الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية

مقدمة:

شهدت الصناعة المصرفية فى الآونة الأخيرة تقدما ملموسا فى مجال السماح لعملاء البنوك بإجراء العمليات المصرفية من خلال شبكات الإتصال الالكترونية ومن المتوقع أن تنتشر هذه العمليات بشكل واسع فى الفترة المقبلة خاصة فى ظل التطور المستمر فى مجال التقنية المصرفية، كما شهد العالم إصدار وسائل دفع لنقود الكترونية Electronic Money كوسيلة لتسوية المعاملات فيما بين مختلف الأطراف.

ونظرا لما يصاحب إجراء العمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية من مخاطر متعددة لاتقتصر فقط على المخاطر التقليدية، فإن الأمر يستلزم وضع الأسس للإدارة الحد من هذه المخاطر والتحديد الدقيق لمسئوليات مختلف الجهات ذات العلاقة بها وما يستلزمه ذلك من الحصول على ترخيص من البنوك المركزية وموافاته بالبيانات اللازمة وذلك على النحو الوارد بهذه الضوابط.

أولا: العمليات المصرفية الالكترونية

(١) التعريف بالعمليات المصرفية الالكترونية:

يقصد بالعمليات المصرفية الالكترونية تقديم البنوك الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات إتصال الكترونية تقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التى تحددها البنوك، وذلك من خلال أحد المنافذ على الشبكة كوسيلة لإتصال العملاء بها بهدف:-

(أ) إتاحة معلومات عن الخدمات التى يؤديها البنك دون تقديم خدمات مصرفية على الشبكة.

(ب) حصول العملاء على خدمات محدودة كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث
بياناتهم وطلب الحصول على قروض.

(ج) طلب العملاء تنفيذ عمليات مصرفية مثل تحويل الأموال.

ولأغراض هذه الضوابط فإن البنوك التى تقوم بتقديم الخدمات الواردة بالبند (ج) فقط تعتبر بنوكا تقدم عمليات مصرفية الكترونية تتطلب توافر سياسات وإجراءات لتقييم المخاطر Assessing والرقابة عليها Controllingومتابعتها Monitoring، إلا أنه يجب أيضا على البنوك مراعاة الإدارة لأية مخاطر بشأن العمليات الواردة بالبندين (أ)، (ب).

وتتمثل مزايا العمليات المصرفية الالكترونية فيما يلى:

- إمكان وصول البنوك إلى قاعدة أعرض من العملاء المودعين والمقترضين وطالبى الخدمات المصرفية.
- تقديم خدمات مصرفية جديدة.
- خفض تكاليف التشغيل بالبنوك وتكاليف إنجاز عمليات التجزئة
- زيادة كفاءة أداء البنوك.

(٢) الأسباب التى تستلزم حصول البنوك على ترخيص لتقديم العمليات المصرفية الإلكترونية:

(أ) حماية السوق المصرفى المحلى من مقدمى الخدمات المصرفية غير المرخص لهم بتقديم هذه الخدمات بما فى ذلك الجهات التى ترغب فى تأسيس كيان مستقل لا يتواجد له فروع مادية بغرض تقديم العمليات المصرفية الالكترونية فقط Virtual bank.

(ب) التحقق من توافر الوسائل الكافية لدى البنوك لإدارة مخاطرالعمليات.

(ج) تطبيق الضوابط الرقابية اللازمة لحصول البنوك على ترخيص لتقديم تلك العمليات.

(٣) شروط حصول البنوك على ترخيص لتقديم العمليات المصرفية الالكترونية:

(أ) يقتصر منح الترخيص على البنوك المسجلة لدى البنوك المركزية وحدها.

(ب) أن يكون البنك مستوفيا للضوابط الرقابية التى تتعلق بمدى التزامه بكل من معيار كفاية رأس المال وأسس تصنيف القروض وتكوين المخصصات والتوازن فى مراكز العملات وتركز التوظيفات لدى المراسلين فى الخارج والتركز الإئتمانى.

(ج) أن يتبع البنك مبادئ حصيفة لإدارة مخاطر تقديم خدماته من خلال شبكات الإتصال الالكترونية والتى تشتمل على تقييم المخاطر والرقابة عليها ومتابعتها (يوضح المرفق رقم (١) مخاطر العمليات المصرفية الالكترونية والمبادئ الإسترشادية لإدارتها).

(د) أن يحدد البنك لدى طلبه للحصول على الترخيص نوعية الخدمات التى سيقوم بتأديتها من خلال الشبكات.

(ه) أن يحدد البنك المسئوليات الواقعة عليه من جراء تقديم الخدمات عبر الشبكات.

(و) أن يحدد البنك المسئوليات الواقعة على العميل من جراء حصوله على الخدمات عبر الشبكات .

(ز) إفصاح البنك المرخص له بالقيام بالعمليات المصرفية الالكترونية وفقا للوارد بالبند أولا على صفحة ال Web الخاصة به بما يفيد حصوله على ترخيص لتقديم خدماته عبر الشبكات ورقم وتاريخ الحصول عليه، مع ربط هذا الموقع بصفحة البنك المركزى المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext Links حتى يتحقق العملاء من صحة الترخيص.

ثانيا: إصدار وسائل دفع لنقود الكترونية

(١) التعريف بإصدار وسائل دفع لنقود الكترونية:

يشتمل إصدار وسائل دفع لنقود الكترونية على مايلى:-

(أ) إصدار البنك لبطاقات القيمة المخزنة value cards – Stored كالبطاقات الذكية Smart cards، أو غيرها، وذلك بالسماح بتخزين وحدات من النقود على هذه البطاقات التى تحمل شرائح ممغنطة تسمح بذلك.

(ب) إتاحة البنك لنقدية إلكترونية Electronic cash بتخزين وحدات من النقود على وسائط الكترونية Electronic device مثل الحاسب الشخصى الذى يتم تحميله ببرنامج خاص لهذا الغرض، وتستخدم هذه النقود لإجراء مدفوعات ذات قيم محدودة بتحويلها إلى الوسائط الالكترونية الخاصة بالأطراف المقابلة.

ولأغراض هذه الضوابط يتعين أن تلتزم البنوك أيضا بالإدارة الحصيفة للمخاطر المرتبطة بوسائل الدفع الأخرى والتى من بينها:

(أ) بطاقات الخصم Debit cards ويقتصر إستخدامها خصما على حسابات دائنة للعملاء.

(ب) بطاقات الإئتمان Credit cards ويتم إستخدامها خصما على حسابات مدينة وفقا للحدود المقررة. وتستخدم الوحدات الطرفية لنقاط البيع sale terminals Point of وآلات الصرف الآلى Automatic teller machines وغيرها كوسائط لإتصال حائزى بطاقات الخصم والإئتمان بشبكة الإتصال الإلكترونية.

(٢) الأسباب التى تستلزم حصول البنوك على ترخيص لإصدار وسائل دفع لنقود الكترونية:

بالنظر إلى أن البنك المركزى هو الجهة المنوط بها قانونا إصدار أوراق النقد للإستخدام كوسيلة دفع لها قوة إبراء، تخضع عملية إصدار وسائل دفع لنقود الكترونية لرقابة البنك المركزى بالدولة خاصة أنه ليس لها قوة إبراء إلا بعد تسوية قيمة المدفوعات التى تمت بها طرف كل من بنك المشترى وبنك البائع.

(٣) شروط حصول البنوك على ترخيص لإصدار وسائل دفع لنقود الكترونية:

(أ) أن يكون البنك مستوفيا للضوابط الرقابية التى تتعلق بمدى التزامه بكل من معيار كفاية رأس المال وأسس تصنيف القروض وتكوين المخصصات والتوازن فى مراكز العملات وتركز التوظيفات لدى المراسلين فى الخارج والتركز الإئتمانى.

(ب) أن يتبع البنك مبادئ حصيفة لإدارة مخاطر إصدار وسائل دفع لنقود الكترونية وأن يحدد تفصيلا أنواع وسائل الدفع التى يرغب فى إصدارها والشروط المتعلقة بها وكذا مسئوليات الجهات ذات العلاقة بهذه النقود والتى تشتمل على مسئوليات البنك والعميل.

(ج) إفصاح البنك المرخص له بإصدار وسائل دفع لنقود الكترونية على صفحة ال Web الخاصة به بما يفيد حصوله على ترخيص بذلك ورقم وتاريخ

الحصول عليه، مع ربط هذا الموقع بصفحة البنك المركزى المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext Links حتى يتحقق العملاء من صحة الترخيص.

(د) أن يتم الحصول على موافقة العميل على الخصم على رصيد حسابه الجارى بالقيمة التى يتيحها له البنك الكترونيا والعمولة التى يتقاضاها البنك لقاء ذلك.

مخاطر العمليات المصرفية الالكترونية والمبادئ الإسترشادية لإدارتها

أولا: مخاطر العمليات المصرفية الالكترونية

يصاحب تقديم العمليات المصرفية الالكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغى قيام البنوك بوضع السياسات والإجراءات التى تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها .

أنواع المخاطر:

(١) مخاطر التشغيل.
(٢) مخاطر السمعة.
(٣) مخاطر قانونية.
(٤) مخاطر أخرى، ومن ذلك مخاطر الإئتمان والسيولة وسعر العائد ومخاطر السوق.

وفيما يلى عرض موجز لهذه المخاطر:

(١) مخاطر التشغيل Operational risk

تنشأ مخاطر التشغيل من عدم التأمين الكافى للنظم أو عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة وكذا نتيجة إساءة الإستخدام من قبل العملاء وذلك على النحو التالى:-

(أ) عدم التأمين الكافي للنظم: security System

تنشأ هذه المخاطر عن إمكان إختراق غير المرخص لهم access Unauthorized لنظم حسابات البنك بهدف التعرف على المعلومات الخاصة بالعملاء وإستغلالها سواء تم ذلك من خارج البنك او من العاملين به، بما يستلزم توافر إجراءات كافية لكشف وإعاقة ذلك الإختراق.

(ب) عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة:

implementation, and maintenance ،design Systems

وهى تنشأ من إخفاق النظم أو عدم كفاءتها (بطىء الاداء Slow- Down على سبيل المثال) لمواجهة متطلبات المستخدمين وعدم السرعة فى حل هذه المشاكل وصيانة النظم وخاصة إذا زاد الإعتماد على مصادر خارج البنوك لتقديم الدعم الفنى بشأن البنية الأساسية اللازمة Outsourcing.

(ج) إساءة الإستخدام من قبل العملاء: Customer misuse of services

ويرد ذلك نتيجة عدم إحاطة العملاء بإجراءات التأمين الوقائية Security precautions أو بسماحهم لعناصر إجرامية بالدخول الى حسابات عملاء آخرين أو القيام بعمليات غسيل الأموال بإستخدام معلوماتهم الشخصية أو قيامهم بعدم إتباع إجراءات التأمين الواجبة.

(٢) مخاطر السمعة risk Reputational

تنشأ مخاطر السمعة فى حالة توافر رأى عام سلبى تجاه البنك، الأمر الذى قد يمتد إلى التأثير على بنوك أخرى، نتيجة عدم مقدرة البنك على إدارة نظمه بكفاءة أو حدوث إختراق مؤثر لها.

(٣) المخاطر القانونية risk Legal

تقع هذه المخاطر فى حالة إنتهاك القوانين أو القواعد أو الضوابط المقررة خاصة تلك المتعلقة بمكافحة عمليات غسيل الأموال، أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الالكترونية ومن ذلك عدم وضوح مدى توافر قواعد لحماية المستهلكين فى بعض الدول أو لعدم المعرفة القانونية Validity لبعض الاتفاقيات المبرمة بإستخدام وسائل الوساطة الالكترونية.

(٤) المخاطر الأخرى

يرتبط أداء العمليات المصرفية الالكترونية بالمخاطرالخاصة بالعمليات المصرفية التقليدية، ومن ذلك مخاطر الإئتمان والسيولة وسعر العائد ومخاطر السوق مع إحتمال زيادة حدتها، فعلى سبيل المثال فإن إستخدام قنوات غير تقليدية للإتصال بالعملاء وإمتداد نشاط منح الإئتمان إلى عملاء عبر الحدود Cross- border قد يزيد من إحتمالات إخفاق بعض العملاء فى سداد التزاماتهم.

ثانيا: مبادئ إدارة المخاطر management Risk

تشتمل إدارة المخاطر على التقييم والرقابة والمتابعة وذلك على النحو التالى:-

(١) تقييم المخاطرrisks Assessing

ويشمل التقييم مايلى:

(أ) تحديد المخاطر التى قد يتعرض لها البنك، ومدى تأثيرها عليه.

(ب) وضع حدود قصوى لما يمكن للبنك أن يتحمله من خسائر نتيجة التعامل مع هذه المخاطر.

(٢) الرقابة على التعرض للمخاطر exposures risk Controlling

تشتمل هذه الرقابة على ستة مجالات على النحو التالى:

(أ) تنفيذ سياسات وإجراءات التأمين security Implementing measures and policies

تستهدف سياسات وإجراءات التأمين ما يلى:-

(١) تحديد شخصية المتعامل مع النظم / التصديق(Identification /authentication).

(٢) ضمان عدم إجراء تعديلات على رسائل العملاء أثناء انتقالها عبر القنوات.

(٣) ضمان الحفاظ على سرية معاملات العملاء Privacy

(٤) ضمان عدم إنكار مرسل الرسالة لها repudiation – Non

ويراعى فى هذا المجال مايلى:-

(١) إتباع سياسات وإجراءات تحقق تأمين الإتصالات من والى النظم لمنع أو الحد من اختراق غير المرخص لهم للنظم أو إساءة إستخدامها.

(٢) الرقابة على دخول النظم وتحديد شخصية المستخدمين.

(٣) حماية النظم من إحتمالات القيام بممارسات غير مرخص بها من قبل العاملين بالبنك السابقين أو الجدد أو المؤقتين.

(د) يتطلب الأمر بالنسبة لإصدار وسائل دفع لنقود الكترونية إتخاذ إجراءات اضافية للتأمين، ويشمل ذلك:

- الإتصال المباشر مع مصدر البطاقات أو المشغل المركزى للحماية من التزييف.

On- line interaction with the issuer or a central operator

- متابعة العمليات الفردية.
- الإحتفاظ بقاعدة بيانات مركزية لتتبع عمليات غسيل الأموال.
- توافر شروط الأمان فى البطاقات الذكية، أو غيرها، مع مراعاة وضع حد أقصى لما يخزن على البطاقة.

(ب) تدعيم الإتصالات بين المستويات المختلفة بالبنك من مجلس إدارة وإدارة عليا، وبين العاملين بشأن سلامة أداء النظم وتوفير التدريب المستمر للعاملين communication internal Coordinating

(ج) إستمرار تقديم وتطوير الخدمات developing and Evaluating services

(د) وضع ضوابط للحد من المخاطر فى حالة الإعتماد على مصادر خارج البنك لتقديم الدعم الفنى:

تشتمل هذه الضوابط على مايلى:-

- متابعة الأداء المالى والتشغيلى لمقدمى الدعم الفنى.
- التأكد من توافر إتفاقيات تعاقدية مع مقدمى الدعم الفنى تحدد التزامات الأطراف تفصيليا.
- التأكد من مقدرة مقدمى الدعم الفنى على توفير التأمين بما يتفق و المتبع داخل البنك فى حالة تعرفهم على بيانات ذات حساسية تخص البنك، و ذلك من خلال مراجعة سياساتهم و اجراءاتهم فى هذا المجال.
- توفير ترتيبات طوارئ لتغطية إحتمالات حدوث تغيير مفاجئ فى مقدمى الدعم الفنى.

(ه) إحاطة العملاء عن العمليات المصرفية الالكترونية وكيفية إستخدامها Providing customer education and disclosure

(و) إعداد خطط طوارئ planning Contingency

- إعداد خطط طوارىء بديلة فى حالة اخفاق النظم عن أداء الخدمات

وذلك فيما يتعلق بما يلى:-

× إعادة البيانات إلى الوضع الذى كانت عليه قبل الإخفاق Data recovery.

× توفير قدرات بديلة لتشغيل البيانات Alternative data – processing capabilities.

× توفير عاملين لمواجهة الظروف الطارئة.

· إختبار نظم التشغيل البديلة systems Backup بصفة دورية للتأكد من فاعليتها.

· توافر التأمين اللازم فى حالة تنفيذ خطط الطوارىء وكذا توافر تعليمات لإستخدام هذه الخطط لدى مقدمى الدعم الفنى.

· إبرام عقود بديلة مع مقدمى دعم فنى آخرين تنفذ فى حالة إخفاق المقدمين الأساسيين.

(٣) متابعة المخاطر risks Monitoring:

تتمثل متابعة المخاطر فى إختبار النظم وإجراء المراجعة الداخلية والخارجية System testing and auditing وذلك على النحو التالى:-

(أ) إجراء اختبارات دورية للنظم، والتى يكون من ضمنها:

· إجراء إختبار إمكان الإختراق Penetration testing الذى يهدف الى تحديد وعزل وتعزيز تدفق البيانات من خلال النظم وإتباع إجراءات لحماية النظم من المحاولات غير العادية للإختراق.

· إجراء مراجعة دورية من خلال النظم للتأكد من فاعلية اجراءات التامين والوقوف على مدى اتساقها مع سياسات واجراءات التامين المقررة.

(ب) اجراءات المراجعة الداخلية والخارجية:

· تسهم المراجعة الداخلية والخارجية فى تتبع الثغرات وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتزام البنك بها.

مسئوليات إسترشادية للبنك
لدى تقديم خدماته عبر شبكات الإتصال الألكترونية

(١) موافقة مجلس إدارة البنك على إستراتيجية تتضمن قيام البنك بتقديم خدماته عبر الشبكات على أن يحاط المجلس بكافة المخاطر الناشئة عن ذلك.

(٢) موافقة مجلس إدارة البنك على سياسة الإدارة التنفيذية للبنك فيما يتعلق بأسلوب إدارة المخاطر، وتدعيم نظم الرقابة الداخلية بشأن تلك المخاطر.

(٣) تصميم نماذج عقود لتأدية مختلف الخدمات المصرفية التى تؤدى عبر شبكات الإتصال الالكترونية وأن يتأكد البنك من توافر القوى البشرية المؤهلة للتعامل مع عملاء البنك عبر الشبكات، مع تحديد ساعات تقديم هذه الخدمات.

(٤) فى حالة وجود طرف آخر تقدم من خلاله الخدمة فيتعين على مجلس إدارة البنك إقرار إتفاقية التشغيل التى تنظم العلاقة بين البنك مع هذا الطرف وتحديد مسئوليته فى الحفاظ على سرية التعليمات والمعاملات التى تتم عبر الشبكات وأية معلومات تتاح له.

(٥) إفصاح البنك على صفحة ال Web الخاصة به بما يفيد حصوله على ترخيص بتقديم خدماته عبر الشبكات من البنك المركزى المصرى ورقم وتاريخ الحصول على الترخيص والخدمات التى يجوز للبنك تقديمها عبر الشبكات، مع ربط هذا الموقع بصفحة البنك المركزى المصرى المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext Links حتى يتحقق العملاء من صحة التصريح.

(٦) إفصاح البنك عن أن القوانين المصرية هى التى تحكم الخدمات التى يقوم بتأديتها للعملاء عبر الشبكات.

(٧) ضرورة أن يتحقق البنك من شخصية طالب / متلقى الخدمة بأساليب قانونية ثابتة تضمن الحقوق المتبادلة.

مسئوليات إسترشادية تقع على العميل
عند تلقى خدماته عبر شبكات الإتصال الالكترونية

(١) يتحمل العميل مسئولية صحة المعلومات التى يقوم بإدخالها عبر الشبكات بإعتباره مستخدما للخدمات التى تؤدى من خلالها، ويقر العميل بأن التعليمات والمعاملات التى يدخلها يتم التعامل عليها بدون أية مراجعة إضافية من البنك أو إشعارات خطية أو التأكد منها بطرق أخرى.

(٢) لايلتزم البنك بقبول أية تعديلات أو الغاء تعليمات أو معاملات سبق أن أرسلها العميل عبر الشبكات.

(٣) يتحمل العميل مسئولية إعداد البيانات الخاصة بالمستفيد أو الإضافة أو التعديل عليها.

(٤) يلتزم العميل بمراعاة إجراءات الحماية فى التعامل عبر الشبكات مع البنك.

(٥) يتحمل العميل مسئولية سوء إستخدام الخدمة الناتج عن عدم الإلتزام بإجراءات الحماية أو الشروط والأحكام الواردة فى العقد الذى يتم إبرامه مع البنك بشأن العمليات المصرفية الألكترونية، أو الناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الإستخدام.

(٦) عدم تحمل البنك مسئولية تعطل الخدمة لظروف خارجة عن إرادته.

(٧) تعتبر سجلات البنك حجة قاطعة ملزمة قانونا على صحة المعاملات والتعليمات.

(٨) يلتزم العميل فى حالة فقد أو سرقة جهاز الشفرة بإخطار البنك لكى يقوم بإبطال هذا الجهاز.

(٩) تعتبر أدوات الحماية وسيلة للتعرف والتحقق من شخصية العميل، وبمجرد إتمام إدخالها بنجاح يعتبر العميل هو مصدر جميع التعليمات والمعاملات.