القاهرة في:

السيد الأستاذ/

رئيس مجلس الإدارة

بنك

تحية طيبة وبعد،

بالإشارة إلي الاهتمام الذي يوليه البنك المركزي المصري لدعم وتحفيز استخدام وسائل وقنوات الدفع الإلكترونية بهدف التحول إلي اقتصاد أقل اعتماداً علي أوراق النقد وتحقيق الشمول المالي، أود الإحاطة بأن مجلس إدارة البنـك المركزي المصري قد وافق بجلسته المنعقدة في ٢٩ نوفمبر ٢٠١٦ على الإصدار الجديد من **القواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول** (مرفق) التي تسري علي كافة البنوك التي تقدم أو ترغب في تقديم خدمات الدفع باستخدام الهاتف المحمول، علما بأنها تحل محل القواعد السابق إصدارها في فبراير ٢٠١٠ وتعديلاتها.

وجدير بالذكر أن إصدار **القواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول** قد تزامن مع إصدار وحدة مكافحة غسل الأموال وتمويل الإرهاب **إجراءات العناية الواجبة بعملاء خدمات الدفع باستخدام الهاتف المحمول** (مرفق) ليمثلا معاً حزمة من التعليمات الرقابية المتكاملة التي تهدف إلي التوسع في استخدام خدمات الدفع من خلال الهاتف المحمول وإلي تحقيق المزيد من التقدم نحو مجتمع مالياً أكثر شمولاً.

برجاء التفضل بالإحاطة والتنبيه بإتخاذ ما يلزم بشأن الالتزام بالقواعد والإجراءات المشار إليها.

وتفضلوا بقبول فائق الاحترام،،،

طارق عامر

المرفقات

- عدد (١٠) نسخ من كلٍ من القواعد والإجراءات.
- صورة من كتاب وحدة مكافحة غسل الأموال وتمويل الارهاب الخاص بإصدار إجراءات العناية الواجبة بعملاء خدمات الدفع باستخدام الهاتف المحمول.

البنك المركزي المصري

القواعد المنظمة لتقديم
خدمات الدفع باستخدام الهاتف المحمول

إصدار نوفمبر ٢٠١٦

البنك المركزي المصري

القواعد المنظمة لتقديم
خدمات الدفع باستخدام الهاتف المحمول

إصدار نوفمبر ٢٠١٦

المحتويات

١- مقدمة

١-١ الغرض

تستهدف خدمات الدفع من خلال الهاتف المحمول تحقيق الشمول المالي، والوصول بالخدمات المصرفية لكل أفراد المجتمع بمن فيهم غير القادرين والشباب والقاطنين بالأماكن النائية، وتعمل تلك الخدمات على توفير حساب مصرفي بسيط يفتح المجال لتوسيع قاعدة المتعاملين مع البنوك.

ونظراً لزيادة توجه الخدمات المصرفية في مصر نحو الاعتماد على التكنولوجيا فإن ذلك يتطلب المزيد من الإصلاحات التنظيمية اللازمة في هذا المجال.

١-٢ نطاق القواعد

- بالرغم من تشابه المخاطر والضوابط بين مختلف قنوات التواصل الخاصة بالخدمات المصرفية إلا أن هذه القواعد تختص بخدمات الدفع باستخدام الهاتف المحمول فقط.
- لا يغطي نطاق القواعد خدمات الدفع باستخدام قنوات التنفيذ الأخرى (مثال: ماكينات الصراف الآلي ATM، والخدمات المصرفية عبر الهاتف الأرضي، والخدمات المصرفية عبر الإنترنت Internet/Mobile Banking)، وقد تم إصدار القواعد التفصيلية المنظمة لبعض هذه الخدمات وسيتم إصدار الباقي تباعاً بشكل مستقل.
- تعتبر هذه القواعد والضوابط هي الحد الأدنى اللازم لتقديم خدمات الدفع باستخدام الهاتف المحمول بطريقة آمنة، وعلى كافة البنوك ألا تكتفى بذلك وأن تتأكد من اتخاذ كافة ما يلزم نحو إدارة المخاطر المرتبطة بتقديم هذا النوع من الخدمات المصرفية.
- تتضمن هذه القواعد بعض الضوابط أو الأهداف الرقابية العامة المتعلقة باستمرارية الأعمال وإسناد الأعمال إلى أطراف خارجية وإدارة مخاطر نظم المعلومات، وبالرغم من ذلك سيتم إصدار القواعد التفصيلية المنظمة لهذه المجالات بشكل مستقل لاحقاً.
- تسرى هذه القواعد فيما يتعلق بتقديم خدمات الدفع باستخدام الهاتف المحمول 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 خدمة الدفع باستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الارهاب.

تسري القواعد على جميع البنوك المسجلة لدى البنك المركزي المصري بما فيها فروع البنوك الأجنبية وتحل محل" قواعد تشغيل أوامر الدفع عن طريق الهاتف المحمول" الصادرة بتاريخ ٢ فبراير لعام ٢٠١٠ وتعديلاتها.

١-٣ الملاحق

- ملحق (أ): الحالات والقواعد الخاصة بالاستعانة بمقدمي الخدمة للتعرف على هوية العملاء كما وردت في "إجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول" الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب لعام ٢٠١٦
- ملحق (ب): التعريفات

٢- إدارة مخاطر خدمات الدفع باستخدام الهاتف المحمول

٢-١ المخاطر المرتبطة بخدمات الدفع باستخدام الهاتف المحمول

يقترن تقديم خدمات الدفع باستخدام الهاتف المحمول بالعديد من المخاطر والمميزات في نفس الوقت. وبينما لا تعتبر تلك المخاطر جديدة على البنوك إلا أن خصائص خدمات الدفع باستخدام الهاتف المحمول قد تزيد من درجات المخاطر بالإضافة إلى خلق تحديات جديدة لإدارة تلك المخاطر. وتتمثل هذه المخاطر فيما يلي وذلك على سبيل المثال لا الحصر:

- **المخاطر الاستراتيجية:**

تتمثل في قرار تقديم خدمات الدفع باستخدام الهاتف المحمول 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 التخطيط لخدمات الدفع باستخدام الهاتف المحمول والقرارات الاستثمارية غير المدروسة يمكنها أن تزيد المخاطر الاستراتيجية التي تتعرض لها البنوك.

- **مخاطر التشغيل/ مخاطر المعاملات:**

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

- **مخاطر الالتزام/ المخاطر القانونية:**

تنشأ هذه المخاطر نتيجة انتشار خدمات الدفع باستخدام الهاتف المحمول والاختلاف بين العمليات الإلكترونية والعمليات اليدوية. وقد تتضمن التحديات التنظيمية/القانونية الخاصة ما يلي:

- إبرام اتفاقية قانونية إلكترونياً مع العملاء لاستخدام خدمات الدفع باستخدام الهاتف المحمول.
- الأساليب التي تستخدمها البنوك للتعرف على هوية العملاء والتحقق منها باعتبارها أحد مصادر المخاطر القانونية التي ينبغي وضع ضوابط كافية للحد منها.
- في ضوء التزام البنوك بقانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣، يتعين على البنوك وضع إجراءات وضوابط للحفاظ على خصوصية البيانات وسرية حسابات العملاء للتمكن من إدارة المخاطر المتزايدة التي تتعلق بتقديم خدمات الدفع باستخدام الهاتف المحمول، وكذلك مسئولية البنوك القانونية تجاه العملاء نتيجة لاحتمال حدوث اختراق لخصوصية البيانات، أو أي مشاكل أخرى بسبب عمليات القرصنة أو الاحتيال أو الإخفاقات التكنولوجية الأخرى والعمل على حماية تلك البيانات من الاستيلاء عليها.
- تتحمل البنوك التي تقدم خدمات الدفع باستخدام الهاتف المحمول درجة أعلى من مخاطر الالتزام وذلك بسبب الطبيعة المتغيرة للتكنولوجيا والتعديلات الرقابية التي تهدف إلى التعامل مع المشاكل الخاصة بتقديم هذا النوع من الخدمات.
- الاحتفاظ بمستندات الالتزام المطلوبة والخاصة بالسجلات والتطبيقات وكشوف الحسابات والافصاحات والإشعارات.
- تحديد وتقييم مخاطر غسل الأموال وتمويل الإرهاب التي قد تنشأ عن خدمات الدفع باستخدام الهاتف المحمول، حيث يجب الانتهاء من هذا التقييم قبل إطلاق خدمات الدفع باستخدام الهاتف المحمول، وفي حالة أن الخدمة قائمة بالفعل لدى البنك، فالأمر يتطلب إعادة إجراء هذا التقييم فور صدور هذه القواعد وذلك في ضوء المتطلبات الرقابية الواردة بها وكذا ما يرد بإجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.

- **مخاطر السمعة:**

يتزايد مستوى المخاطر المتعلقة بالسمعة وذلك نتيجة قرار البنك بتقديم خدمات الدفع باستخدام الهاتف المحمول، وخاصةً فيما يتعلق بالمعاملات الأكثر تعقيداً. وفيما يلي بعض المخاطر التي قد تؤثر على سمعة البنك من خلال تقديم خدمات الدفع باستخدام الهاتف المحمول :

- انعدام الثقة نتيجة وجود معاملات غير مصرح بها على حساب مُستخدم النظام.
- الإفصاح عن معلومات سرية خاصة بمُستخدم النظام لأطراف غير مصرح لها، أو سرقتها.
- الفشل في تقديم خدمات يمكن الاعتماد عليها نتيجة لتكرار تعطل الخدمة أو طول مدة توقفها.
- شكاوى مُستخدم النظام من صعوبة استخدام خدمات الدفع باستخدام الهاتف المحمول أوعدم قدرة موظفي الدعم الفني بالبنك على حل هذه المشاكل.

- **مخاطر أمن المعلومات:**

ينشأ هذا النوع من المخاطر نتيجة احتمال استغلال إحدى الجهات غير المشروعة لنقاط الضعف بأنظمة خدمات الدفع باستخدام الهاتف المحمول لإحداث الضرر، والذى ينتج عنه آثار تتعلق بمستوى سلامة وإتاحة وسرية البيانات.

٢-٢ مسئوليات والتزامات مجلس الإدارة والإدارة العليا

٢-٢-١ يتولى مجلس الإدارة والإدارة العليا مسئولية الإشراف على إعداد استراتيجية العمل الخاصة بالبنك وكذا اتخاذ قرار استراتيجي واضح بشأن رغبة البنك في تقديم خدمات الدفع باستخدام الهاتف المحمول من عدمه، وبصفة خاصة يجب على مجلس الإدارة التأكد مما يلي:

- توافق خطط خدمات الدفع باستخدام الهاتف المحمول مع الأهداف الاستراتيجية للبنك.
- تحليل المخاطر الخاصة بخدمات الدفع باستخدام الهاتف المحمول المقترحة.
- إعداد إجراءات مناسبة لمراقبة المخاطر والحد منها وذلك فيما يتعلق بالمخاطر التي يتم تحديدها.
- المراجعة المستمرة لتقييم نتائج خدمات الدفع باستخدام الهاتف المحمول وفقا للخطط والأهداف المحددة.

٢-٢-٢ يجب على مجلس الإدارة والإدارة العليا ضمان تحليل المخاطر المرتبطة بخدمات الدفع باستخدام الهاتف المحمول المشار إليها في البند (٢-١) والحد منها بالطرق الملائمة، وذلك وفقا لما يلى:

٢-٢-٢-١ وضع رقابة فعالة على المخاطر المرتبطة بتقديم خدمات الدفع باستخدام الهاتف المحمول، بما في ذلك تحديد المسئوليات والسياسات والضوابط الرقابية لإدارة هذه المخاطر:

- يجب على مجلس الإدارة والإدارة العليا الإلمام بجوانب عمليات الدفع باستخدام الهاتف المحمول، والتي قد تفرض تحديات تختلف عن إدارة المخاطر التقليدية على النحو الوارد في البند ٢-١.
- يجب على مجلس الإدارة والإدارة العليا التأكد من عدم تقديم البنك خدمات جديدة للدفع باستخدام الهاتف المحمول أو تبنى وسائل تكنولوجية جديدة إلا إذا توافرت لهذا البنك الخبرات اللازمة التي تمكن من إدارة المخاطر بكفاءة. وينبغي ان تتناسب خبرات الموظفين والإدارة مع الطبيعة الفنية ودرجة تعقيد التطبيقات والتقنيات الخاصة بخدمات الدفع باستخدام الهاتف المحمول.
- يجب على مجلس الإدارة والإدارة العليا تحديد درجة قدرة البنك على تقبل المخاطر Risk Appetite وذلك فيما يتعلق بخدمات الدفع باستخدام الهاتف المحمول 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 الدفع باستخدام الهاتف المحمول.
- يجب على إدارة المراجعة الداخلية أن تقدم لمجلس الإدارة ولجنة المراجعة والإدارة العليا تقييم مستقل وموضوعي عن مدى فعالية الضوابط الرقابية التي يتم تطبيقها للحد من المخاطر الناتجة عن تقديم خدمات الدفع باستخدام الهاتف المحمول بما في ذلك مخاطر التكنولوجيا.

٢-٢-٢-٢ مراجعة واعتماد الجوانب الرئيسية لعملية الرقابة الأمنية الخاصة بالبنك:

- يجب على مجلس الإدارة والإدارة العليا الإشراف على التطوير والصيانة المستمرة للبنية التحتية للرقابة الأمنية التي توفر الحماية المناسبة لنظم وبيانات خدمات الدفع باستخدام الهاتف المحمول من أي تهديدات داخلية أو خارجية. ومن أجل ضمان فعالية عملية تأمين خدمات الدفع باستخدام الهاتف المحمول، يجب على مجلس الإدارة والإدارة العليا التأكد من اتخاذ الإجراءات الآتية:
  - تحديد مسئوليات واضحة خاصة بالإشراف على وضع وإدارة السياسات الأمنية الخاصة بالبنك.
  - 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 بخدمات الدفع باستخدام الهاتف المحمول.
  - توفير الضوابط الإلكترونية اللازمة والتي من شأنها منع أي أطراف داخلية أو خارجية غير مصرح لها من الوصول إلى التطبيقات وقواعد البيانات الخاصة بخدمات الدفع باستخدام الهاتف المحمول.
  - المراجعة الدورية لعمليات اختبار الإجراءات والنظم الأمنية - على سبيل المثال إجراء اختبار الاختراق دوريًا كما هو موضح في البند (٣-١١) - 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.

٢-٢-٣ إعداد آلية شاملة ومستمرة لإجراء الأبحاث النافية للجهالة Due Diligence والرقابة على عمليات التعهيد وعلاقات البنك بأطراف خارجية أخرى يتم الاعتماد عليهم لتقديم خدمات الدفع باستخدام الهاتف المحمول. مع تركيز مجلس الإدارة والإدارة العليا على النقاط التالية على سبيل المثال لا الحصر:

- الإلمام الكامل بالمخاطر المترتبة على إبرام أي ترتيبات خاصة بالإسناد أو الشراكة أو الوكالة فيما يتعلق بنظم أو تطبيقات خدمات الدفع باستخدام الهاتف المحمول بالإضافة إلى توفير الموارد اللازمة للإشراف على هذه الترتيبات.
- إجراء الأبحاث النافية للجهالة اللازمة فيما يتعلق بالكفاءة والبنية التحتية للنظام والقدرة المالية للشريك أو الطرف الخارجي مُقدم الخدمة وذلك قبل إبرام أي اتفاقيات خاصة بالإسناد أو الشراكة أو الوكالة.
- تحديد المسئوليات التعاقدية لكافة الأطراف الخاصة باتفاقيات الإسناد أو الشراكة أو الوكالة بشكل واضح. على سبيل المثال، يتم تحديد مسئوليات توفير المعلومات إلى مُقدِّم الخدمة وتلقيها منه بشكل واضح.
- 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 والمسئوليات والوقت المطلوب لتنفيذ الخدمة وإجراءات وبيانات التصعيد والعقوبات في حال عدم الالتزام، هذا بالإضافة إلى البنود التي تحفظ حق البنك في التدقيق على موردي الخدمات أو الاعتماد على تقارير التدقيق المعتمدة (الصادرة عن جهات تدقيق معتمدة).
- خضوع كافة النظم والعمليات الخاصة بخدمات الدفع باستخدام الهاتف المحمول التي تتم من خلال عملية الإسناد أو الوكالة لنظام إدارة المخاطر وسياسات الخصوصية وأمن المعلومات التي تتفق مع المعايير الخاصة بالبنك.
- 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.
- توفير كافة تقارير التدقيق والتقييم لمفتشي قطاع الرقابة والإشراف بالبنك المركزي المصري.
- وضع خطط طوارئ مناسبة لخدمات الدفع باستخدام الهاتف المحمول التي تتم عن طريق الإسناد أو الوكالة.
- أن تتسم إجراءات فسخ/إنهاء التعاقد بالفاعلية، كما يجب أن تضمن هذه الإجراءات الحفاظ على استمرارية العمل وسلامة البيانات وكذلك نقلها والتخلص منها.
- وبالرغم من قيام البنك بإسناد بعض الخدمات لأطراف خارجية، فإن البنك يظل مسئولاً مسئولية كاملة تجاه مستخدمي النظام وتجاه التزام الأطراف الخارجية بهذه القواعد.

وفقًا لما ورد في البند ١-٢، سيتم إصدار قواعد تفصيلية منظمة تَحكُم أنشطة الإسناد وذلك على نحو منفصل، على أن تشمل الضوابط الرقابية التفصيلية بالإضافة إلى الأهداف الرقابية وكذلك قائمة بالنظم والخدمات المسموح بإسنادها والاستعانة بمصادر خارجية لتنفيذها. ولحين إصدار هذه القواعد، يجب على البنوك عدم إبرام أي اتفاقيات تتعلق بإسناد خدمات الدفع باستخدام الهاتف المحمول أو تطبيقاتها دون الحصول على موافقة مسبقة من البنك المركزي المصري.

٢-٣ إعداد سياسة تأمين المعلومات

٢-٣-١ يجب على الإدارة العليا التأكد من أن سياسة أمن المعلومات المُطبَّقة بالبنك - والمُعتمدة من مجلس الإدارة ويتم تحديثها بشكل دوري - تغطي خدمات الدفع باستخدام الهاتف المحمول. ويسهم ذلك في تحديد السياسات والإجراءات والضوابط الرقابية اللازمة لحماية العمليات البنكية من الاختراقات والانتهاكات الأمنية، كما يحدد المسئوليات الفردية وكذا يوضح آليات التنفيذ والإجراءات التي يجب اتخاذها في حال مخالفة هذه السياسات والإجراءات.

٢-٣-٢ 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.

٢-٤ تصنيف مخاطر خدمات الدفع باستخدام الهاتف المحمول

تقدم البنوك مجموعة مختلفة من خدمات الدفع باستخدام الهاتف المحمول لفئات متنوعة من العملاء ونتيجة لذلك فهي لا تنطوي عادةً على ذات مستوي المخاطر المتأصلة.

ويتطلب هذا التنوع في تقديم الخدمات تبنى البنوك لأساليب أمنية شاملة وتتسم بالمرونة في الوقت ذاته، على أن تكون منهجية التأمين قائمة على تحليل المخاطر والتهديدات الخاصة بخدمات الدفع باستخدام الهاتف المحمول، 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 بالبنك.

٢-٥ قواعد مكافحة غسل الأموال وتمويل الإرهاب

يجب على البنوك التي تقوم بتقديم خدمات الدفع باستخدام الهاتف المحمول تنفيذ ما يلي:

- الالتزام بقانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢ ولائحته التنفيذية والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري، وكذا إجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.
- إيلاء عناية كافية لما يتفق مع طبيعة الخدمة من المؤشرات الإسترشادية الواردة بالبند السابع (المؤشرات الإسترشادية 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 عام ٢٠٠٨.
- في حالة الاشتباه في أية عمليات تتم من خلال تطبيقات الهاتف المحمول، القيام بإخطار وحدة مكافحة غسل الأموال وتمويل الإرهاب بشأنها، وذلك وفقا لأحكام قانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢.

٣- الضوابط الرقابية على خدمات الدفع باستخدام الهاتف المحمول

٣-١ إصدار النقود الإلكترونية وإدارة النظام

٣-١-١ يقتصر حق إصدار وحدات النقود الإلكترونية على البنوك الخاضعة لرقابة البنك المركزي المصري وذلك بعد الحصول على موافقته.

٣-١-٢ يُعِد البنك مُصدر وحدات النقود الإلكترونية ويُشَغِل نظاماً لإدارة سجلات النقود الإلكترونية بشكل كامل ودقيق ومستمر وتوضح هذه السجلات قيمة النقود المُصدرة ومُستخدمي النظام ومُقدمي الخدمة وبيان رصيد الحسابات الخاصة بكل منهم وإجمالي هذه الأرصدة. ويراقب هذا النظام حركة أوامر الدفع الخاصة بوحدات النقود الإلكترونية وإصدار تقارير مُفصلة Audit Trail عن أوامر الدفع، مع ربط العمليات بمُستخدمي النظام ومُقدمي الخدمة. ويمثل عجز النظام عن إصدار تقارير صحيحة - سواء بشكل متعمد أو غير متعمد - إخلالاً بهذه القواعد.

٣-١-٣ يتم استبدال وحدات النقود الإلكترونية بذات قيمة النقد (الجنيه المصري) المقابلة لها وبدون دفع عائد لمُستخدم النظام/مُقدم الخدمة باستثناء مقابل أداء الخدمة المنصوص عليه في العقد بين البنك ومُستخدم النظام أو مُقدم الخدمة.

٣-١-٤ لا يتم إصدار وحدات نقود إلكترونية إلا إذا كان البنك يحتفظ لديه بإيداعات نقدية (بالجنيه المصري) لا تقل قيمتها عن قيمة الوحدات المُصدرة، ويراقب البنك المركزي المصري من خلال التفتيش على البنك المرخص له مدى الالتزام بهذه القاعدة والتأكد من أن قيمة الوحدات المُصدَرة بمعرفة البنك المُصدِر لا تزيد عن الإيداعات النقدية بالجنيه المصري المحتفظ بها لديه لهذا الغرض.

٣-١-٥ يجب ألا يتعدى الحد الأقصى من وحدات النقود الإلكترونية المُصدرة القدر المُصرح به من البنك المركزي المصري لكل بنك وهو ٥% من رأس المال المدفوع للبنك أو ٥٠ مليون جنيه مصري أيهما أقل، ولمحافظ البنك المركزي المصري أن يُعدِل الحد الأقصى لوحدات النقود الإلكترونية المُصدرة لكل بنك.

٣-٢ الاستعانة بمقدم الخدمة

٣-٢-١ يحق للبنك الاستعانة بمُقدمي خدمة للوصول إلى مُستخدمي النظام وتقديم خدمات تخص هذا النظام بعد موافقة البنك المركزي المصري مع مراعاة كافة ما جاء بالبند ٣-٢-٢-٢، ويتم الاتفاق بين البنك ومُقدم الخدمة على العمليات التي يقوم بها مُقدم الخدمة، على ألا تتعدى العمليات الآتية:

٣-٢-١-١ في حالة أن مقدم الخدمة ضمن الجهات الواردة بالبند (٣) من إجراءات العناية الواجبة بعملاء خدمة الدفع بإستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب:

- التعرف على هوية طالب استخدام النظام والتحقق منها وفقا للإجراءات الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب في هذا الشأن.
- استلام وتسجيل نماذج طلبات فتح الحسابات أو أية طلبات أخرى خاصة بالخدمة.
- تقديم التوعية والمعلومات الإرشادية لاستخدام النظام.
- الحصول على نقد (جنيه مصري) من مستخدمي النظام في حدود رصيد مقدم الخدمة من وحدات نقود إلكترونية بالبنك.
- تسليم نقد (جنيه مصري) لمُستخدم النظام مقابل استلام وحدات نقود إلكترونية منه.

٣-٢-١-٢ في حالة أن مقدم الخدمة جهة أخرى بخلاف الجهات الواردة بالبند (٣):

- تقديم التوعية والمعلومات الإرشادية لاستخدام النظام.
- الحصول على نقد (جنيه مصري) من مُستخدمي النظام في حدود رصيد مُقدم الخدمة من وحدات نقود إلكترونية بالبنك.
- تسليم نقد (جنيه مصري) لمُستخدم النظام مقابل استلام وحدات نقود إلكترونية منه.

٣-٢-٢ يجب أن يتمتع مُقدم الخدمة بوضع مالي جيد ويكون حسن السمعة.

٣-٢-٣ يقوم مقدم الخدمة بفتح حساب جاري دائن لدى البنك.

٣-٢-٤ يقتصر حجم وحدات النقود الإلكترونية الممنوحة لمُقدم الخدمة على مقدار ما أودعه نقدا (جنيه مصري) أو ضمانات لدي البنك ليقوم بتحويلها إلي مُستخدمي النظام مقابل متحصلات نقدية منهم، ولا يجوز لمُقدم الخدمة تلقي أموال من مُستخدمي النظام دون تحويل وحدات نقود إلكترونية لهم ولا يجوز له استلام وحدات النقود الإلكترونية منهم دون تسليمهم نقد (جنيه مصري).

٣-٢-٥ يلتزم مقدم الخدمة بإرسال مستندات التعرف على هوية طالب فتح الحساب للبنك وفقا لما تنص عليه إجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب.

٣-٢-٦ يُعِد مقدم الخدمة مكانا مناسبا لإجراء المعاملات المالية المتعلقة بالنظام.

٣-٢-٧ يلتزم مُقدم الخدمة بتوفير سيولة نقديه لتغطية عمليات السحب النقدي المتوقعة.

٣-٢-٨ يكون البنك مسئولاً مسئولية كاملة تجاه مُستخدمي النظام وتجاه التزام مُقدمي الخدمة بتنفيذ هذه القواعد وكذا الأحكام والضوابط والقواعد والإجراءات الصادرة في شأن مكافحة غسل الأموال وتمويل الإرهاب.

٣-٢-٩ لا يحق لمُقدم الخدمة إسناد تنفيذ تعاقده مع البنك إلى آخرين، ولا يحق له حوالة تعاقده مع البنك أو التنازل عنه لصالح آخرين، ويتم النص على ذلك صراحة في التعاقد بين البنك ومُقدم الخدمة.

٣-٣ إدارة حسابات خدمات الدفع باستخدام الهاتف المحمول

٣-٣-١ يلتزم البنك عند فتح حسابات الهاتف المحمول بالتعرف على هوية طالب استخدام النظام والتحقق منها وفقا "لإجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول" الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب، كما يلتزم بقانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢ ولائحته التنفيذية والضوابط الرقابية للبنوك في شأن مكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري.

٣-٣-٢ يلتزم البنك بتوثيق كافة البيانات الخاصة بمكان وتوقيت فتح حسابات الهاتف المحمول وكذا عمليات السحب والإيداع.

٣-٣-٣ تحتفظ البنوك بكافة الوثائق الخاصة بالنظام وذلك بطريقة حفظ آمنة وللمدد القانونية المقررة.

٣-٣-٤ يتم ربط كل رقم هاتف محمول بحساب هاتف محمول واحد فقط.

٣-٣-٥ يقتصر فتح حسابات الهاتف المحمول لمستخدمي النظام من الأشخاص الطبيعيين على الحاصلين على الجنسية المصرية فقط.

٣-٣-٦ يُسمح لمستخدم النظام بفتح أكثر من حساب للهاتف المحمول بحد أقصي ثلاثة حسابات على مستوي كافة البنوك التي تقدم الخدمة في مصر.

٣-٣-٧ تلتزم البنوك بتطبيق كافة الإجراءات والضوابط الرقابية التي تمكنها من تحديد هوية القائمين بأي معاملات إلكترونية مرتبطة بالحسابات المصرفية، وذلك في الحالات التي يصرح فيها لأكثر من مستخدم بالتعامل على هذا الحساب.

٣-٣-٨ تلتزم البنوك بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية.

٣-٣-٩ تلتزم البنوك بتطبيق الضوابط الخاصة بالتشغيل البيني المشار إليها بالبند ٣-٧.

٣-٣-١٠ يتم فتح حساب دون عائد لكل مُستخدم للنظام أو مُقدم خدمة للتعامل عليه من خلال النظام - يسمي حساب هاتف محمُول - ويكون البنك مسئولاً عن إدارة هذا الحساب، ويودع به وحدات نقود إلكترونية بمقدار ما أودعه مُستخدم النظام أو مُقدم الخدمة من نقد - جنيه مصري - لدى البنك لتغذية حساب الهاتف المحمُول.

٣-٣-١١ تلتزم البنوك بالتأكد بصفة دورية من حيازة صاحب حساب الهاتف المحمول لنفس رقم الهاتف المحمول المُسجل على النظام.

٣-٣-١٢ يقوم البنك ومقدم الخدمة بتطبيق أحكام الحفاظ على سرية الحسابات وفقا لما يقتضيه قانون البنك المركزي والجهاز المصرفي والنقد الصادر بالقانون رقم ٨٨ لسنة ٢٠٠٣ وتعديلاته.

٣-٣-١٣ لا يجوز منح مُستخدم النظام أو مُقدم الخدمة أي ائتمان بأي شكل من الأشكال مقابل وحدات النقود الإلكترونية.

٣-٣-١٤ تلتزم البنوك باستخدام أساليب يمكن الاعتماد عليها للتحقق من هوية المودع في حالة تغذية حساب الهاتف المحمول.

٣-٣-١٥ تلتزم البنوك باستخدام أساليب يمكن الاعتماد عليها للتحقق من هوية وصلاحيات العملاء الراغبين في الاشتراك في خدمات الدفع باستخدام الهاتف المحمول.

٣-٣-١٦ تلتزم البنوك بإجراء عمليات التدقيق اللازمة للتأكد من هوية مُستخدم النظام عند طلبه إجراء تعديل في بيانات حساب خدمات الدفع باستخدام الهاتف المحمول الخاص به، أو تعديل أي بيانات يستخدمها مُستخدم النظام لمتابعة أنشطة حساب الهاتف المحمول. ويطبق ذلك على عمليات إعادة تفعيل الحساب وإعادة إصدار كلمة سر جديدة لمُستخدم نظام خدمات الدفع باستخدام الهاتف المحمول وتغيير بيانات الاتصال الخاصة به مثل عنوان البريد الإلكتروني ورقم الهاتف الأرضي وعنوان المراسلات. كما يجب على البنوك أن تأخذ في الاعتبار تطبيق المعايير التالية عند التعامل مع تلك الطلبات:

- في حال تقدم مُستخدم النظام بطلب لتعديل البيانات الخاصة به في أحد الفروع أو لدى أحد منافذ مقدم الخدمة، يتم تطبيق الإجراءات اللازمة للتأكد من هويته.
- أما في حال طلبات التعديل المقدمة من خلال أنظمة الدفع عن طريق الهاتف المحمول فيجب استخدام وسائل التصديق الموضحة بالبند ٣-٤-٥-١ مع التأكد من وجود آليات مراقبة فعالة.
- تطبيق البنوك الإجراءات اللازمة للتحقق من هوية مُستخدم النظام في حالة تسليمه معلومات أو أدوات أو أجهزة تتيح له الدخول على حساب الدفع عن طريق الهاتف المحمول الخاص به (مثال: الرقم السري PIN وأجهزة رموز الأمان Tokens..إلخ).
- في حال عدم توافر معايير مماثلة لتلك الموضحة أعلاه، تتجنب البنوك إرسال المستندات أو الأدوات المهمة (مثال: أجهزة رموز الأمان البديلة ..إلخ) إلى العملاء الذين قاموا بتغيير عناوين مراسلاتهم حديثاً على وجه الخصوص. ويلتزم مُستخدم النظام في هذه الحالة باستلام هذه المستندات أو الأدوات بنفسه من أحد فروع البنك بعد التحقق من هويته طبقا للقواعد المعمول بها.
- إجراء عمليات التحقق والفحص الإضافية للتأكد من هوية مُستخدم النظام، وذلك فيما يتعلق بالطلبات التي تتم من خلال الهاتف - المكالمات التي ترد من العملاء فقط - لإرسال أجهزة رموز الأمان الجديدة أو أي مستندات هامة أخرى وكمثال لعملية التحقق الإضافية: سؤال مُستخدم النظام عن معلومات تتغير من وقت لآخر بالإضافة إلى الأسئلة المتعلقة بالتفاصيل الشخصية بصفة عامة (مثال: الأرصدة التقريبية في الحساب وآخر معاملات تم تنفيذها على الحساب).

٣-٣-١٧ يراعى عند إغلاق الحساب، أو إنهاء التعاقد الخاص برقم هاتف محمول، وضع الإجراءات المناسبة التي تكفل سحب وحدات النقود الإلكترونية الموجودة بحساب الهاتف المحمول والتأكد من شخصية الساحب وتوثيق إغلاق الحساب.

٣-٤ وسائل إثبات الهوية (التصديق)

٣-٤-١ تلتزم البنوك باستخدام وسائل فعَّالة يمكن الاعتماد عليها لإثبات هوية العملاء المستخدمين لخدمات الدفع باستخدام الهاتف المحمول. وعادةً ما تكون عملية التصديق أكثر فاعلية عند الجمع بين اثنين من العناصر التالية:

- أحد الأشياء المعروفة للعميل (مثال: اسم المستخدم وكلمة السر).
- أحد الأشياء التي بحوزة مُستخدم النظام (مثال: التوقيع الرقمي أو كلمات السر المستخدمة لمرة واحدة التي تصدر باستخدام أجهزة رموز الأمان).
- أحد السمات المميزة والخاصة بمُستخدم النظام (مثال: الصفات البيومترية، كالبصمات).

٣-٤-٢ يجب على البنوك تحديد وسائل التصديق التي ستستخدمها لخدمات الدفع باستخدام الهاتف المحمول وذلك بناءاً على تحليل المخاطر المرتبطة بالنظام، مع الأخذ في الاعتبار تقييم نوعية المعاملات المصرفية التي تقدم عبر خدمات الدفع باستخدام الهاتف المحمول.

٣-٤-٣ تحتاج البنوك إلى عمل تقييم دقيق لتحديد ما إذا كانت الوسيلة المستخدمة للتصديق مناسبة من الناحية الأمنية حتى إذا كان الهاتف المحمول الخاص بمُستخدم النظام عرضة للتهديدات، مثال: سرقة/ضياع الهاتف المحمول أوعن طريق برامج خبيثة وبرامج التجسس عن طريق تسجيل الضغط على لوحة المفاتيح.

٣-٤-٤ في حالة الدخول إلى نظام الدفع من خلال التطبيق على الهاتف المحمول وحيث لا يمكن التحقق من رقم الهاتف، يجب أن يشمل التحقق من هوية الدخول من خلال رمز إشاري غير قابل للتكرار- قد يكون رقم الهاتف نفسه - ورقم التعريف الشخصي PIN الذي يجب أن تتوافر به مواصفات الرقم السري PIN المذكورة في البند ٣-٥-٢. وفي حالة تصنيف الخدمات المتاحة للعميل كخدمات ذات مخاطر مرتفعة يجب إستبدال رقم التعريف الشخصي PIN بكلمة سرية معقدة على النحو المذكور في البند رقم ٣-٥-٣.

٣-٤-٥ يجب على البنوك إعادة التصديق عند إجراء عمليات الدفع على النحو التالي:

٣-٤-٥-١ في حالة تنفيذ الأنشطة ذات المخاطر المرتفعة (يشمل ذلك على سبيل المثال لا الحصر: أوامر الدفع الخاصة بتحويل الأموال لأكثر من مستفيد في المرة الواحدة، أوامر الدفع المستثناة من الحد الأقصى للتحويل، تغيير بيانات الاتصال بمُستخدم النظام ..إلخ) وحيث لا يُسمح بتنفيذ الأنشطة ذات المخاطر المرتفعة إلا من خلال تطبيق إلكتروني، يجب استخدام وسيلتين معاً (مثال: كلمات السر المستخدمة لمرة واحدة التي تصدر باستخدام أجهزة/تطبيقات رموز الأمان على النحو المذكور في البند رقم ٣-٥-٤ مع عدم السماح بمنح كلمات السر المستخدمة بشكل آلي ومباشر عبر الرسائل النصية القصيرة أو البريد الإلكتروني للعملاء من الأفراد والأشخاص الاعتبارية ..إلخ).

حيث يجب أن تعمل وسيلة التصديق المُستخدمة بالتزامن مع الضوابط الأخرى المُطبَّقة على تعزيز الأبعاد التالية:

- عدم الإنكار
- سلامة وتكامل البيانات
- سرية البيانات
- صحة الهوية

٣-٤-٥-٢ في حالة تنفيذ المعاملات التي لا تُصنف كمعاملات ذات مخاطر مرتفعة يجب إعادة التصديق على المعاملات بإدخال رقم التعريف الشخصي PIN. ويطبق ذلك أيضاً على خدمات الدفع ببروتوكول USSD.يجب على البنوك إنشاء آلية للتحقق من التصديق على النحو التالي:

- منع دخول المستخدم إلى خدمات الدفع باستخدام الهاتف المحمول بعد عدد محدد من المحاولات الفاشلة - يحدده البنك - ويجب على البنك إعداد إجراءات واضحة لإعادة تفعيل حساب المستخدم الذي تم إيقافه.
- عدم إعطاء أي معلومات بعد المحاولات الفاشلة للدخول على النظام إلى الشخص الذى قام بتلك المحاولات مثل الإفصاح عن عدم وجود اسم هذا المستخدم أو أن كلمة السر غير صحيحة.
- القيام بالرقابة بصورة منتظمة لمحاولات الدخول الفاشلة لخدمات الدفع باستخدام الهاتف المحمول، وعند اكتشاف أي تجاوز جسيم، يجب التحقيق فيه وتحديد التهديدات المحتملة واتخاذ التدابير اللازمة.

٣-٥ إدارة كلمة السر

٣-٥-١ يجب على البنوك مراعاة التدابير الرقابية التالية عند التعامل مع كلمات السر الخاصة بالعملاء وإتباع مواصفات كلمات السر الموضحة أدناه.

- تطبيق الرقابة المزدوجة و/أو الفصل بين المهام لعملية إنشاء كلمات السر وتسليمها للعملاء وعملية تفعيل حسابات خدمات الدفع باستخدام الهاتف المحمول.
- يجب على البنوك استخدام التكنولوجيا المناسبة لإنشاء كلمات السر. كما يجب استخدام آلية تشفير قوية أو أن يكون طول مفتاح التشفير مناسب.
- تعزيز تأمين عملية إنشاء كلمة السر لضمان عدم تعرضها للكشف.
- التأكد من أن كلمات السر لا يتم معالجتها أو إرسالها أو تخزينها كنص واضح، وألا يظهر الرقم السري بشكل مقروُء على أي جزء من الشبكة أو نظم الحاسب التي تُدير النظام وذلك في أية مرحلة من العملية.
- تطبيق الوسائل اللازمة للحفاظ على سرية كلمات السر في حالة تسليمها للعميل إما باليد أو إلكترونياً.
- وجوب توجيه مستخدمي ومديري أنظمة الدفع عن طريق الهاتف المحمول لتغيير كلمة السر الصادرة فور الدخول إلى النظام لأول مرة.
- الحفاظ على تاريخ كلمات السر المستخدمة والتأكد من عدم إعادة استخدامها مرة أخرى خلال عدد مرات أو مدة زمنية يحددها البنك.
- يجب أن يكون هناك حد أقصى للمحاولات الغير ناجحة لإدخال الرقم السري - لا تتجاوز خمس محاولات - قبل إيقاف حساب المستخدم.
- يجب على البنوك وضع إجراءات واضحة لما يلي:
  - إعداد الأرقام السرية الأولية.
  - إعادة تفعيل حساب المستخدم الموقوف.
- تطبيق قواعد انتهاء صلاحية كلمة السر على أساس مدة صلاحية محددة مسبقا من قبل البنك.

٣-٥-٢ الحد الأدنى لمواصفات الرقم السري PIN:

- يجب أن لا يقل الرقم السرى عن ستة أرقام كحد أدنى (ويفضل ثمانية أرقام).
- لا ينبغي السماح بالأرقام السهلة كرقم سرى PIN مثال: ١١١١١١ أو ١٢٣٤٥٦.

٣-٥-٣ مواصفات كلمة السر لتطبيقات الدفع على الهاتف المحمول:

- أن تكون كلمات سر معقدة (مثال: تتكون من ثمانية أحرف وتتضمن حروف وأرقام ورموز خاصة ..إلخ).
- التأكد من أن آلية "تذكر كلمة السر" لا يمكن استخدامها (أي لا يتم السماح بتخزين كلمة السر على تطبيقات الهاتف المحمول).

٣-٥-٤ كلمات السر المستخدمة لمرة واحدة التي تصدر باستخدام أجهزة/تطبيقات رموز الأمان:

- يجب على البنوك مراعاة الحد الأدنى لمواصفات كلمة السر لمرة واحدة والتي يتم استخدامها لإجراء المعاملات ذات المخاطر المرتفعة - طبقاً لتقييم البنك كما هو موضح بالبندين (٣-٤-٢) و(٣-٤-٥-١) - على أن تكون كما يلي:
  - يجب ألا تكون كلمة السر أقل من ٦ رموز.
  - يجب ألا يزيد الوقت الزمنى لصلاحية استخدام كلمة السر عن ٩٠ ثانية.
  - التأكد من أن نظام الحلول الحسابية Algorithm لإنشاء كلمة السر يوفر العشوائية الكافية من القيم الرمزية.

- يجب أن يتم حماية جهاز/تطبيق رموز الأمان برقم سري PIN طبقاً لما يلي:
  - يجب أن يكون الحد الأدنى لمواصفات كلمة السر PIN على النحو الوارد بالبند ٣-٥-٢.
  - يجب أن يكون هناك حد أقصى للمحاولات الغير ناجحة لإدخال الرقم السري - لا تتجاوز خمس محاولات - قبل إيقاف جهاز/تطبيق رموز الأمان.
  - يجب على البنوك وضع إجراءات واضحة لإعادة تفعيل أجهزة/تطبيقات رموز الأمان الموقوفة.

٣-٦ الضوابط الخاصة بعمليات تحويل الأموال

٣-٦-١ باستثناء ما تم ذكره بالبند ٣-٦-١٠، تتم عمليات التحويل داخل جمهورية مصر العربية فقط وبالعملة المحلية (الجنيه المصري) فقط ولا يسُمح بتبادل عملات أخرى أو إجراء عمليات تبادل للعملات أو مقاصة بين حسابات العملاء ذات العملات الأخرى دون الرجوع إلى البنك المركزي المصري للحصول على موافقة تشمل ضوابط التحويل.

٣-٦-٢ تقتصر عمليات تحويل الأموال على الحالات الآتية:

٣-٦-٢-١ بين حسابات الهواتف المحمولة المختلفة.
٣-٦-٢-٢ بين حساب الهاتف المحمول الخاص بمُقدم الخدمة وحسابه المصرفي لدى نفس البنك.
٣-٦-٢-٣ بين حساب الهاتف المحمول الخاص بمستخدم النظام وحسابه المصرفي لدى نفس البنك.

٣-٦-٣ يجب أن يتيح النظام تحويل الأموال إلى أنظمة دفع هاتف محمول أخرى مشابهة، وسيقوم البنك المرسل بتحويل الأموال من الحسابات الخاصة بهذا النظام إلي الحسابات المُشابهة في الأنظمة الأخرى وفقا للضوابط الخاصة بالتشغيل البيني بالبند ٣-٧.

٣-٦-٤ يجب على البنوك التي تقدم خدمة تحويل الأموال من حسابات عملائها إلى حسابات أطراف أخرى من خلال خدمات الدفع عن طريق الهاتف المحمول، وضع الضوابط المناسبة التي تساعد على تقليل المخاطر المصاحبة لتلك الخدمة لتصل إلى مستوى مقبول ومعتمد من البنك.

٣-٦-٥ يجب على البنوك تطبيق مبدأ الرقابة المزدوجة على الأقل - المعد/المدقق والمصرح - على تحويلات أموال الأشخاص الاعتبارية لمستفيدين آخرين – إلا في حالة طلب الشركة أو الشخص الاعتباري غير ذلك كتابياً - مع ضرورة استخدام كل من المعد/المدقق والمصرح لوسائل إثبات الهوية - التصديق - الواردة بالبند ٣-٤.

٣-٦-٦ يتعين على البنك في ضوء تقييمه للمخاطر المرتبطة بالخدمة وبمستخدم النظام وضع حدود قصوى للرصيد وقيمة وعدد كل من العمليات اليومية والشهرية التي تتم على حساب الهاتف المحمول طبقا لما يلي:

٣-٦-٦-١ لا يتجاوز الحد الأقصى اليومي للسحب والتحويل وأي عمليات خصم من الحساب مبلغ ٦٠٠٠ (ستة آلاف) جنيهاً مصرياً.
٣-٦-٦-٢ لا يتجاوز الحد الأقصى الشهري للسحب والتحويل وأي عمليات خصم من حساب الهاتف المحمول الخاص بمستخدمي النظام من الأشخاص الطبيعيين مبلغ ٥٠,٠٠٠ (خمسون ألف) جنيها مصرياً ومن الأشخاص الاعتباريين مبلغ ١٠٠,٠٠٠ (مائة ألف) جنيها مصرياً.
٣-٦-٦-٣ لا يتجاوز الحد الأقصى لرصيد الحساب مبلغ ١٠,٠٠٠ (عشرة آلاف) جنيها مصرياً، والحد الأقصى لإجمالي أرصدة الحسابات الخاصة بعميل واحد بالبنك مبلغ ١٠,٠٠٠ (عشرة آلاف) جنيهاً مصرياً.

ولمحافظ البنك المركزي المصري أن يعدل تلك الحدود القصوى.

٣-٦-٧ يستثنى من الخضوع للحدود المذكورة بالبند ٣-٦-٦ مستخدمي النظام الذين خضعوا لإجراءات التعرف والتحقق من هويتهم بموجب قواعد التعرف على هوية العملاء بالبنوك الصادرة عن وحدة مكافحة غسل الأموال وتمويل الارهاب عام ٢٠١١ وتعديلاتها على أن يلتزم البنك بما يلي:

٣-٦-٧-١ تقييم المخاطر المرتبطة بالخدمة وبمستخدم النظام ووضع حدود قصوى للرصيد وقيمة وعدد كل من العمليات اليومية والشهرية التي تتم على حساب الهاتف المحمول.
٣-٦-٧-٢ في ضوء تقييم البنك للمخاطر المتعلقة بالخدمة يتعين على البنك النظر في مدي ملائمة اعتبار الخدمة ذات مخاطر مرتفعة وتطبيق إجراءات العناية المشددة تجاه مستخدم النظام والتعاملات الخاصة به.
٣-٦-٧-٣ الأخذ في الاعتبار بوسائل التصديق المذكورة بالبند ٣-٤-٥-١.
٣-٦-٧-٤ التأكد من عدم تركز النقود الإلكترونية في عدد محدود من العملاء.
٣-٦-٧-٥ يتم إيلاء عناية خاصة للعميل، بما يشمل مراقبة التحويلات المتعلقة به بشكل منتظم، والتأكد من عدم وجود أي شبهة تتعلق بغسل الأموال أو تمويل الإرهاب أو أية جريمة.

٣-٦-٧-٦ الحصول على إقرار كتابي من المفوض بالتوقيع عن الشخص الاعتباري بأن التحويلات من وإلى هذه الحسابات مرتبطة بعلاقة عمل أو علاقة تعاقدية مع بيان طبيعة هذه العلاقة.

٣-٦-٨ يجب على البنوك إخطار عملائها من مستخدمي خدمات الدفع عن طريق الهاتف المحمول بأي معاملات مالية أو أنشطة ذات مخاطر مرتفعة تتم على حساباتهم – إلا في حالة طلب مُستخدم النظام غير ذلك – وذلك من خلال وسيلة مميكنة بديلة (مثل الرسائل النصية القصيرة أو رسائل البريد الإلكتروني).

٣-٦-٩ لا يتم إنشاء أمر الدفع من خلال رسائل SMS ويتاح استخدام هذه الرسائل للتأكيد على إتمام عملية الدفع.

٣-٦-١٠ يسمح لمستخدمي النظام بتلقي التحويلات من الخارج بالعملات الأجنبية وإضافتها إلى حساب الهاتف المحمول بالجنيه المصري وفقاً للضوابط الآتية:

٣-٦-١٠-١ تقتصر هذه الخدمة على العملاء من الأشخاص الطبيعيين.

٣-٦-١٠-٢ يتم إيلاء عناية خاصة لمراقبة التحويلات الواردة إلى العملاء بشكل منتظم، والتأكد من عدم وجود أي شبهة تتعلق بغسل الأموال أو تمويل الإرهاب أو أية جريمة.

٣-٦-١٠-٣ يقوم البنك بتحديد الحد الأقصى للتحويل من الخارج طبقا لتقييم المخاطر والقواعد المقررة لذلك على أن يلتزم بما ورد بالبند ٣-٦-٦ و٣-٦-٧.

٣-٦-١٠-٤ يتخذ البنك الإجراءات المناسبة للتأكد من أن التحويل يخص ذات مُستخدم النظام وأن القيمة قد تم إضافتها بالجنيه المصري لحساب الهاتف المحمول الخاص به.

٣-٦-١٠-٥ يتعين ألا يتم إضافة قيم التحويلات الواردة من الخارج إلى حساب الهاتف المحمول قبل فحص هذه التحويلات للقيام بما يلي:

- تحديد التحويلات التي لا تتضمن الحد الأدنى من المعلومات المشار إليها بإجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول، والتعامل بشأنها وفقاً لما ورد في هذا الشأن بإجراءات العناية الواجبة المذكورة.
- التحقق من عدم إدراج طرفي التحويل بالقوائم السلبية المحلية والدولية وأية قوائم أخرى يرى البنك ضرورة الرجوع إليها.

٣-٧ الضوابط الخاصة بالتشغيل البيني Interoperability

٣-٧-١ يقوم المحول القومي بإتاحة خدمات تحويل الأموال بين أنظمة دفع الهاتف المحمول المختلفة.

٣-٧-٢ تقوم شركة بنوك مصر للتقدم التكنولوجي بدور المحول القومي.

٣-٧-٣ تتم التحويلات بين حسابات الهاتف المحمول لحظياً على أن تتم التسويات بين البنوك طبقا للقواعد التي تصدر من المحول القومي.

٣-٧-٤ تلتزم البنوك الحاصلة على ترخيص لتقديم خدمات الدفع باستخدام الهاتف المحمول بما يلي:

٣-٧-٤-١ الربط مع المحول القومي طبقا للبند ٣-٧-٥-٢ على أن يتم استخدام رسائل قياسية معتمدة في الإرسال والاستقبال.

٣-٧-٤-٢ الالتزام بقواعد التشغيل التي تصدر عن المحول القومي والمُعتمدة من البنك المركزي المصري.

٣-٧-٤-٣ إمداد المحول القومي ببيانات مستخدمي النظام الحاليين والجدد طبقا لما هو منصوص عليه بقواعد التشغيل المعتمدة المذكورة بالبند ٣-٧-٥-١ ويعتبر ذلك شرط رئيسي لإتمام عملية تسجيل مستخدمي النظام لدى المحول القومي.

٣-٧-٤-٤ إمداد المحول القومي بشكل لحظي بكل البيانات اللازمة لإجراء تحويل أوامر الدفع ما بين البنوك.

٣-٧-٤-٥ إبلاغ المحول القومي بإلغاء تسجيل أي من مستخدمي النظام لديه حيث يعتبر شرط رئيسي لإتمام عملية الإلغاء.

٣-٧-٥ يلتزم المحول القومي بكافة ما يحدده البنك المركزي المصري من ضوابط ومتطلبات بحد أدني ما يلى:

٣-٧-٥-١ إصدار قواعد التشغيل بما لا يتعارض مع البند ٣-٧ واعتمادها من البنك المركزي المصري في موعد أقصاه شهرين من تاريخ إصدار "القواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول".

٣-٧-٥-٢ اعتماد رسوم مقابل الخدمة من البنك المركزي المصري.

٣-٧-٥-٣ التحويل والمقاصة للعمليات الخاصة بحسابات الهاتف المحمول بين البنوك.

٣-٧-٥-٤ إصدار قواعد لحل المنازعات علماً بأن سجلات المحول القومي هي حجة قاطعة بشرط عدم حدوث خلل في النظام وبشرط وجود سجلات كاملة للمعاملات محل المنازعة.

٣-٧-٥-٥ توفير البيان الخاص بإسم المستفيد إلى البنك المُصدر للتحويل عند طلبه وذلك لأغراض مكافحة غسل الأموال وتمويل الإرهاب.

٣-٧-٥-٦ التأكد من ربط كل رقم هاتف محمول واحد لحساب هاتف محمول واحد.

٣-٧-٥-٧ التأكد من عدم تجاوز عدد حسابات الهاتف المحمول المتعلقة بمستخدم النظام لأكثر من ثلاثة حسابات على مستوى كافة البنوك المقدمة للخدمة.

٣-٧-٥-٨ تطبيق أحكام الحفاظ على سرية الحسابات وفقا لما يقتضيه قانون البنك المركزي والجهاز المصرفي والنقد الصادر بالقانون رقم ٨٨ لسنة ٢٠٠٣ وتعديلاته.

٣-٧-٥-٩ توفير خدمات التشغيل البيني لخدمات الدفع باستخدام الهاتف المحمول بين البنوك على مدار الساعة، مع ضمان أداء الخدمة للبنوك طبقاً لقواعد التشغيل الخاصة بالمحول القومي والمعتمدة من البنك المركزي المصري.

٣-٧-٥-١٠ التأكد من وجود سجلات لكافة الحسابات والمعاملات الخاصة بخدمات التشغيل البيني التي تتم عبر أنظمة المحول القومي. كما يجب ضمان حماية تلك السجلات ضد أي تلاعب أو تغيير غير مُصرَّح به، وأن يتم الاحتفاظ بها لمدة زمنية تتوافق مع ما تحدده سياسات المحول القومي تطبيقاً للمتطلبات القانونية وطبقاً للضوابط والتعليمات الرقابية الصادرة في هذا الشأن.

٣-٧-٥-١١ وضع الخطط المناسبة لضمان استمرارية العمل على أن يتم مراعاة الممارسات التالية:

- في حال حدوث عطل في الخدمة، يجب أن تحتوي خطة استمرارية العمل على خطوات محددة لكيفية استئناف أو استرجاع خدمات الدفع عن طريق الهاتف المحمول، تحدد هذه الخطوات بناء على أهداف وقت ونقطة الاسترجاع RTO & RPO المحددة بقواعد التشغيل الخاصة بالمحول القومي والمعتمدة من البنك المركزي المصري.
- يتم إبلاغ البنك المركزي المصري في حاله وجود أي أعطال تتخطي أوقات ونقطة الاسترجاع المشار إليها بقواعد التشغيل.

٣-٧-٥-١٢ تطبيق إجراءات أمن المعلومات الواردة بالقواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول والصادرة عن البنك المركزي المصري أو أية قواعد مستقبلية تخص حوكمة نظم المعلومات بالإضافة إلي إتباع المعايير القياسية وأفضل الممارسات المطبقة في هذا الشأن.

٣-٧-٥-١٣ إرسال الملفات الخاصة بعمليات حسابات الهاتف المحمول للتسوية على حسابات البنوك لدي البنك المركزي المصري.

٣-٧-٥-١٤ إتاحة خدمات الربط مع أنظمة دفع قومية أخرى بعد أخذ موافقة البنك المركزي المصري.

٣-٧-٥-١٥ موافاة البنك المركزي المصري بكافة التقارير المتعلقة بخدمة الدفع من خلال الهاتف المحمول بالطريقة التي يحددها البنك

٣-٧-٥-١٦ لا يحق لشركة بنوك مصر أن تقوم بتعهيد (اسناد) أي من التزاماتها أو مهامها الخاصة بالتشغيل البيني إلا بالموافقة الكتابية من البنك المركزي المصري.

كما يلتزم المحول القومي بأي ضوابط أو تعديلات تصدر عن البنك المركزي المصري في ما يخص "القواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول" والضوابط الخاصة بالتشغيل البيني.

٣-٨ سرية وسلامة المعلومات

٣-٨-١ يتضمن تقديم خدمات الدفع باستخدام الهاتف المحمول تداول بيانات سرية - مثل كلمات السر الخاصة بخدمات الدفع باستخدام الهاتف المحمول والمعاملات المالية ..إلخ - عبر تطبيقات الهاتف المحمول والشبكة الداخلية للبنك. لذلك يجب على البنوك استخدام الأساليب المناسبة للحفاظ على سرية وسلامة المعلومات المتداولة عبر الشبكات الداخلية والخارجية للبنك.

٣-٨-٢ يتم استخدام تكنولوجيا التشفير لحماية سرية وسلامة المعلومات التي تتسم بالحساسية. حيث 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.

٣-٨-٣ يجب على البنوك أيضاً تنفيذ ضوابط أخرى بخلاف أساليب التشفير، وذلك للحفاظ على سرية وسلامة المعلومات التي يتم تداولها عبر نظم خدمات الدفع باستخدام الهاتف المحمول. ويتضمن هذا على سبيل المثال:

٣-٨-٣-١ الضوابط وأعمال التدقيق المدرجة بتطبيقات خدمات الدفع باستخدام الهاتف المحمول للتأكد من سلامة تسوية أرصدة العملاء بعد تنفيذ المعاملات بالإضافة إلى التأكد من سلامة البيانات التي يتم نقلها بين الأنظمة المختلفة.

٣-٨-٣-٢ مراقبة المعاملات غير المعتادة بما في ذلك المعاملات محل الاشتباه الخاصة بخدمات الدفع باستخدام الهاتف المحمول أو السجلات التي يشتبه التلاعب فيها، كما هو موضح في البند ٤-٢.

٣-٨-٤ يجب على البنوك تشفير العملية بداية من الهاتف المحمول المُستخدم لإجراء العملية وصولاً إلى أجهزة الخادم Servers الخاصة بتنفيذ أمر الدفع.

٣-٨-٥ 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 كما يلي:

٣-٨-٥-١ عدم السماح لموظف واحد فقط بالقيام بإنشاء حساب مستخدم لخدمات الدفع باستخدام الهاتف المحمول والتصريح بالموافقة عليه وإلغائه دون مشاركة موظفين آخرين بالبنك للتحقق من سلامة تصرفات هذا الموظف.

٣-٨-٥-٢ يجب على البنك تصميم الإجراءات الخاصة بتعاملات الدفع باستخدام الهاتف المحمول بما يضمن عدم انفراد أحد الأشخاص بإنشاء التعاملات والموافقة عليها وتنفيذها على النظام مما قد يدعم عملية احتيال أو إخفاء تفاصيل خاصة بتلك المعاملات.

٣-٨-٦ يجب أن تنفذ جميع عمليات التحقق من الصلاحيات المتاحة للمستخدم Authorization Checks وكذلك القواعد المنظمة لعمليات التحويل على جانب الخادم، أي في النظم الخلفية بالبنك، قبل إتمام العملية المطلوبة (مثال: تنفيذ عمليات التحويل بشكل عكسي بسبب عدم التحقق من صلاحيات المستخدم والتي قد تُمكن مُستخدم النظام من إضافة الأموال إلى حساب هاتفه المحمول بدلاً من الخصم عليه).

٣-٩ تأمين التطبيقات

يجب على البنوك التأكد من توفير مستوى مناسب من تأمين التطبيقات الخاصة بخدمات الدفع باستخدام الهاتف المحمول مع أخذ الممارسات السليمة التالية بعين الاعتبار:

٣-٩-١ يجب على البنوك عند اختيار أدوات تطوير النظام أو لغات البرمجة من أجل تطوير التطبيقات الخاصة بخدمات الدفع باستخدام الهاتف المحمول أن تقيم الخصائص الأمنية التي يمكن أن توفرها الأدوات أو اللغات المختلفة لضمان إمكانية تنفيذ الحماية الفعالة للتطبيقات.

٣-٩-٢ يجب إجراء عملية تحقق شاملة وفعالة حول صحة المدخلات - بما في ذلك البيانات المدخلة من قبل المستخدم والاستعلام من خلال قواعد البيانات التي قد يقوم المستخدم بطلب تنفيذها - وذلك من خلال خوادم الشبكة، ويمنع هذا نظام الدفع باستخدام الهاتف المحمول من معالجة المعطيات غير الصحيحة التي يتم إدخالها بطريقة متعمدة، الأمر الذي قد يؤدى إلى الوصول غير المصرح به إلى البيانـات، أو تنفيذ الأوامـر الواردة في هذه المعطيات، أو حدوث هجمات تؤدى إلى تجاوز سعة الذاكرة.

٣-٩-٣ يجب أن تعمل أنظمة خدمات الدفع باستخدام الهاتف المحمول بأقل الصلاحيات الممكنة الخاصة بإدارة النظام. كذلك يجب منع استخدام كلمات السر المعروفة أو كلمات السر الموحدة التي تعد مع نشأة النظام.

٣-٩-٤ يجب ألا تكشف رسائل الأخطاء التي تصدر من النظام لعملاء خدمات الدفع باستخدام الهاتف المحمول عن معلومات دقيقة خاصة بالنظام ويجب تسجيل الأخطاء بشكل مناسب.

٣-٩-٥ يجب على البنوك اتخاذ الإجراءات اللازمة لعلاج أي نقاط ضعف بنظام الدفع باستخدام الهاتف المحمول يتم اكتشافها، وذلك استناداً إلى الإجراءات الأمنية المتبعة في البنك.

٣-٩-٦ في حال إطلاق البنك لإصدار جديد لتطبيق الدفع باستخدام الهاتف المحمول Mobile Application يتعلق بأمن وسرية المعلومات فيجب على البنك اتخاذ الاجراءات التي تلزم العميل بتحميل الإصدار الجديد قبل استخدام التطبيق.

٣-٩-٧ يجب على البنوك عمل الترتيبات الأمنية المناسبة لبعض الخدمات التي تتضمن اتصالات مع الشبكات العامة - كخدمات البريد الإلكتروني للتواصل مع عملاء خدمات الدفع باستخدام الهاتف المحمول - لتجنب الهجمات على أنظمة/تطبيقات خدمات الدفع باستخدام الهاتف المحمول من خلال هذه الخدمات.

٣-٩-٨ على البنك أن يقوم بتأمين عملية تشفير شاملة على مستوى طبقة التطبيقات Application Layer للبيانات المرسلة عبر الهاتف المحمول، حتى لا يتم كشف الأرقام السرية وكلمات السر الخاصة بمُستخدم النظام في أي مرحلة وسيطة لتداول البيانات بين التطبيقات وخادم الاستضافة Host، حيث يتم التحقق من أرقام التعريف الشخصية PIN وكلمات السر.

٣-٩-٩ يجب على البنوك القيام بالاختبارات اللازمة للتأكد من عدم إمكانية تجاوز عملية التصديق أو إغفالها للدخول على النظام/التطبيق.

٣-٩-١٠ عندما يتم نشر تطبيق الدفع عن طريق الهاتف المحمول على مخازن البرامج Applications Stores، يجب نشرها من خلال الحساب الرسمي للبنك مع العلامة التجارية المناسبة. ويمكن إتاحة الرابط الخاص بتحميل التطبيق من مخازن البرامج وذلك على الموقع الإلكتروني الخاص بالبنك. كما يجب على البنوك إجراء البحث عن تطبيقات الهواتف المحمولة المزيفة الموجودة في متاجر ومواقع توزيع التطبيقات من أجل الحد من مخاطر البرمجيات الخبيثة Malware التي تستخدم للحصول على بيانات مُستخدم النظام الخاصة بالدخول على خدمات الدفع باستخدام الهاتف المحمول.

٣-٩-١١ يجب التأكد من توفير ضوابط أمنية كافية عند استخدام مكونات/أجزاء تطبيقات جاهزة مقدمة من طرف ثالث Third Party Library لبناء تطبيق الدفع باستخدام الهاتف المحمول.

٣-٩-١٢ يجب ألا تعرض تطبيقات الدفع باستخدام الهاتف المحمول أي خدمة لتطبيق طرف ثالث يعمل على نفس الجهاز أو قادم من أي مصدر خارجي آخر باستثناء الأنظمة الخلفية للبنك.

٣-٩-١٣ نظراً لسهولة الوصول إلى قواعد البيانات ذات الحماية الضعيفة من خلال الشبكات الداخلية والخارجية، لذا يجب التشديد على توافر الآتي:

- إجراءات صارمة بشأن تحديد الهوية والصلاحيات للدخول على الأنظمة وقواعد البيانات.
- تصميم آمن وسليم لعمليات النظام System Processes.
- مسارات تدقيق ملائمة Audit Trails.

٣-٩-١٤ يجب الحد من تخزين بيانات على الذاكرة الداخلية للهاتف المحمول، وفى حالة الاحتفاظ بأي بيانات على الهاتف المحمول - للضرورة القصوى - يجب استخدام الوسائل المناسبة لحماية ما تم تخزينه.

٣-٩-١٥ يجب منع تطبيق الدفع باستخدام الهاتف المحمول من حفظ أو عرض اسم المستخدم أو كلمات السر السابق إدخالها من مُستخدم النظام.

٣-٩-١٦ يجب إنهاء تسجيل الدخول على تطبيقات الدفع باستخدام الهاتف المحمول تلقائياً بعد فترة من الوقت - يقوم البنك بتحديدها - في حال عدم وجود أي نشاط على النظام/التطبيق، إلا إذا تم إعادة تصديق بيانات مُستخدم النظام مرة أخرى، الأمر الذى يمنع أي مُخترق من الإبقاء على التطبيق مفتوح على الهاتف المحمول إلى أجل غير محدد.

٣-٩-١٧ يُوصى بأن يقوم تطبيق الدفع باستخدام الهاتف المحمول بتنفيذ آليات كشف كافية تضمن أن الهاتف المحمول ليس عرضة للمخاطر مثل Jailbroken/Rooted مثال: يقوم المخترق بتحميل برنامج على الجهاز المحمول يمكنه من الدخول إلى الملفات السرية الخاصة بالمستخدم.

٣-٩-١٨ يُوصى بأن يتم حماية التطبيق الخاص بالهواتف الذكية من الهندسة العكسية Reverse Engineering (مثال:Code Obfuscation).

٣-٩-١٩ يُوصى بأن يتم حماية تطبيقات الدفع باستخدام الهاتف المحمول ضد أي لقطات تلقائية Screenshots والتي يمكن أن تتم عن طريق برامج تجسس تعمل على نفس جهاز الهاتف المحمول.

٣-٩-٢٠ يجب أن تخضع أنظمة خدمات الدفع باستخدام الهاتف المحمول إلى اختبارات مُتعددة قبل التشغيل للتأكد من قدرتها على القيام بالمهام المُوكلة لها.

٣-١٠ البنية التحتية والمتابعة الأمنية لخدمات الدفع باستخدام الهاتف المحمول

٣-١٠-١ يجب على البنوك إنشاء بيئة تشغيل ملائمة تعمل على دعم وحماية أنظمتها الخاصة بخدمات الدفع باستخدام الهاتف المحمول، بحيث تحتوي تلك البيئة على بنية تحتية آمنة لخدمات الدفع باستخدام الهاتف المحمول - والتي تشمل على سبيل المثال لا الحصر إعداد خوادم الشبكة وأنظمة اكتشاف ومنع الاختراق وأجهزة جدار الحماية Firewall وأجهزه التوجيه وخلافه - كما تحتوى أيضا على إجراءات حماية ملائمة للشبكات الداخلية وروابط الشبكات مع الجهات الخارجية.

٣-١٠-٢ تتم إدارة النظام تحت الإشراف والمسئولية الكاملة للبنوك حيث تقوم البنوك بتقديم الخدمة بمراعاة عناية الرجل الحريص، ويجب على البنوك مراقبة كل من أنظمة/تطبيقات الدفع باستخدام الهاتف المحمول 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.

٣-١٠-٣ يجب على البنوك التأكد من وجود مسارات التدقيق Audit Trails لكل المعاملات المصرفية التي تتم عبر أنظمة/تطبيقات الدفع باستخدام الهاتف المحمول على أنظمة البنك. 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 User ID على نظام الدفع باستخدام الهاتف المحمول.
- أي عملية ذات تبعات مالية.
- أي تصريح يمنح لعميل/ مستخدم لتجاوز أي من الحدود أو الصلاحيات.
- أي تعديل أو إضافة أو إلغاء لصلاحيات المستخدمين أو امتيازات خاصة بالدخول على الأنظمة.

٣-١٠-٤ 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.

٣-١٠-٥ يمكن للبنوك الرجوع إلى (الملحق أ) الخاص بالممارسات المتعلقة بتصميم وإنشاء ومراقبة البنية التحتية المنصوص عليه في القواعد المنظمة لتقديم الخدمات المصرفية عبر الإنترنت في القطاع المصرفي المصري الصادرة في نوفمبر ٢٠١٤.

٣-١٠-٦ 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.

٣-١١ تقييم النظام الأمني لخدمات الدفع باستخدام الهاتف المحمول

٣-١١-١ يجب على البنوك دورياً تقييم الوضع الأمني لكافة الأنظمة - التطبيقات، والشبكات، وأجهزة التأمين، وخوادم نظام أسماء النطاقات وخوادم البريد الإلكتروني، إلخ - المتعلقة بأعمال الدفع باستخدام الهاتف المحمول، وذلك في المركز الرئيسي للمعلومات والمركز الاحتياطي الذى يستخدم في حالات الكوارث. يوضح البندان ٣-١١-٢ و ٣-١١-٣ الحد الأدنى من أنشطة التقييم الواجب إجراؤها.

٣-١١-٢ يجب على البنوك إجراء تقييم دوري لنقاط الضعف Vulnerability Assessment كل ثلاثة أشهر على الأقل أو عند حدوث تغييراً جوهرياً في البيئة التشغيلية لنظام خدمات الدفع باستخدام الهاتف المحمول لاكتشاف نقاط الضعف في بيئة تكنولوجيا المعلومات، وتقييمها. ويمكن أن يتولى هذا التقييم مستشار أو مقدم خدمة خارجي، أو 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.

٣-١١-٣ 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 قبل البدء في تقديم أي خدمات حيوية جديدة، 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.
- يجب على مقدم الخدمة الخارجي إصدار تقرير نهائي موقع منه عن اختبار الاختراق لكى يقوم البنك بتقديمه إلى البنك المركزي المصري، بجانب التقرير المبدئي الأول.
- غير مسموح باختيار نفس مقدم الخدمة الخارجي لأداء أكثر من اختباري اختراق متتاليين.

٣-١١-٤ يجب أن يتضمن نطاق أنشطة التقييم الواردة بالبندين ٣-١١-٢ و٣-١١-٣ على تقييم كافة الإصدارات لتطبيق الدفع عن طريق الهاتف المحمول Mobile Application المتاحة لاستخدام عملاء البنك.

٣-١٢ الاستجابة للأحداث وإدارتها

٣-١٢-١ 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 في الأنظمة الخاصة بخدمات الدفع باستخدام الهاتف المحمول، 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 وحفظها بطريقة مناسبة وبأسلوب يضمن الرقابة على تلك الأدلة، لتسهيل التحقيقات اللاحقة وإقامة دعوى قضائية ضد مخترقي النظام والمشتبه فيهم إذا لزم الأمر بالإضافة إلى تنفيذ عملية مراجعة لهذا الحدث.

٣-١٢-٢ 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.

٣-١٢-٣ يجب على البنوك إعداد سجل بالأحداث العارضة المرتبطة بخدمات الدفع باستخدام الهاتف المحمول والتفاصيل الخاصة بها بالإضافة إلى إعداد تقرير دوري للعرض على الإدارة العليا لاتخاذ الإجراءات المناسبة لتلافي تكرارها.

٣-١٢-٤ يتولى مسئول الالتزام بالبنك مسئولية التأكد من إبلاغ البنك المركزي المصري بصورة صحيحة وفي الوقت المناسب، 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 بخدمات الدفع باستخدام الهاتف المحمول.
- أي عملية تخريبية للبيانات المتعلقة بأنظمة خدمات الدفع باستخدام الهاتف المحمول والتي لا يمكن استرجاعها.
- الإيقاف التام المتعمد أو العارض لخدمات الدفع باستخدام الهاتف المحمول لفترة تزيد عن الفترة المحددة كهدف لوقت الاسترجاع RTO المحدد من قبل البنك.
- أي حالة من حالات الاحتيال الداخلي ذات الصلة بخدمات الدفع باستخدام الهاتف المحمول.

على أن يتم إرسال هذه التقارير إلى البنك المركزي عن طريق إحدى قنوات الاتصال التالية:

- إرسالها بالفاكس إلى رقم : ٢٥٩٧٦٠٥٧ أو ٢٥٩٧٦٠٤٧ عناية قطاع الرقابة والإشراف – إدارة الرقابة المكتبية، أو
- إرسالها بالبريد الالكتروني على العنوان التالي cbe.infosec@cbe.org.eg

٣-١٢-٥ عند وقوع هجمات إلكترونية، يمكن أن يؤخذ في الاعتبار من ضمن التدابير التي يتبناها البنك التواصل مع فريق التدخل السريع لمكافحة الجرائم الإلكترونية EGYPTIAN-CERT التابع لوزارة الاتصالات.

٣-١٣ اعتبارات الأداء وضمان استمرارية العمل

٣-١٣-١ يجب على البنوك توفير خدمات الدفع باستخدام الهاتف المحمول 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.

٣-١٣-٢ يجب على البنوك وضع معايير لتقييم ومتابعة مستوى أداء تقديم خدمات الدفع باستخدام الهاتف المحمول. كما يجب اتخاذ التدابير اللازمة للتأكد من قدرة نظم خدمات الدفع باستخدام الهاتف المحمول والنظم الداخلية الخاصة بتقديم الخدمة على التعامل مع حجم العمليات المتوقعة والنمو المستقبلي لهذا النوع من الخدمات.

٣-١٣-٣ يجب أن تأخذ البنوك في اعتبارها التخطيط لضمان استمرارية العمل عند تطويرها لخدمات الدفع باستخدام الهاتف المحمول، 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 خدمات الدفع باستخدام الهاتف المحمول، تحدد هذه الخطوات بناء على أهداف وقت ونقطة الاسترجاع RTO & RPO المحددين مسبقاً.
- وجود نسخ احتياطية للبيانات لاستعادة البيانات ووجود خطط عمل بديلة للطوارئ.
- يجب أن تتمتع خطة استمرارية العمل الخاصة بخدمات الدفع باستخدام الهاتف المحمول بالقدرة على التعامل مع أي من الحالات التي يتم فيها الإسناد لأطراف خارجية لتقديم الخدمة (كمتعهدين لتقديم خدمات الدفع باستخدام الهاتف المحمول).

٤- أمن العملاء وضوابط لبعض المخاطر الأخرى

٤-١ عقد تقديم الخدمة / نموذج طلب الخدمة

يجب على البنوك أن تحدد بدقة كافة الحقوق والالتزامات بينها وبين عملائها ضمن عقد تقديم خدمات الدفع باستخدام الهاتف المحمول، ويجب استيفاء العقد للمتطلبات التالية:

- تتم صياغة العقد بصورة واضحة ومحددة بحيث يسهل فهمه بالنسبة لأي عميل مع تجنب استخدام الكلمات والعبارات التي تحمل أكثر من معنى.
- يوضح التزامات كل من البنك ومُستخدم النظام في حالة الإخلال بأي من شروط التعاقد.
- يحتوي العقد على بنود محددة واضحة والتي يجب أن تتضمن ما يلي كحد أدنى:
  - التأكيد على أوقات توفير الخدمة طبقا لتقييم البنك لهدف وقت الاسترجاع RTO الوارد في خطة استمرارية الأعمال، وينبغي إخطار العملاء في حالة انقطاع الخدمة لعمل صيانة محددة مسبقاً.
  - توضيح مستوى خصوصية بيانات العملاء ومدى إتاحتها للغير داخل البنك أو خارج البنك 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.
  - يقوم البنك بإيجاد آلية لدراسة الشكاوي ويُنص صراحة في عقد الاشتراك بالخدمة على طريقة تقديم الشكوى إلى البنك والحد الأقصى للوقت المُستغرق للتحقيق في الشكوى من قِبل البنك.
  - في حالة وجود منازعات على المعاملات المالية أو وجود شكاوى من قِبل مُستخدمي النظام، تخضع عمليات تسوية المنازعات إلى قواعد ثابتة ومُعلنة لمُستخدم النظام ويجب أن تكون هذه القواعد واردة في العقد بين مُستخدم النظام والبنك، علماً بأن سجلات النظام هي حجة قاطعة بشرط عدم حدوث خلل في النظام وبشرط وجود سجلات كاملة للمعاملات محل المنازعة.
  - 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 من خلال تطبيق الهاتف المحمول لأى تغيير في الشروط والأحكام الذى سيظهر من خلال النظام إلكترونيا يعتبر التزاماً قانونياً.
  - التأكيد على أن يكون الهاتف المحمول الخاص بمُستخدم النظام والمستخدم في عمليات الدفع عن طريق الهاتف المحمول غير مخترق Rooted/Jailbroken.
  - التأكيد بوضوح على أن القوانين المصرية ذات الصلة ولوائحها التنفيذية والتعليمات والقواعد الرقابية هي التي تحكم الخدمات التي يقوم البنك بتقديمها للعملاء عبر الهاتف المحمول ويتم تسوية النزاعات داخل جمهورية مصر العربية.
  - توضيح مسئوليات المُستخدم في الحفاظ على كلمة السر/الرقم السري الخاص به والإبلاغ عن فقد هاتفه المحمول فور فقده، ويجب نشر نسخة من نموذج العقد على الموقع الخاص بالبنك على شبكة الإنترنت.
  - توضيح مسئولية مستخدم النظام في إبلاغ البنك/مقدم الخدمة في حالة تخليه عن رقم الهاتف المحمول المُستخدم في إنشاء الحساب تمهيداً لإغلاق الحساب.
  - النص على حق مُستخدم النظام في استبدال وحدات النقود الإلكترونية بالنقد (جنيه مصري) في أي وقت وشروط الاستبدال، إن وجدت، وعلى أي مقابل لأداء الخدمة أو أية رسوم لإجراء عملية الاستبدال، إن وجدت، وإعلام مستخدم النظام بأي تغييرات تطرأ على مقابل الخدمة.
  - في حالة إنهاء عمل النظام من قِبل البنك أو في أي أحوال أخرى ينتج عنها توقف تقديم الخدمة لمستخدم النظام، يلتزم البنك بالوفاء بتعهداته قِبل مُستخدمي النظام بما في ذلك القيام باستبدال وحدات النقود الإلكترونية بالنقد (جنيه مصري) طبقا للشروط الواردة في العقد بين البنك ومُستخدم النظام وفي أسرع وقت ممكن.
- يجب أن يحصل البنك على توقيع يدوي من العميل على العقد الخاص بالخدمة، على أن يستثني من ذلك العملاء الذين قاموا مسبقاً بالموافقة كتابياً على قبول استخدام البنك للوسائل الإلكترونية للحصول على موافقة العميل على أي تغييرات في الشروط والأحكام الخاصة بالخدمات المصرفية على أن تشمل تلك الموافقة كافة قنوات تقديم الخدمات المصرفية وفي تلك الحالة يقوم العميل بالموافقة على الشروط والأحكام إلكترونياً.

٤-٢ رصد الأنشطة غير العادية

٤-٢-١ يتعين على البنوك وضع تدابير فعالة للرقابة المستمرة لضمان سرعة اكتشاف أي معاملات غير عادية عبر الهاتف المحمول 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 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 آخرين.
- تغيير عنوان مراسلات مُستخدم النظام، يتبعه بفترة وجيزة أنشطة قد تدل على وجود عمليات غير مشروعة محتملة مثل طلب إرسال بعض الوثائق الهامة - على سبيل المثال، طلب إرسال الرقم السري الخاص بالخدمة - على العنوان الجديد.

٤-٢-٢ يجب أن تتمتع آلية الرقابة المتبعة بالقدرة على سرعة إصدار تحذيرات إلى المختصين بالمتابعة والرصد لخدمات الدفع باستخدام الهاتف المحمول عند حدوث أي تحويل أموال محل شبهة احتيال، وكذلك أي أنشطة غير معتادة باستخدام الهاتف المحمول. 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.

٤-٢-٣ إخطار العملاء فوراً في حالة رصد أي أنشطة غير معتادة محل شبهة احتيال على حساباتهم.

٤-٢-٤ يجب على البنك تطبيق إجراءات محددة ومُعتمدة للتعامل مع حالات الاحتيال.

٤-٣ توعية مُستخدم النظام

٤-٣-١ نظراً لأن الأجهزة التي يستخدمها العملاء للدخول على خدمات الدفع باستخدام الهاتف المحمول 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 خدمات الدفع باستخدام الهاتف المحمول والتزامهم حيال ذلك.

٤-٣-٢ التأكيد على العملاء وتوعيتهم أن موظفي البنك - أو وكلاءه – 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.

٤-٣-٣ توعية عملاء خدمات الدفع باستخدام الهاتف المحمول بالطرق التي يمكنهم من خلالها التأكد من صحة التطبيق الرسمي للبنك.

٤-٣-٤ تختلف النصائح الخاصة بالاحتياطات الأمنية الواجب إتباعها وفقا لطبيعة العملاء، وطبيعة خدمات الدفع باستخدام الهاتف المحمول المقدمة، وتشمل النصائح ما يلى كحد أدنى:

٤-٣-٤-١ اختيار وحماية كلمات السر الخاصة بخدمات الدفع باستخدام الهاتف المحمول (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 أو جزء من اسم مُستخدم النظام يسهل التعرف عليها.

٤-٣-٤-٢ 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 لأى شخص بما في ذلك موظفي البنك أو وكلائه.

٤-٣-٥ يجب على البنوك مراجعة النصائح والإرشادات الخاصة بالاحتياطات التأمينية التي يتم تقديمها للعملاء للتأكد من كفايتها وملائمتها للتغيرات التي تستجد على البيئة التكنولوجية وخدمات الدفع باستخدام الهاتف المحمول.

٤-٣-٦ يتم إخطار عميل النظام بوسيلة التصرف في حالة اكتشاف أي شخص آخر للرقم السري الخاص بمُستخدم النظام.

٤-٣-٧ 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، والرسائل المطبوعة على كشوف 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.

٥- إجراءات الحصول على ترخيص لتقديم الخدمة

٥-١ يجب على البنوك التي ترغب في تقديم خدمات الدفع باستخدام الهاتف المحمول لعملائها أو البنوك التي حصلت على ترخيص بعد إصدار القواعد وتود أن تضيف وظائف جديدة أن تتقدم بطلب للحصول على موافقة البنك المركزي المصري وذلك باستيفاء المستندات التالية كحد أدنى:

- قائمة بالوظائف والخدمات التي يرغب البنك في تقديمها أو إضافتها.
- بيان يوضح أي حالة من حالات عدم الالتزام الجزئي أو الكلى بالقواعد الخاصة بتقديم خدمات الدفع باستخدام الهاتف المحمول الصادرة من البنك المركزي المصري.
- تقرير اختبارات الاختراق Penetration Test Report الذى تم على بيئة التشغيل الفعلية قبل إطلاق الخدمة، على أن يكون قد تم إجراؤه وفقا للبند ٣-١١-٣ وفى فترة لا تتجاوز ثلاثة أشهر سابقة لتاريخ إرسال طلب البنك. يُمكن تأجيل تقديم هذا التقرير إلى ما بعد الحصول على موافقة البنك المركزي المصري المبدئية مع التزام البنك بعدم إطلاق الخدمة إلا بعد إرسال التقرير إلى البنك المركزي المصري وتصريحه للبنك بتفعيل الخدمة.

٥-٢ يجب على البنوك السابق حصولها على ترخيص بمزاولة تقديم خدمات الدفع باستخدام الهاتف المحمول قبل إصدار تلك القواعد أن تقوم بتوفيق أوضاعها والالتزام بما يلى:

- تقديم المستندات المذكورة في البند ٥-١.
- تقديم خطة توفيق الأوضاع طبقاً لجدول زمنى محدد وذلك فيما يتعلق بالفجوات بين الوضع الحالي بالبنك والمعايير والضوابط الصادرة من البنك المركزي المصري وذلك خلال فترة أقصاها ثلاثة أشهر من تاريخ إصدار هذه القواعد.
- تلتزم البنوك بتوفيق أوضاعها مع القواعد الصادرة من البنك المركزي المصري وذلك خلال فترة سماح لا تزيد عن تسعة أشهر من تاريخ تقديم خطة توفيق الأوضاع.
- تلتزم البنوك بتوفيق أوضاعها مع الضوابط الخاصة بالتشغيل البيني Interoperability وذلك خلال فترة سماح لا تزيد عن ستة أشهر من تاريخ إصدار "القواعد المنظمة لتقديم خدمات الدفع باستخدام الهاتف المحمول".
- عدم توفيق البنك للأوضاع خلال الفترة الزمنية المحددة قد يؤدي إلى إلغاء رخصة تقديم خدمات الدفع باستخدام الهاتف المحمول الممنوحة للبنك مسبقا.

٥-٣ يجب إبلاغ البنك المركزي المصري وإبلاغ مستخدمي النظام بطريقة معلنة بأية تعديلات في تعريفة الخدمة.

٥-٤ يقوم البنك بتقديم تقارير شهرية إلى البنك المركزي المصري تشمل حجم وحدات النقود الإلكترونية المُصدرة وعدد مُستخدمي النظام الذين لديهم أرصدة وعدد مُستخدمي النظام الذين ليس لديهم أرصدة وعدد مقدمي الخدمة وحجم المعاملات اليومية بأنواعها المختلفة وأية بيانات أخرى يطلبها البنك المركزي المصري.

٥-٥ تنطبق المعايير على مُشغل النظام ككل أو أي مُشغل يقوم بتشغيل جزئي للنظام ويحق للبنك المركزي المصري التفتيش على أي جزء من أجزاء النظام للتأكد من مطابقته للمعايير وللمواصفات المبلغة من قِبل البنك المركزي المصري ويعتبر عدم تسهيل مهمة البنك المركزي المصري في هذا الشأن إخلالا بهذه القواعد من قِبل البنك الذي يُدير النظام.

ملحق (أ): الحالات والقواعد الخاصة بالاستعانة بمقدمي الخدمة للتعرف على هوية العملاء كما وردت في "إجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول" الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب لعام ٢٠١٦

يمكن للبنك الاستعانة بمقدم الخدمة في تطبيق إجراءات "التعرف على هوية العملاء والتحقق منها" الواردة في "إجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول"، وذلك في الحالات التالية:

١. أن يكون مقدم الخدمة شركة هاتف محمول مرخص لها بالعمل في جمهورية مصر العربية طبقا لقانون الاتصالات رقم ١٠ لسنة ٢٠٠٣ من قبل الجهة المختصة، سواء تم تقديم الخدمة من خلال أحد فروعها أو منافذها الثابتة أو المتنقلة، على أن يتم تطبيق اجراءات "التعرف على هوية العملاء والتحقق منها" من قبل أحد موظفي الشركة.

٢. أن يكون مقدم الخدمة أحد مكاتب البريد التابعة للهيئة القومية للبريد، على أن يتم تطبيق اجراءات "التعرف على هوية العملاء والتحقق منها" من قبل أحد موظفي الهيئة المذكورة.

٣. أن يكون مقدم الخدمة شركة أو جمعية أو مؤسسة أهلية حاصلة على ترخيص بممارسة نشاط التمويل متناهي الصغر من الهيئة العامة للرقابة المالية وفقا لأحكام القانون رقم ١٤١ لسنة ٢٠١٤ والقرارات الصادرة تنفيذا له، على أن يتوافر ما يلي:

- أن يكون للجهة سجل تجاري ساري وبطاقة ضريبية سارية في حالة الشركات أو نظام أساسي معتمد من وزارة التضامن الاجتماعي فى حالة الجمعيات والمؤسسات الأهلية.
- خطاب من الهيئة العامة للرقابة المالية يفيد الموافقة على أن تكون الجهة مقدم للخدمة.
- أن يقتصر تقديم الجهة للخدمة على عملائها الحاصلين على تمويل متناهي الصغر، وبما لا يخالف أحكام القانون رقم ١٤١ لسنة ٢٠١٤ والقرارات الصادرة تنفيذا له.

٤. أن يكون مقدم الخدمة جهة أخرى بخلاف ما ورد في البنود السابقة على أن يتوافر ما يلى:

- أن يكون للجهة سجل تجاري ساري وبطاقة ضريبية سارية.
- في حالة تقديم الجهة للخدمة من خلال منفذ تابع لها بجهة أخرى، يكون للجهة الأخرى سجل تجاري ساري وبطاقة ضريبية سارية.
- قيام البنك بإخضاع مالكي الجهة والقائمين على إدارتها لإجراءات العناية الواجبة بعملاء البنوك، وجمع أية معلومات يرى 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.

وفي كل الأحوال السابقة يتعين تطبيق القواعد التالية:

١. يقوم البنك بتحديد اجراءات "التعرف على هوية العملاء والتحقق منها" بما يتفق مع ما ورد بالبند رقم (٥) من الإجراءات المذكورة بعاليه، ويقوم مقدم الخدمة بتطبيق هذه الاجراءات باعتباره وكيلاً عن البنك في تطبيقها، ويكون البنك مسئولاً مسئولية كاملة عن سلامة هذه الاجراءات وفعالية تطبيقها.

٢. يتعين على البنك وضع إجراءات مناسبة للتحقق بشكل دوري من التزام مقدم الخدمة بكافة إجراءات "التعرف على هوية العملاء والتحقق منها"، وفى حالة وجود مخالفات جوهرية أو متكررة في هذا الشأن – وفقا لمعايير يضعها البنك - يتعين أن ينظر البنك في مدى ملاءمة استمراره في الاستعانة بمقدم الخدمة لتطبيق اجراءات "التعرف على هوية العملاء والتحقق منها".

٣. يتعين أن يتضمن العقد الموقع من قبل البنك مع مقدم الخدمة التزامات ومسئوليات كل طرف بالنسبة لتطبيق إجراءات "التعرف على هوية العملاء والتحقق منها"، بما يشمل التزام مقدم الخدمة بالسماح لمفتشي البنك المركزي المصري بزيارة مقار تقديم الخدمة للتحقق من سلامة وفعالية تطبيق هذه الإجراءات.

٤. يقوم البنك بالتحقق من تلقي العاملين بالفروع والمنافذ التابعة لمقدم الخدمة التدريب اللازم للقيام بإجراءات "التعرف على هوية العملاء والتحقق منها".

٥. يتعين على مقدم الخدمة أن يرسل للبنك كافة المستندات المتعلقة بفتح حساب الخدمة للعميل وذلك بحد أقصى ثلاثين يوماً من تاريخ فتح الحساب، وفى حالة عدم الالتزام بذلك يتم إيقاف الحساب، وخلال تلك الفترة يتعين على البنك تطبيق الاجراءات اللازمة لإدارة مخاطر غسل الأموال وتمويل الإرهاب، بما يشمل وضع حدود على عدد وقيم ونوعية العمليات التي يمكن تنفيذها.

ويلتزم البنك بما يصدر لاحقاً من وحدة غسل الأموال ومكافحة تمويل الارهاب في هذا الشأن.

ملحق (ب): التعريفات

الدفع عن طريق الهاتف المحمول	أوامر الخصم على حساب الهاتف المحمول الخاص بمستخدم النظام لدى أي من البنوك المسجلة في مصر والتي يرخص لها البنك المركزي المصري بتشغيل النظام التي يصدرها المستخدم ويرسلها إلى البنك الذي يتعامل معه عن طريق الهاتف المحمول الخاص بالمستخدم ذاته.
النظام	نظام إلكتروني يضعه ويشغله بنك مسجل في مصر للدفع عن طريق الهاتف المحمول وفقا لهذه القواعد، وذلك بعد الحصول على ترخيص من البنك المركزي المصري.
وحدات النقود الإلكترونية	وحدات إلكترونية ذات قيمة نقدية تعادل كل وحدة جنيه مصري فقط دون غيره من العملات الأخرى يصدرها بنك مسجل بالبنك المركزي المصري، وهذه الوحدات تمثل التزاما على البنك المُصدر لها، وذلك شريطة استلام البنك قيمة من النقد (الجنيه المصري) لا تقل عن قيمة وحدات النقود الإلكترونية، ويكون لهذه الوحدات المحددات التالية: ▪ مُخزنة على أجهزة أو وسائط إلكترونية. ▪ تُقبل على أنها وسيلة دفع من قِبل أشخاص أو جهات أخرى بالإضافة للبنك المُصدر لها. ▪ قابلة للاستبدال إلي نقد (الجنيه المصري). ▪ مُصدرة طبقا للقواعد الصادرة عن البنك المركزي المصري شريطة الحصول على ترخيص من البنك المركزي المصري لتشغيل النظام.
البنك	الجهة المنوط بها الاحتفاظ بالإيداعات النقدية المتعلقة بالعمليات الخاصة بإصدار وحدات النقود الإلكترونية، والتأكد من اتفاق هذه العمليات مع الضوابط الرقابية الخاصة بمكافحة غسل الأموال وتمويل الإرهاب الصادرة عن البنك المركزي المصري وإجراءات العناية الواجبة بعملاء خدمة الدفع باستخدام الهاتف المحمول الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب، خاصة في مجال تحديد هوية مُستخدمي النظام (العملاء) وُمقدمي الخدمة (وفقا للتعريف الوارد أدناه)، ووضع إطار لإدارة المخاطر المرتبطة بهذه الخدمة، وتشغيل نظم الحاسبات وإدارة التسويات على حسابات مُستخدمي النظام ومُقدمي الخدمة.
شركة الهاتف المحمول	الشركة المرخص لها داخل جمهورية مصر العربية وهي الجهة المنوط بها توفير البنية التحتية للاتصالات وتوفير التقنيات اللازمة لإرسال أوامر الدفع عن طريق الهواتف المحمولة وإرسال التأكيدات الخاصة بتنفيذ هذه الأوامر، ويمكن للبنك القيام بتلك الأدوار.
مُستخدم النظام	الشخص الطبيعي أو الاعتباري المشترك في خدمة الدفع عن طريق الهاتف المحمول.
مُقدم الخدمة	أي من المنشآت التي يتعاقد معها البنك لتقديم الخدمات الواردة بالبند ٣-٢ الخاص بمقدمي الخدمة، شريطة قيام تلك المنشآت بإيداع نقود (جنيه مصري) أو ضمانات مناسبة لدى البنك مقابل تلقي وحدات نقود إلكترونية منه، ويجوز لمُقدم الخدمة تحويل هذه الوحدات إلي مُستخدمي النظام وفقاً للتفصيل الوارد بالبند ٣-٢ الخاص بمقدمي الخدمة.
حساب الهاتف المحمول	حساب يتم فتحه لدى أحد البنوك المسجلة والمرخص لها بتشغيل النظام باسم كل مُستخدم للنظام أو مُقدم للخدمة، ويتم من خلاله عمليات الإيداع والتحويل والسحب الخاصة بهذا المُستخدم أو مُقدم الخدمة.
المخاطر المتأصلة Inherent Risk	مستوى المخاطر دون الأخذ في الاعتبار أي من الضوابط الرقابية أو إجراءات المعالجة المنفذة من قبل البنك وتتكون من عنصرين: التأثير واحتمالية الحدوث.
المخاطر المتبقية Residual Risk	المخاطر التي قد يتعرض لها البنك بعد تنفيذه لضوابط أو إجراءات تعويضيه خاصة بالمخاطر المتأصلة.
التصديق Authentication	الأساليب والإجراءات والعمليات المستخدمة لتدقيق الهوية والصلاحية للعملاء الجدد والحاليين.
كلمات السر المستخدمة لمرة واحدة One-Time Password	كلمة السر المستخدمة والصالحة لأغراض التصديق لمرة واحدة فقط للدخول على النظام أو لفترة زمنية محددة - مثال: نحو ٩٠ ثانية - لضمان عدم إعادة استخدامها لأغراض التصديق في مرات لاحقة في حال تسجيلها عن طريق الهاكرز.
خطة استمرارية العمل Business Continuity Plan	إعداد وتدقيق خطط لوجستية لكيفية تعافي البنك واستعادة الوظائف الحيوية التي تم اعتراضها بصورة جزئية أو كلية (العاجلة) وذلك خلال فترة زمنية محددة مسبقاً بعد الكوارث أو استمرار تعطل الخدمة. ويطلق على هذه الخطة اللوجستية خطة استمرارية العمل.
الرقم السري Personal Identification Number(PIN)	يتكون رقم التعريف الشخصي من مجموعة من الأرقام السرية التي تُستخدم للتصديق على دخول المستخدم على النظام. وبصفة أساسية، يطلب من المستخدم إدخال معلومة غير سرية كاسم مُستخدم النظام ومعلومة سرية وهي الرقم السري للدخول على النظام. وفور استلام اسم المستخدم والرقم السري، يقارن النظام الرقم السري باسم المستخدم بالإضافة إلى مقارنة الرقم السري الصادر بالمسجل. وعندئذ يتم منح المستخدم صلاحية الدخول على النظام عند مطابقة الأرقام التي تم إدخالها مع تلك المسجلة على النظام.
إدارة المخاطر Risk Management	العملية المستمرة لتحديد وقياس ومراقبة وإدارة التعرضات للمخاطر المحتملة.

القدرة على تحمل المخاطر Risk Appetite	مستوى المخاطر التي يمكن للبنك تحملها لتحقيق أهداف الأعمال.
خطة المعالجة Remediation Plan	الخطة اللازمة لتنفيذ إجراءات المعالجة لتهديد أو عدد من التهديدات الذي يواجه نظام المؤسسة. وتتضمن الخطة بصفة أساسية عدد من الخيارات المطلوبة لإزالة هذه التهديدات والأولويات الخاصة بخطة المعالجة.
اتفاقية مستوى الخدمة Service Level Agreement	اتفاقية مستوى الخدمة - يشار إليها اختصاراً SLA - هي جزء من عقد الخدمة والتي يتم من خلالها تحديد مستوى الخدمة بصفة رسمية. وبصورة عملية، يشير هذا المصطلح عادة إلى الزمن اللازم للتنفيذ طبقاً للعقد أو أداء العقد.
تقييم نقاط الضعف Vulnerability Assessment	يبحث المسح الخاص بالثغرات في النظام والتقارير ويكشف التعرضات المحتملة. ويغطي النطاق بصورة أساسية كافة البني التحتية في بيئة البنوك العاملة.
اختبار الاختراق Penetration Testing	الاختبار اليدوي المصمم لاستغلال نقاط الضعف في هيكل النظام أو بيئة الحاسب الآلي.

طبع بمطابع البنك المركزى المصرى
www.cbe.org.eg