدام العملاء لحساباتهم المصرفية من خلال تطبيقات مقدمي خدمات الدفع المعتمدين والتي تشمل إتاحة أنواع الحسابات المصرفية التالية كحد أدني للتعامل على شبكة المدفوعات اللحظية (حساب جاري-حساب توفير).

٣-١-٧ توفير أدوات الدعم الفني الكاملة للعملاء بما يتناسب مع مستوي أداء الخدمات المصرفية.

٣-١-٨ ضرورة إخطار العملاء بالرسوم الخاصة بالمعاملات بصوره واضحة قبل تنفيذ أي معاملة.

٣-١-٩ ضرورة إخطار العملاء بالمعاملات التي تمت على أدوات الدفع الإلكترونية الخاصة بهم بصوره واضحة من خلال رسائل نصية أو أية وسيلة أخرى يتم اعتمادها

٣-١-١٠ تخضع رسوم المعاملات المنفذة من خلال التطبيقات الخاصة بمقدمي خدمات الدفع (PSPs) إلى قواعد شبكة المدفوعات اللحظية.

٣-٢ التزامات البنك مقدم خدمات الدفع لشبكة المدفوعات اللحظية (PSP Bank)

٣-٢-١ يمكن للبنك مقدم خدمات الدفع الحصول على التراخيص التالية:

- مقدم خدمات دفع من خلال قنوات البنك الإلكترونية (Pre-authorized PSP Bank).
- مقدم خدمات الدفع من خلال تطبيقات مقدمي خدمات الدفع (Full Fledge PSP Bank).
- حال قيام البنك بالحصول على ترخيص تقديم خدمات الدفع من خلال قنوات البنك الإلكترونية (Pre-authorized PSP Bank) يلتزم البنك بإتاحة خدمات شبكة المدفوعات اللحظية من خلال القنوات الإلكترونية المختلفة للبنك فقط لا غير وذلك مع الالتزام بالمحددات التالية:

- يمكن للبنك تفعيل القنوات الإلكترونية مثل الإنترنت البنكي (Internet Banking) وتطبيق الهاتف المحمول البنكي (Mobile Banking).
- يقوم البنك بتحديد الحدود القصوى لعدد وقيم المعاملات اليومية والشهرية وفقاً لتقييم المخاطر لدي البنك.
- يقتصر تفعيل تلك الخدمة على قنوات البنك الإلكترونية الخاصة بالبنك فقط لا غير وللحسابات الصادرة عن البنك فقط.

٣-٢-٢ حال قيام البنك بالحصول على ترخيص مقدم خدمات الدفع (Full Fledge PSP Bank) فيمكن للبنك التعاقد مع مقدمي خدمات الدفع وذلك بعد استيفاء كافة الموافقات اللازمة من البنك المركزي المصري ومراعاة ما يلي:

- **يتم السماح للبنك مقدم الخدمة (Full Fledge PSP Bank) بإطلاق عدد ٥ تطبيقات كحد أقصي مع مقدمي الخدمة المعتمدين.**
  ولمحافظ البنك المركزي المصري أن يقوم بتعديل عدد مقدمي خدمات الدفع التي يتم السماح للبنك مقدم الخدمة بالتعاقد معهم.
- يُسمح للبنك مقدم خدمات الدفع التعاقد مع مقدمي خدمات الدفع لتوفير القنوات الإلكترونية لعملاء شبكة المدفوعات اللحظية من خلال تطبيق هاتف محمول خاص بمقدم خدمات الدفع يستخدم من قبل العملاء لتنفيذ عمليات مالية مختلفة من خلال حساباتهم لدي البنوك المصدرة.
- يسمح لمقدم خدمات الدفع (PSP) بالتعاقد **مع بنك واحد فقط لا غير** كبنك مقدم خدمات الدفع (PSP Bank).
- يكون البنك مقدم خدمات الدفع مسئول عما يلي:

- التعاقد مع مقدمي الخدمة وإتاحة خدمتهم للعملاء وذلك بعد الحصول على موافقة البنك المركزي المصري.
- توافق والتزام مقدمي خدمات الدفع (PSPs) بكافة التعليمات والقواعد الصادرة عن البنك المركزي المصري وشبكة المدفوعات اللحظية.
- الربط المباشر مع شبكة المدفوعات اللحظية وتفعيل تطبيق الواجهة الآمنة (Secure library "SL") الخاصة بشبكة المدفوعات اللحظية على كافة تطبيقات مقدمي خدمات الدفع.
- معامل التصديق الأول (1st factor of authentication) من خلال عملية الربط مع هاتف العميل المحمول (Hard Binding) وذلك بالتعاون مع مقدم خدمات الدفع (PSP) وفقاً لقواعد شبكة المدفوعات اللحظية.
- يتم معالجة كافة البيانات التي تتسم بالسرية من خلال تطبيق الواجهة الآمنة (Secure library "SL") والتي تشمل على سبيل المثال لا الحصر على بيانات التصديق وتأكيد الهوية، الرقم السري الخاص بحساب العميل (IPN PIN)، الرقم السري المتغير (One Time Password - OTP)، عرض رصيد العميل وكذلك كشف الحساب المختصر الخاص به.
- **يحظر علي مقدم خدمات الدفع (PSP) تسجيل أو طلب او عرض اي من البيانات التي تتسم بالسرية المشار لها سابقاً والمشار إليها كذلك في قواعد شبكة المدفوعات اللحظية خارج تطبيق الواجهة الآمنة (Secure library "SL").**

- التأكد من أن كافة المعاملات والمعلومات المعالجة بواسطة مقدمي خدمات الدفع (المرخص لهم تتم على أنظمة مؤمنة متواجدة داخل جمهورية مصر العربية) ولا يتم معالجة هذه المعاملات خارج جمهورية مصر العربية إلا بعد الحصول على موافقة البنك المركزي المصري.
- إتمام عمليات التفتيش الدوري على مقر وأنظمة مقدمي خدمات الدفع للتأكد من توافق قواعد العمل التي يتم إتباعها مع القواعد المصدرة من البنك المركزي المصري وشبكة المدفوعات اللحظية وشروط التعاقد الخاصة بالبنك.
- يتعين على البنك في ضوء تقييمه للمخاطر المرتبطة بالخدمة القيام بوضع الآليات والسبل اللازمة للتأكد من تشغيل المنظومة بكفاءة وفقاً لأعلي المعايير.

٣-٣ التزامات البنك القابل (Acquirer Bank) من خلال شبكة المدفوعات اللحظية

٣-٣-١ يلتزم البنك القابل لمعاملات شبكة المدفوعات اللحظية بقبول كافة المعاملات وفقاً والمواصفات الفنية القياسية المحددة من قبل شبكة المدفوعات اللحظية.

٣-٣-٢ يلتزم البنك القابل بقبول كافة المعاملات من قبل أي تطبيق/ قناة الكترونية معتمدة من قبل البنك المركزي المصري وشبكة المدفوعات اللحظية.

٣-٣-٣ اعتماد وسيلة القبول الإلكتروني من قبل البنك المركزي المصري وشبكة المدفوعات اللحظية.

٣-٣-٤ إمكانية قيام البنك القابل بالتعاقد مع التجار/الشركات مباشرة أو من خلال الاستعانة بميسري عمليات الدفع (Payment Facilitator) بعد الحصول على الموافقات اللازمة من قبل البنك المركزي المصري.

٣-٤ الخدمات المتاحة من قبل شبكة المدفوعات اللحظية

يمكن للبنوك تقديم الخدمات التالية للعملاء من خلال شبكة المدفوعات اللحظية:

٣-٤-١ المعاملات المالية:

- تحويل الأموال.
- عمليات الشراء.

٣-٤-٢ المعاملات غير المالية:

- الاستعلام عن الرصيد.
- كشف الحساب المختصر.
- تعيين رقم سري (IPN PIN) لكل حساب مصرفي مسجل

٣-٤-٣ تسجيل العملاء من خلال تطبيقات مقدمي خدمات الدفع وتشمل ما يلي:

- إنشاء عنوان دفع لحظي لكل حساب (Instant Payment Address - IPA).
- ربط رقم الهاتف المحمول بعنوان الدفع اللحظي (Mobile Number Mapped to IPA).
- تفعيل الحسابات على شبكة المدفوعات اللحظية وتعيين الرقم السري للحساب.


24/7

٤. ضوابط عامة

٤-١ يجب على جميع أطراف منظومة شبكة المدفوعات اللحظية الالتزام بتنفيذ جميع المعاملات المالية والغير مالية بصورة لحظية على مدار ال ٢٤ ساعة وطوال العام وفقا لقواعد شبكة المدفوعات اللحظية.

٤-٢ يحق للبنك الاستعانة بمقدم خدمة تكنولوجية (Technology Service Provider - TSP) بعد اعتماده من قبل البنك المركزي المصري وشبكة المدفوعات اللحظية للقيام ببعض المهام التكنولوجية بالنيابة عن البنك كتوفير وإدارة نظم البنك الإلكترونية المتعاملة مع شبكة المدفوعات اللحظية على أن يكون هناك تعاقد مباشر بين البنك ومقدم الخدمات التكنولوجية.

٤-٣ الالتزام بتعليمات حماية حقوق العملاء الصادرة عن البنك المركزي المصري في فبراير ٢٠١٩ وكافة تعديلاتها، كما يلتزم كافة أطراف المنظومة بالنقاط التالية على سبيل المثال لا الحصر:

٤-٣-١ إخطار العملاء برسوم المعاملات قبل تنفيذها.

٤-٣-٢ عدم استخدام بيانات العملاء بما يخالف الشروط والأحكام التي تمت موافقة العملاء عليها.

٤-٣-٣ إخطار العملاء لحظياً بنتيجة المعاملة المنفذة (مقبولة أو مرفوضة).

٤-٣-٤ إضافة أو خصم المبالغ المالية لحظياً من وإلى حسابات العملاء.

٤-٣-٥ توفير وسائل خدمة ودعم فني مناسبة للعملاء.

٤-٣-٦ توفير آليات لقيام العملاء بعمليات الاعتراض.

٤-٤ فيما يخص تطبيقات الهاتف المحمول الخاصة بمقدمي الخدمات، فيلتزم البنك مقدم خدمات الدفع بالتأكد مما يلي:

٤-٤-١ موافقة العميل علي الشروط والأحكام الخاصة بالخدمة وذلك بعد تحقق البنك المصدر لأدوات الدفع الإلكترونية وفقاً للشروط المشار اليها بالبند الخاص بإدارة وسائل التصديق والذي بدوره يعد موافقة من قبل العميل على تنفيذ المعاملات من خلال التطبيق الخاص بمقدم الخدمة.

٤-٤-٢ يُفضل ان تكون لغة التطبيق موحدة مع لغة نظام التشغيل (Operating System) الخاص بجهاز المحمول مع اتاحة حرية الاختيار للعميل في تغيير اللغتين العربية/الإنجليزية

٤-٥ فيما يخص عناوين المستفيدين (Payment Addresses) فيتم الالتزام بما يلي:

- يتم السماح بتبادل المعاملات المالية من خلال أحد عناوين المستفيدين التالية:
- رقم الحساب وكود البنك.
- رقم الحساب المصرفي الدولي (IBAN).
- رقم محفظة هاتف محمول مقبولة من خلال المحول القومي لخدمات الدفع باستخدام
- الهاتف المحمول.

- رقم بطاقة دفع إلكترونية.
- الأكواد الإشارية الخاصة بشبكة المدفوعات اللحظية والتي تشمل ما يلي:
  - عنوان المدفوعات اللحظي (Instant Payment Address (IPA.
  - رقم الهاتف المحمول (Mobile Number).
  - الكود التعريفي للتاجر (Merchant ID).

٤-٦ فيما يخص عنوان الدفع اللحظي فيتم الإلتزام بالمعايير التالية:

٤-٦-١ إمكانية تعيين عنوان دفع لحظي (Instant Payment Address - IPA) لكل حساب مصرفي يتم إضافته من خلال تطبيقات مقدمي خدمات الدفع.

٤-٦-٢ عنوان الدفع اللحظي هو عنوان لا يتكرر على مستوي الشبكة وتعود ملكيته الأصلية إلي العميل ويقوم على حفظه مقدمي خدمات الدفع.

٤-٦-٣ يتم تعيين المميز الإشاري الخاص بمقدم خدمات الدفع من خلال شبكة المدفوعات اللحظية.

٤-٧ فيما يخص إدارة وسائل التصديق:

٤-٧-١ تخضع كافة المعاملات المالية المنفذة من خلال شبكة المدفوعات اللحظية لعامل توثيق مزدوج (two factors of authentication).

٤-٨ فيما يخص المعاملات المنفذة من خلال تطبيقات مقدمي خدمات الدفع (PSPs):

٤-٨-١ التأكد من التزام مقدم خدمات الدفع بكافة الإجراءات الواجبة للمحافظة على تنفيذ عملية التصديق الأول (1st factor of authentication) بشكل سليم والتأكد من إتمام عملية الربط مع هاتف العميل المحمول (Hard Binding) والذي يقوم بربط بصمة الجهاز المحمول (Mobile Device Fingerprint - MDF) ورقم الهاتف المحمول (بناءً على عملية التنشيط) في أنظمة مقدم الخدمة وفقاً لقواعد شبكة المدفوعات اللحظية.

٤-٨-٢ التزام البنك المصدر بأن يكون الرقم السري الخاص بكل حساب مصرفي داخل شبكة المدفوعات اللحظية (IPN PIN) هو معامل التصديق الثاني (2nd factor of authentication) ويكون مسؤولية البنك المصدر لأداة الدفع الإلكترونية (Issuer Bank) الذي يدير الحساب المصرفي منفرداً، على أن يقوم العميل بتعيين رقم سري (IPN PIN) خاص بكل حساب يقوم بتسجيله من خلال تطبيقات الدفع المقدمة من خلال مقدمي خدمات الدفع.

٤-٨-٣ التزام البنك المصدر بإنشاء الرقم السري عند إضافة الحساب لأول مره على أي من تطبيقات الدفع وذلك من خلال استخدام مكتبة التأمين المشفرة الخاصة بشبكة المدفوعات اللحظية (IPN Secure Library).

٤-٨-٤ التزام البنك المصدر بالحفاظ على الرقم السري الخاص بحساب العميل بصورة مشفرة وفي كل الأحوال يحظر على أطراف المنظومة بما فيهم شبكة المدفوعات

اللحظية تسجيل او حفظ الرقم السري الخاص بالعميل (أو اي بيانات سرية آخري) وتكون مسؤولية حفظ وحماية الرقم السري هي مسئولية مشتركة بين البنك المصدر للحساب والعميل الخاص به.

٤-٨-٥ فيما يخص المعاملات المنفذة من خلال قنوات البنك الإلكترونية (eChannel's)، تخضع العمليات المنفذة من خلال قنوات البنك الإلكترونية (Pre-authorized transaction through eChannel's) لنفس معايير المصادقة الخاصة بهذه القنوات وفقاً للموافقات الخاصة بها والصادرة عن البنك المركزي المصري.

٤-٩ فيما يخص إدارة الرقم السري من خلال شبكة المدفوعات اللحظية (IPN PIN) فيلتزم البنك بما يلي:

٤-٩-١ الرقم السري يتكون من ٦ ارقام ولا يحتوي على حروف او رموز خاصة

٤-٩-٢ لا ينبغي السماح بالأرقام السهلة كرقم سرى مثال: ١١١١١١ أو ١٢٣٤٥٦.

٤-٩-٣ يجب تغيير الرقم السري باستخدام آلية تشفير قوية لا يوجد لها أي ثغرات او نقاط ضعف معروفة وان يكون طول مفتاح التشفير مناسب.

٤-٩-٤ أن الرقم السري لا يتم معالجته او ارساله او تخزينه كنص واضح وألا يظهر الرقم السري بشكل مقروء على أي جزء من شبكة المدفوعات اللحظية.

٤-٩-٥ التزام البنك المصدر لأداة الدفع الإلكترونية بالتنبيه على العملاء ان الرقم السري (IPN PIN) هو أساس تأمين حساباتهم وضرورة عدم تبادله مع اي طرف آخر.

٤-٩-٦ أن يتم تعليق التعامل على أداة الدفع من خلال شبكة المدفوعات اللحظية بشكل مؤقت عند تكرار دخول الرقم السري بطريقه خاطئة مع تحديد آليه واضحة لإعادة التفعيل.

٤-١٠ فيما يخص الاستعانة بمقدمي الخدمات التكنولوجية (Technology Service Provider - TSP) فيلتزم البنك بالإجراءات التالية:

٤-١٠-١ تحديد المسؤوليات التعاقدية للبنك ومقدم الخدمة في التعاقد بشكل واضح على سبيل المثال لا الحصر، يتم تحديد مسؤوليات إدارة وتشغيل الأنظمة بشكل واضح ومسؤوليات كل طرف.

٤-١٠-٢ بنود تخص بإدارة البنك لبيانات عملاءه والتزام مقدم الخدمة بالحفاظ علي سرية تلك البيانات وعدم الإفصاح عنها أو استخدامها إلا في حدود التعاقد مع البنك أو للأسباب القانونية المعتد بها.

٤-١٠-٣ وضع بنود تخص حق البنك والبنك المركزي في الرقابة والتفتيش على أداء مقدم الخدمة ودورية ذلك.

٤-١٠-٤ أن تتسم إجراءات فسخ/إنهاء التعاقد بالفاعلية، كما يجب أن تضمن هذه الإجراءات الحفاظ على استمرارية العمل وسلامة البيانات وكذلك نقلها والتخلص منها.

٤-١٠-٥ لا يصرح لمقدم الخدمة بالتعاقد مع شركات أخرى (أطراف ثالثة) من الباطن (Sub-Contracting) للقيام بالأعمال الموكلة له من قبل البنك من خلال هذا التعاقد إلا بالموافقة الكتابية من البنك مع بيان قائمة بالأعمال المسندة من قبل مقدم الخدمة للأطراف الآخرين.

٤-١٠-٦ التزام مقدمي الخدمات من خلال العقود المبرمة معهم بإخطار البنك عن أية أحداث يمكن أن يكون لها أثر كبير على مقدرتهم بالاضطلاع بالمهام الموكلة إليهم بالفاعلية المطلوبة.

٤-١٠-٧ ضرورة التزام مقدم الخدمة بإخطار البنك في حالة حدوث أي حالات قد يشتبه أنها غير مشروعه سواء كانت فعلية أو مشتبه بها أو انقطاع / عدم ثبات الخدمة على الأنظمة.

٥. مسؤوليات شركة بنوك مصر

٥-١ شركة بنوك مصر هي المسؤولة عن إصدار قواعد شبكة المدفوعات اللحظية وتحديثاتها وذلك بعد استيفاء موافقة البنك المركزي المصري.

٥-٢ تحدد شركة بنوك مصر اللوائح والمبادئ التوجيهية والأدوار والمسؤوليات والالتزامات الخاصة بالمشاركين فيما يتعلق بشبكة المدفوعات اللحظية ويشمل ذلك أيضًا معالجة المعاملات وتسويتها، وإدارة المنازعات.

٥-٢ تدير شركة بنوك مصر شبكة المدفوعات اللحظية (IPN - Instant Payment Network).

٥-٢ تحديد العمولات التبادلية لأطراف المنظومة.

٥-٥ تحديد القواعد والأطر التنظيمية لإنشاء عنوان الدفع اللحظي وتحديثها بصورة دورية بما يضمن وجود قائمة بالعناوين المحظور استخدامها على المنظومة.

٥-٦ تقوم شركة بنوك مصر بتسوية كافة معاملات شبكة المدفوعات اللحظية من خلال منظومة التسويات اللحظية للمدفوعات كبيرة القيمة (Real Time Gross Settlement) الخاصة بالبنك المركزي على حسابات البنوك الأعضاء بالشبكة.

٥-٧ تلتزم شركة بنوك مصر بكافة القواعد الصادرة عن البنك المركزي المصري.

٦. التسويات

٦-١ تتم عملية التسوية في حسابات البنوك داخل البنك المركزي المصري من خلال منظومة التسوية اللحظية بالجنيه المصري.

٦-٢ يجب على البنك في ضوء تقييمه لمخاطر التسوية التأكد من وجود رصيد كاف لتسوية كافة المعاملات.

٧. الضوابط الرقابية على خدمات شبكة المدفوعات اللحظية

٧-١ سرية وسلامة المعلومات

٧-١-١ يتضمن تقديم خدمات التحويل اللحظية من خلال تطبيقات الدفع الإلكترونية لمقدمي خدمات الدفع تداول بيانات سرية عبر تطبيقات الهاتف المحمول والشبكة الداخلية للبنك لذلك يجب على البنوك ومقدمي خدمات الدفع لشبكة المدفوعات اللحظية استخدام الأساليب المناسبة للحفاظ علي سرية وسلامة المعلومات المتداولة عبر الشبكة الداخلية والخارجية للبنك وذلك بما يتوافق مع متطلبات شبكة المدفوعات اللحظية.

٧-١-٢ يجب على البنوك اختيار تكنولوجيا التشفير التي تتناسب مع حساسية وأهمية المعلومات وكذا درجة الحماية المطلوبة، وفي هذا السياق يوصى دائما بتبني البنوك لتكنولوجيا التشفير التي تستخدم طرق التشفير المتعارف عليها دولياً، حيث تخضع نقاط القوة في هذه الطرق لاختبارات شاملة. وينبغي أن تطبق البنوك الممارسات السليمة لإدارة مفاتيح التشفير اللازمة لحماية هذه المفاتيح وذلك بما يتوافق مع متطلبات شبكة المدفوعات اللحظية.

٧-١-٣ قيام البنك بتأمين عملية تبادل أي بيانات أو ملفات بين البنك وشركاءه من مقدمي خدمات الدفع على أن تكون البيانات او الملفات مشفرة ويكون التبادل من خلال القنوات التالية:

- خط ربط مؤمن (Leased Line).
- شبكة ربط افتراضية (Virtual Private Network).

٧-١-٤ في حالة استخدام مقدمي خدمات الدفع بنية تحتية خارج مقره من قبل مقدمي البنية التحتية، فيجب على البنك الحصول على موافقة من البنك المركزي المصري قبل التعاقد مع مقدم خدمات الدفع.

٧-١-٥ ألا يتم اتصال البنك والأنظمة الخاصة به بالشبكة العالمية (الانترنت) أو أي من الشبكات غير المعتمدة دون الحصول على موافقة البنك المركزي المصري.

٧-١-٦ يجب على البنوك أيضاً تنفيذ ضوابط أخرى بخلاف أساليب التشفير، وذلك للحفاظ على سرية وسلامة المعلومات التي يتم تداولها من خلال المنظومة ويتضمن هذا على سبيل المثال لا الحصر:

- الضوابط وأعمال التدقيق اللازمة للتأكد من سلامة تسوية أرصدة العملاء بعد تنفيذ المعاملات بالإضافة إلى التأكد من سلامة البيانات التي يتم نقلها بين الأنظمة المختلفة.
- مراقبة المعاملات غير المعتادة بما في ذلك المعاملات محل الاشتباه أو السجلات التي يشتبه التلاعب فيها
- يجب على البنوك التأكد من تشفير العملية بداية من قناة الدفع المستخدمة لإجراء العملية وصولاً إلى أجهزة الخادم Servers الخاصة بتنفيذ أمر الدفع.

٧-١-٧ ينبغي على البنك تطبيق سياسة الفصل بين المهام، وذلك للتأكد من عدم إمكانية قيام أي موظف داخل البنك بأي عمل غير مصرح له وإخفائه، ويتضمن هذا على سبيل المثال لا الحصر، إدارة حساب المستخدم وتنفيذ المعاملات وحفظ وإدارة مفاتيح الشفرة الخاصة بالنظام وإدارة النظام System Administration وتشغيله System Operations.

٧-١-٨ يجب الحد من تخزين بيانات على الذاكرة الداخلية للهاتف المحمول، وفى حالة الاحتفاظ باي بيانات على الهاتف المحمول – للضرورة القصوى – يجب استخدام الوسائل المناسبة لحماية ما تم تخزينه.

٧-١-٩ يجب بان يقوم تطبيق الهاتف المحمول بتنفيذ أليات كشف كافية تضمن ان الهاتف المحمول ليس عرضة للمخاطر مثل Jailbroken/Rooted مثال: يقوم المخترق بتحميل برنامج على الجهاز المحمول يمكنه من الدخول إلى الملفات السرية الخاصة بالمستخدم.

٧-١-١٠ يجب بأن يتم حماية تطبيقات الهاتف المحمول ضد أي لقطات تلقائية Screenshots والتي يمكن أن تتم عن طريق برامج تجسس تعمل على نفس جهاز الهاتف المحمول حال وجود إمكانية فنية لتطبيقه.

٧-١-١١ يجب أن تخضع أنظمة البنك وكذلك تطبيقات مقدمي خدمات الدفع إلى اختبارات مُتعددة قبل التشغيل للتأكد من قدرتها على القيام بالمهام المُوكلة لها وفى حالة تحديث تلك الأنظمة يتم إعادة اختبارها بذات الوسائل لضمان استمرار سلامتها.

٧-١-١٢ يجب استخدام وتفعيل المصادقة الثنائية (2-factor authentication) في جميع التطبيقات.

٧-٢ البنية التحتية والمتابعة الأمنية للمنظومة

٧-٢-١ يجب على البنوك إنشاء بيئة تشغيل ملائمة تعمل على دعم وحماية أنظمتها الخاصة المرتبطة بتطبيقات شبكة المدفوعات اللحظية، بحيث تحتوي تلك البيئة على بنية تحتية آمنة لتلك الخدمات - والتي تشمل على سبيل المثال لا الحصر إعداد خوادم الشبكة وأنظمة اكتشاف ومنع الاختراق وأجهزة جدار الحماية Firewall وأجهزه التوجيه وخلافه - كما تحتوي أيضا على إجراءات حماية ملائمة للشبكات الداخلية وروابط الشبكات مع الجهات الخارجية بما يشمل شركة بنوك مصر بصفتها الشركة المسؤولة عن شبكة المدفوعات اللحظية.

٧-٢-٢ تقع المسؤولية الكاملة لتقديم الخدمات على البنوك المشتركة بالخدمة والتي يجب عليها بذل العناية الواجبة لضمان أمان كافة المعاملات، وكذا مراقبة كل من الأنظمة المتصلة بالشبكة والبنية التحتية بصورة استباقية بشكل دائم على مدار ٢٤ ساعة طوال الأسبوع، وذلك لرصد وتسجيل أي مخالفات أمنية، أو أي اختراقات، أو نقاط ضعف مشتبه فيها، وكذلك أي أنشطة غير طبيعية محل اشتباه تتم على الأنظمة.

٧-٢-٣ يجب على البنوك التأكد من وجود مسارات التدقيق Audit Trails لكل المعاملات المصرفية التي تتم عبر أنظمة/تطبيقات شبكة المدفوعات اللحظية كما يجب

ضمان حماية تلك المسارات ضد أي تلاعب أو تغيير غير مُصرَّح به، وأن يتم الاحتفاظ بها لمدة زمنية تتوافق مع ما تحدده سياسات البنك تطبيقاً للمتطلبات القانونية وطبقاً للضوابط والتعليمات الرقابية الصادرة في هذا الشأن ويهدف هذا الإجراء إلى تسهيل إجراءات التحقيق في أي عملية احتيال، وحل أي نزاع أو شكوى إذا لزم الأمر وعند تحديد ما سيتم الاحتفاظ به في مسارات التدقيق، يمكن الأخذ في الاعتبار الأنواع التالية من الأنشطة وذلك كحدٍ أدنى:

- عمليات فتح أو تعديل أو إغلاق حساب مستخدم على الانظمة المختلفة الخاصة بالخدمة.
- أي عملية ذات تبعات مالية.
- أي تصريح يمنح مستخدم لتجاوز أي من الحدود أو الصلاحيات.
- أي تعديل أو إضافة أو إلغاء لصلاحيات المستخدمين أو امتيازات خاصة بالدخول على الأنظمة

٧-٢-٤ يجب أن يتم مراجعة كافة ما يتم إصداره من سجلات تدقيق Audit Logs وإنذارات التأمين اللحظية Real Time Security Alerts -مثل إنذارات أنظمة كشف ومنع الاختراق - بواسطة الموظفين أو فرق العمل المعنية وذلك بطريقة دورية وفى الوقت المناسب.

٧-٢-٥ تطبيق معايير وإجراءات حصيفة فيما يخص إمكانية الدخول إلى أماكن عمل النظام Physical Security بما في ذلك البرامج والأجهزة المُشغِلة للنظام والشبكات وأجهزة التشفير ومراكز المعلومات التي تقوم بتشغيل جزء أو أجزاء من النظام.

٧-٣ تقييم النظام الأمني للخدمة

٧-٣-١ يجب على البنوك دورياً تقييم الوضع الأمني لكافة الأنظمة - التطبيقات، والشبكات، وأجهزة التأمين، وخوادم نظام أسماء النطاقات وخوادم البريد الإلكتروني، إلخ - المتعلقة بتشغيل المنظومة، وذلك في المركز الرئيسي للمعلومات والمركز الاحتياطي الذي يستخدم في حالات الكوارث.

٧-٣-٢ يجب على البنوك إجراء تقييم دوري لنقاط الضعف Vulnerability Assessment كل ثلاثة أشهر على الأقل أو عند حدوث تغييراً جوهرياً في البيئة التشغيلية للأنظمة المختلفة الخاصة بالخدمة لاكتشاف نقاط الضعف في بيئة تكنولوجيا المعلومات، وتقييمها. ويمكن أن يتولى هذا التقييم مستشار أو مقدم خدمة خارجي للبنك وأن يكون مقدم الخدمة مختلف عن مقدم الخدمة القائم باختبارات الاختراق، أو أن يتولى هذا التقييم إدارة أمن المعلومات بالبنك، وذلك على النحو التالي:

- يجب أن يحتوي نطاق تقييم نقاط الضعف على اختبار الثغرات الشائعة في الشبكة (مثل: الثغرات التي تُمكِّن المخترق من حقن قواعد البيانات SQL Injection وتخطى عملية التصديق Authentication Bypass والتخزين غير الآمن للبيانات Insecure Storage.. إلخ).

- يجب على البنك إعداد خطة لمعالجة المشاكل التي تظهر في تقييم نقاط الضعف، ثم التحقق من صحة هذه المعالجة عن طريق إعادة الاختبار لإثبات أنه قد تم التعامل مع هذه المشاكل بالكامل.

٧-٣-٣ التزام البنك بعدم إطلاق الخدمات الجديدة قبل الانتهاء من موافاة البنك المركزي المصري بتقرير اختبارات الاختراق Penetration Test Report على بيئة العمل الفعلية والذي يفيد عدم وجود أي نقاط ضعف عالية أو متوسطة الخطورة ومن ثم الحصول على موافقة البنك المركزي المصري بتفعيل الخدمة، على ان يتم تقديم التقرير المشار اليه إلى البنك المركزي المصري في مدة لا تتجاوز ثلاثة أشهر من تاريخ اصداره.

٧-٣-٤ يجب على البنك القيام باختبارات الاختراق Penetration Testing وذلك لعمل تقييم مفصل ومتعمق للوضع الأمني للنظام من خلال محاكاة للهجمات الفعلية على النظام على أن يتم ذلك على الأقل مرة واحدة سنويا، أو عند حدوث تغيير في النظام، على أن تتم مراعاة ما يلي:

- يجب أن يتولى إجراء اختبار الاختراق أحد مقدمي الخدمة الخارجيين المستقلين، حيث يجب عليه أولاً التوقيع على اتفاقية السرية وعدم الإفصاح قبل مزاولة العمل Non-Disclosure Agreement.
- يجب أن يكون لدى البنوك تقرير مبدئي عن اختبار الاختراق وخطة المعالجة Penetration Test Report & Remediation Plan، التي تم اصدارها والموقعة من مقدم الخدمة الخارجي.
- يجب على البنوك التحقق من صحة معالجة الملاحظات الناتجة عن اختبار الاختراق سواء كان على الأنظمة الرئيسية أو الأنظمة البديلة المستخدمة لمواجهة الكوارث مع مراعاة إجراء اختبار الاختراق على الانظمة في مركز الطوارئ.
- يجب على مقدم الخدمة الخارجي إصدار تقرير نهائي موقع منه عن اختبار الاختراق لكي يقوم البنك بتقديمه إلى البنك المركزي المصري، بجانب التقرير المبدئي الأول.
- غير مسموح باختيار نفس مقدم الخدمة الخارجي لأداء أكثر من اختباري اختراق متتاليين.

٧-٤ الاستجابة للأحداث وإداراتها

٧-٤-١ يجب على البنوك وضع إجراءات للاستجابة للحدث وإدارته خلال تقديم الخدمة، بهدف الإبلاغ والمعالجة الفورية لأي اختراقات أمنية سواء كانت فعلية أو مشتبه فيها، وكذلك أي حالات احتيال أو انقطاع/عدم ثبات الخدمة، سواء أثناء أو بعد ساعات العمل. ويجب على البنوك اتخاذ الإجراءات الضرورية التالية (على سبيل المثال لا الحصر):

- سرعة اكتشاف مصدر الحدث، وتحديد ما إذا كان قد وقع نتيجة وجود نقاط ضعف في النظم التأمينية بالبنك من عدمه.
- تقييم النطاق المحتمل للحدث ومدي تأثيره.
- تصعيد الأمر إلى الإدارة العليا للبنك بشكل فوري، إذا كان هذا الحدث قد يضر بسمعة البنك أو يؤدى إلى خسائر مالية.
- إخطار العملاء المتضررين على الفور، إذا لزم الأمر.
- احتواء الخسائر المتعلقة بأصول البنوك وبياناتها وسمعتها، وبوجه خاص الخسائر المتعلقة بعملائها.
- جمع الأدلة الجنائية الرقمية والأدلة الجنائية وحفظها بطريقة مناسبة وبأسلوب يضمن الرقابة على تلك الأدلة وضمان عدم التلاعب بها لتغيير محتواها، لتسهيل التحقيقات اللاحقة وإقامة دعوى قضائية ضد مخترقي النظام والمشتبه فيهم إذا لزم الأمر بالإضافة إلى تنفيذ عملية مراجعة لهذا الحدث.

٧-٤-٢ يجب تكوين فريق للتدخل السريع لإدارة الحدث للتعامل معه بما يتوافق مع الإجراءات الموضحة أعلاه على أن يتم منح هذا الفريق الصلاحيات اللازمة للتصرف في حالة الطوارئ، كما يجب أن يتلقى التدريب الكافي على استخدام الأجهزة التأمينية، والقدرة على تفسير أهمية البيانات ذات الصلة في سجلات التدقيق، وتحديد الإجراءات المناسبة اللازم اتخاذها - كمنع حركة مرور معينة على الشبكة، أو غلق بعض الخدمات.

٧-٤-٣ يجب على البنوك إعداد سجل بالأحداث العارضة المرتبطة بالخدمة المقدمة والتفاصيل الخاصة بها بالإضافة إلى إعداد تقرير دوري للعرض على الإدارة العليا لاتخاذ الإجراءات المناسبة لتلافي تكرارها.

٧-٤-٤ يتولى مسئول الالتزام بالبنك مسئولية التأكد من إبلاغ البنك المركزي المصري بصورة صحيحة وفي خلال ٦ ساعات من اكتشاف الحادث بكافة الحالات الواردة أدناه:

- أي هجمات احتيال لتسريب أو إفشاء هوية مُستخدم النظام أو وثائق اعتماد الشخصية (كالاحتيال Phishing، وملفات التجسس (حصان طروادة (Trojans، والبرمجيات الخبيثة Malware.. إلخ).
- الدخول غير المصرح به إلى أنظمة تكنولوجيا المعلومات بالبنك لتسريب بيانات مُستخدم النظام المتعلقة بالخدمات المقدمة.
- أي عملية تخريبية للبيانات المتعلقة بأنظمة الخدمات المقدمة والتي لا يمكن استرجاعها.
- الإيقاف التام المتعمد أو العارض للخدمات المقدمة لفترة تزيد عن الفترة المحددة كهدف لوقت الاسترجاع RTO المحدد من قبل البنك.
- أي حالة من حالات الاحتيال الداخلي ذات الصلة بتلك الخدمات المقدمة يتم إرسال جميع التقارير بالبريد الالكتروني على العناوين التالية:
  cbe.infosec@cbe.org.eg
  eg-fincirt@cbe.org.eg

٧-٥ اعتبارات الأداء وضمان استمرارية العمل

٧-٥-١ يجب على البنوك توفير الخدمات المقدمة على مدار الساعة، مع ضمان أداء الخدمة للعملاء بالسرعة المناسبة طبقا لما تم ذكره في الأحكام والشروط الخاصة بالخدمة مع أخذ توقعات العملاء بعين الاعتبار.

٧-٥-٢ يجب على البنوك وضع معايير لتقييم ومتابعة مستوى أداء تقديم الخدمات المقدمة كما يجب اتخاذ التدابير اللازمة للتأكد من قدرة نظم تلك الخدمات والنظم الداخلية الخاصة بتقديم الخدمة على التعامل مع حجم العمليات المتوقعة والنمو المستقبلي لهذا النوع من الخدمات.

٧-٥-٣ يجب أن تأخذ البنوك في اعتبارها التخطيط لضمان استمرارية العمل عند تطويرها للخدمات المقدمة، على أن يتم أيضا مراعاة الممارسات التالية:

- في حال حدوث عطل في الخدمة، يجب أن تحتوي خطة استمرارية العمل على خطوات محددة لكيفية استئناف أو استرجاع تلك الخدمات، تحدد هذه الخطوات بناء على أهداف وقت ونقطة الاسترجاع RTO & RPO المحددين مسبقاً مع ضرورة دورية المراجعة والتحديث بأي مستجدات أو مخاطر.
- وجود نسخ احتياطية للبيانات لاستعادة البيانات ووجود خطط عمل بديلة للطوارئ.
- يجب أن تتمتع خطة استمرارية العمل الخاصة بالخدمات المقدمة بالقدرة على التعامل مع أي من الحالات التي يتم فيها الإسناد لأطراف خارجية.

٨. أمن العملاء وضوابط لبعض المخاطر الأخرى

٨-١ يجب على البنوك أن تحدد بدقة كافة الاحكام والشروط بينها وبين عملائها من خلال تطبيقات مقدمي خدمات الدفع او من خلال أي قناة دفع الكترونية متصلة بشبكة المدفوعات اللحظية وبما لا يتعارض مع تعليمات حماية حقوق عملاء البنوك المصدرة في فبراير ٢٠١٩ وكافة تعديلاتها مع مراعاة ما يلي:

٨-١-١ تحديد كافة الشروط والاحكام الخاصة بالاشتراك على شبكة المدفوعات اللحظية وتنفيذ المعاملات من خلال تطبيق الهاتف المحمول وانه لا يتم الاشتراك في الخدمة الا بعد الموافقة الكترونيا على تلك الشروط والاحكام.

٨-١-٢ صياغة الشروط والاحكام بصورة واضحة ومحددة بحيث يسهل فهمه بالنسبة لأي عميل مع تجنب استخدام الكلمات والعبارات التي تحمل أكثر من معنى.

٨-١-٣ توضيح التزامات كل من مقدم خدمات الدفع ومُستخدم النظام في حالة الإخلال بأي من شروط التعاقد.

٨-١-٤ تحتوي الشروط والاحكام على بنود محددة واضحة والتي يجب أن تتضمن ما يلي كحد أدنى:

- تفويض مقدم خدمات الدفع بإرسال المعاملات لشبكة المدفوعات اللحظية لتقديم الخدمات المتفق عليها واحقية العميل في ايقاف الخدمة.
- توضيح مستوى خصوصية بيانات العملاء ومدى إتاحتها للغير بما يتوافق مع التعليمات الرقابية الصادرة من البنك المركزي المصري أو القوانين المنظمة لذلك.
- توضيح بشكل مُفصَّل الخطوات الواجب على مُستخدم النظام إتباعها لتفعيل الخدمة في حالة الاشتراك لأول مرة أو في حالة وقف الخدمة أو إعادة تشغيلها، موضحاً الوقت اللازم لإيقاف الخدمة من لحظة طلب إيقافها من قِبل مُستخدم النظام والطرق المختلفة لطلب إيقاف الخدمة.
- إتاحة امكانية إيقاف استخدام الخدمة عند إساءة استخدامها من قبل مستخدم النظام.

٨-١-٥ يقوم البنك المصدر لاداه الدفع الإلكترونية وكذلك مقدم خدمات الدفع بإيجاد آلية لدراسة الشكاوى ويُنص صراحة في بنود واحكام تقديم الخدمة على طريقة تقديم الشكوى إلى البنك أو مقدم خدمات الدفع والحد الأقصى للوقت المُستغرق للتحقيق في الشكوى من قِبل الأطراف المختلفة.

٨-١-٦ في حالة وجود منازعات على المعاملات المالية أو وجود شكاوى من قِبل مُستخدمي النظام، تخضع عمليات تسوية المنازعات إلى قواعد ثابتة ومُعلنة لمُستخدم النظام وتكون تسوية المنازعات وفقاً لقواعد شبكة المدفوعات اللحظية، علماً بأن سجلات النظام هي حجة قاطعة بشرط عدم حدوث خلل في النظام وبشرط وجود سجلات كاملة للمعاملات محل المنازعة.

٨-١-٧ التأكيد على التزام مُستخدم النظام بقراءة التحذيرات والإطارات التنبيهية (مثل التنبيهات الأمنية أو تنبيهات محاولات الاحتيال/الهندسة الاجتماعية Social Engineering.. إلخ) والتأكيد أيضًا على أن قبول مُستخدم النظام لأي تغيير في الشروط والأحكام التي ستظهر من خلال النظام إلكترونيا والموافقة عليها الكترونيا للاستمرار في الحصول على الخدمة.

٨-١-٨ التأكيد بوضوح على أن القوانين المصرية ذات الصلة ولوائحها التنفيذية والتعليمات والقواعد الرقابية هي التي تحكم الخدمات التي يقوم البنك ومقدمي خدمات الدفع (PSPs) بتقديمها للعملاء من خلال شبكة المدفوعات اللحظية ويتم تسوية النزاعات داخل جمهورية مصر العربية.

٨-١-٩ توضيح مسئوليات المُستخدم في الحفاظ على كلمة السر/الرقم السري الخاص به وإبلاغ البنك في حال فقدانه للرقم السري او اشتباه العميل في ان بياناته السرية التي قد تؤدي إلي الإخلال بسلامة حساباته قد تم الاطلاع عليها من قبل الغير.

٨-٢ رصد الأنشطة غير العادية

٨-٢-١ يتعين على البنوك وضع تدابير فعالة للرقابة المستمرة لضمان سرعة اكتشاف أي معاملات غير عادية تحدث من خلال المنظومة يُشتبه أن تؤدى إلى عمليات احتيال وعلى وجه الخصوص، ينبغي أن تكون تلك التدابير قادرة على اكتشاف حالات مثل:

- حدوث العديد من عمليات تحويل أموال باستخدام تطبيقات الهاتف المحمول إلى حساب مستفيد آخر خلال فترة زمنية وجيزة، وخاصة إذا كانت المبالغ المحولة تقترب من الحد الأقصى المسموح به. وكذلك الزيادة المفاجئة في الأموال المحولة لحسابات مستفيدين.

٨-٢-٢ يجب أن تتمتع آلية الرقابة المتبعة بالقدرة على سرعة إصدار تحذيرات إلى المختصين بالمتابعة والرصد للخدمات المقدمة عند حدوث أي تحويل أموال محل شبهة احتيال، وكذلك أي أنشطة غير معتادة ويجب على البنوك في تلك الحالات أن تقوم بالتحقق من ذلك مع أصحاب هذه الحسابات التي تتم عليها هذه المعاملات أو الأنشطة في أسرع وقت ممكن وإخطار الجهات المختصة.

٨-٢-٣ يتم الرجوع الى العملاء فور رصد أي معاملة غير اعتيادية للتحقق من قيامهم بها.

٨-٢-٤ يجب على البنك تطبيق إجراءات محددة ومُعتمدة للتعامل مع المعاملات المشتبه بها.

٨-٣ توعية مستخدمين النظام

٨-٣-١ نظراً لأن الأجهزة التي يستخدمها العملاء للدخول على تطبيق الهاتف المحمول الخاص بمقدمي خدمات الدفع وكذلك القنوات الإلكترونية الخاصة بالبنك تقع خارج نطاق سيطرة البنك، فإن احتمال ظهور مخاطر أمنية تزداد في حالة عدم معرفة مُستخدم النظام بالاحتياطات الأمنية الضرورية لاستخدام الخدمة أو سوء فهمها ولذلك يجب على البنك أن يولي اهتماماً خاصاً لتوعية العملاء عن طريق تقديم نصائح سهلة الفهم وواضحة تتعلق بالاحتياطات الأمنية الواجب اتخاذها عند التعامل مع تلك الخدمات والتزامهم حيال ذلك.

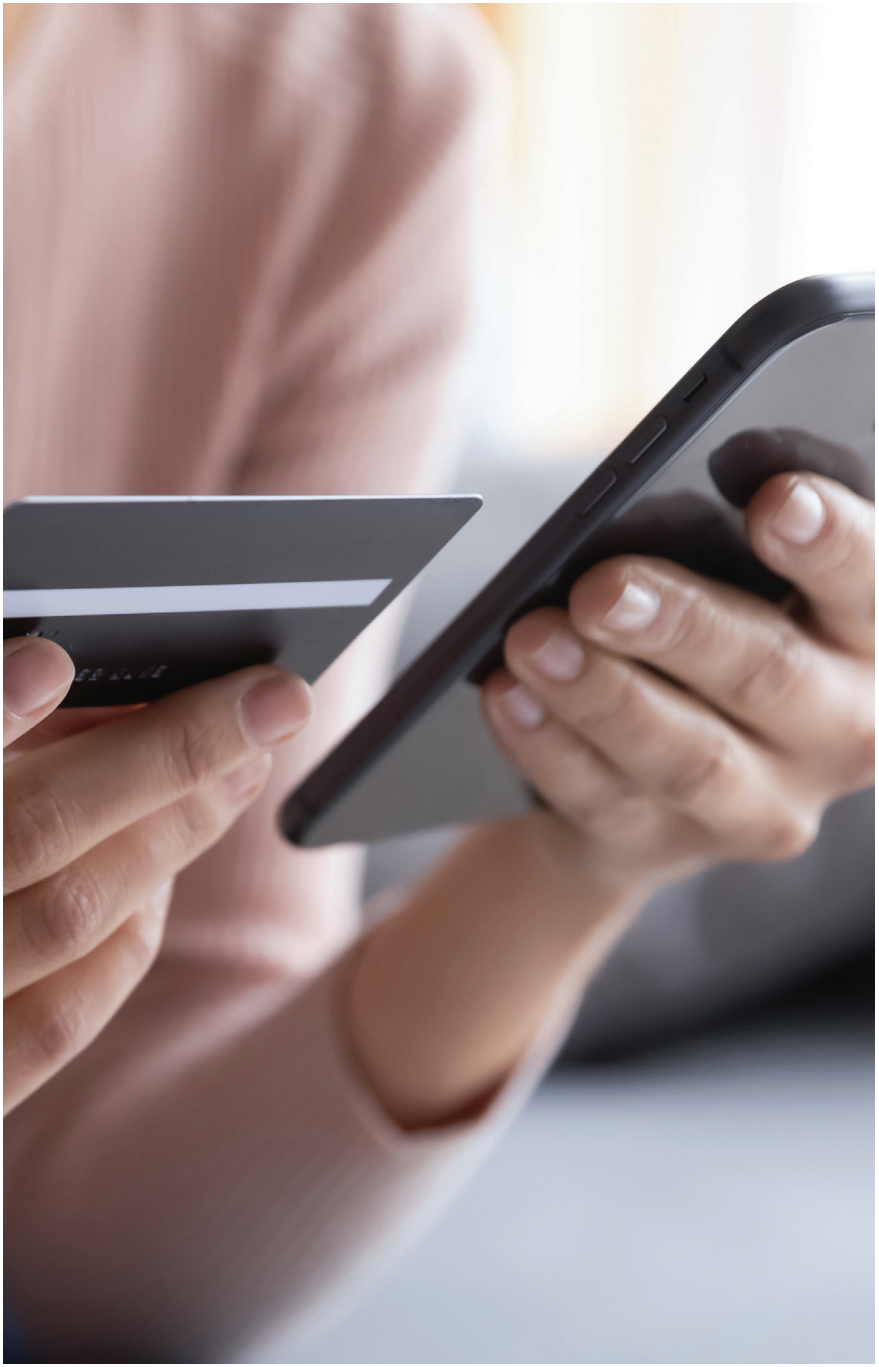
٨-٣-٢ التأكيد على العملاء وتوعيتهم أن موظفي البنك أو وكلاءه أو مقدمي خدمات الدفع لا يجوز لهم أن يطلبوا من مُستخدم النظام الإفصاح عن البيانات السرية (كالأرقام التعريفية أو كلمات السر) عن طريق البريد الإلكتروني أو غيره وفي حالة وقوع ذلك يجب على مُستخدم النظام الاتصال بالبنك في أسرع وقت ممكن.

٨-٣-٣ توعية عملاء تلك الخدمات بالطرق التي يمكنهم من خلالها التأكد من صحة التطبيق الرسمي.

٨-٣-٤ تختلف النصائح الخاصة بالاحتياطات الأمنية الواجب إتباعها وفقا لطبيعة العملاء، وطبيعة الخدمات المقدمة، وتشمل النصائح ما يلي كحد أدنى:

- اختيار وحماية كلمات السر الخاصة بالعميل (وأيضا اسم المستخدم في حالة السماح للعميل باختياره). على سبيل المثال، يجب على البنوك أن تنصح العملاء بإنشاء كلمة سر معقدة وعدم اختيار كلمات سر تتضمن معلومات مثل تاريخ الميلاد أو رقم الهاتف قد يكون من السهل التعرف عليها.
- الحماية ضد تقنيات الهندسة الاجتماعية Social Engineering Techniques حيث يجب توعية العملاء بضرورة عدم الإفصاح عن أي معلومات شخصية - كبطاقة الهوية أو جواز السفر أو العناوين أو أرقام حسابات البنك الخاصة بهم - لأي شخص لم يتأكد من هويته أو استخدام تطبيقات هواتف محمولة موضع شك. كما يجب التأكيد على العملاء بعدم الإفصاح عن كلمات السر لأي شخص بما في ذلك موظفي البنك أو وكلائه.
- يجب على البنوك مراجعة النصائح والإرشادات الخاصة بالاحتياطات التأمينية التي يتم تقديمها للعملاء للتأكد من كفايتها وملائمتها للتغيرات التي تستجد على البيئة التكنولوجية والخدمات المقدمة.
- يتم إخطار مستخدم النظام بوسيلة التصرف في حالة اكتشاف أي شخص آخر للرقم السري الخاص بمُستخدم النظام.

٨-٣-٥ نظراً لوجود صعوبة في توفير العملاء لوقت طويل لاستيعاب الإرشادات الطويلة والمعقدة، يمكن للبنوك ابتكار أساليب وقنوات فعالة لإبلاغ العملاء وتوعيتهم بالاحتياطات التأمينية التي يجب اتخاذها من جانبهم, ويمكن للبنك الاستفادة من العديد من الأساليب - كالمواقع الإلكترونية للبنك، ووسائل التواصل الاجتماعي المعتمدة، والرسائل المطبوعة والإلكترونية لكشوف حسابات العملاء، والمنشورات الترويجية، وكذلك في الأحوال التي يتواصل فيها عادة موظفي المكاتب الأمامية للبنك أو مُقدم الخدمة مع العملاء - للتأكيد على ضرورة الالتزام ببعض التدابير الاحتياطية الأساسية.



٩. إجراءات الحصول على التراخيص

٩-١ يجب على البنوك التي ترغب في الحصول على تراخيص العمل كبنك مصدر (Issuer Bank) من خلال شبكة المدفوعات اللحظية أن تتقدم بطلب للحصول على موافقة البنك المركزي المصري، وذلك مع استيفاء ما يلي:

٩-١-١ الالتزام بإنهاء كافة الاختبارات والإجراءات الخاصة بشبكة المدفوعات اللحظية وفقاً لخطة عمل لا تتجاوز ٦ أشهر اعتبارا من تاريخه.

٩-١-٢ تقديم خطة عمل لمدة ثلاث سنوات تتضمن التالي:

- عدد الحسابات والبطاقات الخاصة بالعملاء المستهدف إتاحتها لشبكة المدفوعات اللحظية.
- عدد وقيم المعاملات السنوية المستهدف تنفيذها.
- تقديم خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها على أن يوضح بالخطة الميزانية المعتمدة لذلك.

٩-٢ يجب على البنوك التي ترغب في الحصول على تراخيص العمل كبنك مقدم خدمات الدفع (PSP Bank) من خلال شبكة المدفوعات اللحظية أن تتقدم بطلب للحصول على موافقة البنك المركزي المصري وذلك مع استيفاء ما يلي:

٩-٢-١ في حال طلب ترخيص مقدم خدمات دفع من خلال قنوات البنك الإلكترونية (Pre-authorized PSP Bank) :

- الالتزام بإنهاء كافة الاختبارات والإجراءات الخاصة بشبكة المدفوعات اللحظية.
- القنوات الإلكترونية التي سيتم إتاحتها لتنفيذ المعاملات على سبيل المثال لا الحصر (الإنترنت البنكي –تطبيق الهاتف المحمول البنكي).
- تقديم خطة عمل لمدة ثلاث سنوات تتضمن ما يلي:
  - عدد وقيم المعاملات السنوية المستهدف تنفيذها.
  - تقديم خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها على ان يوضح بالخطة الميزانية المعتمدة لذلك.

٩-٢-٢ في حال تقديم البنك تطبيق هاتف محمول خاص به لجميع عملاء شبكة المدفوعات اللحظية (Full Fledge PSP Bank):

- بيان يوضح اسم التطبيق والفئات المستهدفة به.
- إسم الشركة الراغبة في الحصول على ترخيص مقدم خدمات دفع (PSP) من خلال شبكة المدفوعات اللحظية.
- سجل تجاري ساري وبطاقة ضريبية سارية للشركة الراغبة في الحصول على الترخيص.
- قيام البنك بإخضاع مالكي الشركة والقائمين على إدارتها لإجراءات العناية

- الواجبة بعملاء البنوك وجمع أي معلومات يري ضرورة الحصول عليها بشأنهم.
- قيام البنك بالتحقق من عدم تعرض أي من مالكي الجهة والقائمين على إدارتها لعقوبات تتعلق بجنايات أو عقوبات على جرائم مخلة بالشرف أو الأمانة.
- تضمين شروط التعاقد مع الجهة ضرورة توافر نظم وإجراءات لديها تشترط توافر مستويات مرتفعة من الكفاءة والنزاهة لدى العاملين بها وبالمنافذ التابعة لها، على أن تتضمن هذه النظم والاجراءات كحد أدنى الاستفسار عن العمل السابق والحصول على صحيفة الحالة الجنائية.
- الالتزام بإنهاء كافة الاختبارات والإجراءات الخاصة بشبكة المدفوعات اللحظية.
- قائمة بأنواع الخدمات التي سوف يقوم مقدم الخدمة بتقديمها.
- خطوات العمل التفصيلية التي سيتم اتباعها لكل خدمة على حدة.
- تقديم خطة عمل لتفعيل الخدمة مدتها ثلاث سنوات تتضمن التالي:
  - عدد وقيم المعاملات الشهرية والسنوية المستهدف تنفيذها.
  - خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها على ان يوضح بالخطة الميزانية المعتمدة لذلك.
  - نموذج التسعير الخاص بالخدمة.

٩-٣ يجب على البنوك التي ترغب في الحصول على تراخيص العمل كبنك قابل (Acquirer Bank) من خلال شبكة المدفوعات اللحظية أن تتقدم بطلب للحصول على موافقة البنك المركزي المصري وذلك باستيفاء المستندات التالية كحد أدنى:

٩-٣-١ بيان يوضح ما إذا كان نشر القبول لدي التجار سوف يتم من خلال البنك مباشرة أو من خلال مقدم خدمات دفع (PSP) متعاقد مع البنك.

٩-٣-٢ بيان يوضح الفئات المستهدفة من خلال البنك او مقدمي خدمات الدفع (PSPs).

٩-٣-٣ الالتزام بإنهاء كافة الاختبارات والإجراءات الخاصة بشبكة المدفوعات اللحظية.

٩-٣-٤ قائمة بأنواع الخدمات التي سوف يقوم مقدم الخدمة بتقديمها.

٩-٣-٥ خطوات العمل التفصيلية التي سيتم اتباعها لكل خدمة على حدة.

٩-٣-٦ بيان يوضح قنوات التوزيع التي يرغب البنك أو مقدم خدمات الدفع (PSP) في الحصول على ترخيص لها فعلي سبيل المثال لا الحصر (القبول الإلكتروني من خلال رمز الاستجابة السريع (QR Code) – القبول الإلكتروني من خلال تطبيقات هاتف محمول خاصة بالتجار – القبول الإلكتروني من خلال نقاط البيع – القبول الإلكتروني من خلال الشراء عبر الأنترنت).

٩-٣-٧ تقديم خطة عمل لتفعيل الخدمة مدتها ثلاث سنوات تتضمن التالي:

- خطة البنك لعدد التجار المستهدف التعاقد معهم.
- عدد وقيم معاملات الشراء المستهدف قبولها من خلال جميع قنوات التوزيع على شبكة المدفوعات اللحظية.
- خطة تسويقية شاملة للتعريف بالخدمة وتفعيل استخدامها على أن يوضح بالخطة الميزانية المعتمدة لذلك.

٩-٤ في حال تعاقد البنك مع مقدم الخدمات التكنولوجية (Technology Service Provider) يلتزم البنك بتقديم نفس البيانات الخاصة السابق ذكرها فيما يخص التعاقد مع الشركات مقدمة خدمات الدفع (PSPs).


< Back
Money Received
Check your Balance

البنك المركزي المصري
CENTRAL BANK OF EGYPT

الفرع الرئيسي

العنوان:

٥٤ شارع الجمهورية ١١٥١١, القاهرة, مصر

الموقع الإلكتروني:

www.cbe.org.eg

البريد الإلكتروني:

info@cbe.org.eg

التليفون:

١٦٧٧٧