أمانة مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

مخاطر الجرائم المالية الإلكترونية وآثارها على نظم الدفع

اللجنة العربية لنظم الدفع والتسوية

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
COUNCIL OF ARAB CENTRAL BANKS AND MONETARY AUTHORITIES GOVERNORS

رقم
104
2019

أمانة
مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

مخاطر الجرائم المالية الإلكترونية وآثارها على نظم الدفع

اللجنة العربية لنظم الدفع والتسوية

صندوق النقد العربي
أبوظبي – دولة الإمارات العربية المتحدة

تـقديـم

أرسى مجلس محافظي المصارف المركزية ومؤسسات النقد العربية تقليداً منذ عدة سـنوات، بدعوة أحد أصـحاب المعالي والسـعادة المحافظين لتقديم ورقة عمل حول تجربة دولته في أحد المجالات ذات العلاقة بعمل المجلس. كما يصـــدر عن اللجان وفرق العمل المنبثقة عن المجلس، أوراق عمل تتناول الموضوعات والقضايا التي تناقشها هذه اللجان والفرق. إضافة إلى ذلك، يعد صندوق النقد العربي ضمن ممارسته لنشاطه كأمانة فنية لهذا المجلس، عدداً من التقارير والأوراق في مختلف الجوانب النقدية والمصـــرفية التي تتعلق بأنشـطة المصـارف المركزية ومؤسـسـات النقد العربية. وتعد هذه التقارير والأوراق من أجل تسهيل اتخاذ القرارات والتوصيات التي يصدرها المجلس. وفي ضـــوء ما تضـــمنته كل هذه الأوراق والتقارير من معلومات مفيدة عن موضوعات ذات صلة بأعمال المصارف المركزية، فقد رأى المجلس أنه من المناســب أن تتاح لها أكبر فرصـــة من النشـــر والتوزيع. لذلك، فقد باشـــر الصـــندوق بنشـــر هذه الســـلســـة التي تتضـــمن الأوراق التي يقدمها الســـادة المحافظين إلى جانب التقارير والأوراق التي تعدها اللجان والصـــندوق حول القضايا النقدية والمصرفية ذات الأهمية. ويتمثل الغرض من النشر، في توفير المعلومات وزيادة الوعي بهذه القضـــايا. فالهدف الرئيســـي منها هو تزويد القارئ بأكبر قدر من المعلومات المتاحة حول الموضوع. نأمل أن تساعد هذه السلسة على تعميق الثقافة المالية والنقدية والمصرفية العربية.

والله ولي التوفيق،

عبد الرحمن بن عبد الله الحميدي
المدير العام رئيس مجلس الإدارة
صندوق النقد العربي

المحتويات

أولاً: تمهيد

تعد الجرائم المالية الإلكترونية من الجرائم الخطيرة والمعقدة كونها جرائم عابرة للحدود، تستخدم فيها أحدث التقنيات الحديثة، وهي ناتجة عن التطور الهائل في التقنيات الإلكترونية الحديثة والإبتكارات المرافقة لها التي غزت عالم الأعمال في السنوات الماضية. يقدر أن تتسبب الهجمات الإلكترونية في خسارة الإقتصاد العالمي نحو 3 تريليونات دولار بحلول عام 2020، إذا لم تتخذ الحكومات التدابير اللازمة لمواجهة هجمات القرصنة الإلكترونية .

استحوذ الموضوع على اهتمام كبير من قبل الأطر والمؤسسات المالية والمصارف المركزية في مختلف دول العالم، كما أقدمت المصارف والمؤسسات المالية على تبني خطط عمل وبرامج لمواجهة تحديات الجرائم المالية الالكترونية واقتناء الأنظمة والبرمجيات المناسبة.

نظراً لأهمية الموضوع، قامت اللجنة العربية لنظم الدفع والتسوية بمناقشة مخاطر الجرائم المالية وتداعياتها على كفاءة نظم الدفع. تم التفاهم على إعداد ورقة تتناول التعريف بالجرائم المالية الالكترونية وتجارب الدول العربية، من حيث استعراض أهم الإجراءات المتخذة من طرف السلطات الإشرافية والرقابية في الدول العربية، لمواجهة الجرائم المالية الالكترونية.

ثانياً: أنواع الجرائم المالية الالكترونية

تضم الجريمة الإلكترونية مجموع الجرائم التي ترتكب ضد أفراد أو مجموعات لإلحاق الضرر عمداً بهم، أو التسبب بالأذى المالي للضحية بشكل مباشر أو غير مباشر، من خلال استخدام شبكات الاتصال الحديثة مثل الإنترنت والهواتف النقالة وغيرها من الوسائل. يشمل هذا النوع من الجرائم كافة الأفعال الإجرمية التي تتم من خلال الحواسيب والشبكات كعمليات الاختراق والقرصنة.

ثالثاً ـ الخسائر الناتجة عن الجرائم الالكترونية – تجارب دولية

تبلغ خسائر الاقتصاد العالمي جراء الجرائم الإلكترونية حوالي 400 مليار دولار سنوياً، وهناك توقعات بارتفاعها في السنوات القادمة مع استمرار تلك الجرائم، ومن المتوقع أن تتسبب الهجمات الإلكترونية في خسارة الاقتصاد العالمي كما سبقت الإشارة نحو 3 تريليونات دولار بحلول عام 2020 .

يعتبر الهجوم على مصرف بنغلاديش مثال واحد من أمثلة عديدة على الجرائم المالية الالكترونية التي عصفت بالنظام المصرفي العالمي على مدى السنوات القليلة الماضية. تعتبر قارة آسيا أكثر المناطق ضعفاً، وتشير التقديرات إلى أن الجرائم الإلكترونية كلفت الشركات الآسيوية حوالي 81 مليار دولار في عام 2016 وحده، وهو رقم يمثل أكثر من ربع المجموع العالمي البالغ 315 مليار دولار. ومن أهم العوامل التي جعلت آسيا معرضة لمثل هذه الهجمات:

- عدم تطور نظم أمن المعلومات نسبياً في العديد من المصارف الآسيوية.
- نقص الوعي عن مخاطر الجرائم المالية الالكترونية .

وعلى الرغم من أن آسيا تبدو في الوقت الحاضر منطقة ضعيفة، فإن الجريمة المالية الإلكترونية أصبحت الآن مشكلة عالمية حقيقية بالنسبة للبنوك والمؤسسات المالية. ولعل أفضل مثال على ذلك عندما تمكنت عصابة Carbanak من سرقة حوالي مليار دولار من 100 مصرف في 30 دولة حول العالم. ووفقا لشركة Kaspersky Lab العالمية فإن السرقة تنطوي على:

- قرصنة كل أنظمة البنك المستهدف والشبكات، بواسطة استخدام "البرمجيات الخبيثة."
- "Spear Phishing"، الذي يمكن القراصنة من ارسال رسائل مشبوهة لموظفي البنوك من أجل السيطرة على أجهزة الكمبيوتر.
- استغلال القراصنة للمشكلة إلى حد كبير بسبب مستوى الوعي الغير كافي من قادة المصارف، حيث وجدت دراسة استقصائية من KPMG

أن 12 في المائة من الرؤساء التنفيذيين في البنوك لم يعرفوا ما إذا كانت البنوك قد تم اختراقها.

حددت الوكالة الرئيسية لإنفاذ القانون في الاتحاد الأوروبي مؤخراً اثنين من المخاطر الأكثر تهديدا للصناعة المصرفية:

- البرامج الخبيثة: والتي تنطوي على استخدام البرامج الخبيثة للحصول على البيانات السرية المتعلقة بعملاء البنك باستخدام الخدمات المصرفية عبر الإنترنت وأنظمة الدفع.
- احتيالات الدفع: التي تنطوي على هجمات البرمجيات الخبيثة على أجهزة الصراف الآلي وبطاقات الائتمان.

ومع أن هذه التهديدات أصبحت مشكلة حقيقية للبنوك في جميع أنحاء العالم، يبدو أنها ستضطر إلى:

- زيادة قدراتها الدفاعية وبسرعة، بسبب زيادة في عدد وتعقد الهجمات.
- التعاون بين البنوك من أجل التصدي بفعالية لهذه التهديدات.
- أن تكون المصارف أكثر انفتاحا لتبادل المعلومات عند الاستيلاء عليها كوسيلة للحفاظ على سلامة شبكة المدفوعات العالمية.

ونتيجة لهذه التهديدات، قررت أكبر البنوك في الولايات المتحدة المواجهة من خلال تشكيل تحالف من أكبر ثمانية بنوك في الولايات المتحدة من أجل تبادل المعلومات حول الهجمات المحتملة لأنظمتها الأمنية على الإنترنت، ولمساعدة الأعضاء على تبادل بيانات الجرائم المالية الإلكترونية.

أما في الهند فقد تعرضت بنوك القطاعين العام والخاص الكبيرة للاختراق الأمني بحيث تم اختراق بطاقات الإئتمان الخاصة بالعملاء والموظفين، وتأثرت أكبر البنوك في الهند بما في ذلك البنك المركزي. حاولت البنوك الهندية احتواء الضرر الذي خلفته قرصنة أكثر من 3.2 مليون بطاقة تم اختراقها من بطاقات الإئتمان، واستطاعت البنوك استرجاع آلاف البطاقات واوقفت أخرى تخشى

أن تكون قد تعرضت للاختراق، كما نصحت، العملاء بتغيير أرقام التعريف الشخصية الخاصة بهم.

رابعاً: تجارب الدول العربية

قامت اللجنة العربية لنظم الدفع والتسوية، بإعداد استبيان حول الجرائم المالية الالكترونية والإجراءات المتخذة، وفيما يلي خلاصة عن أهم نتائجه التي تبرز الجهد التي تقوم بها المصارف المركزية ومؤسسات النقد العربية:

- **البنك المركزي الأردني:** يقوم البنك المركزي بشكل مستمر إعداد دراسات شاملة حول عدة مواضيع بخصوص مخاطر القرصنة الإلكترونية وكيفية التخفيف منها ويعمل على تحسين الاستراتيجيات الموجودة لديه والتصدي لتهديدات الامن السيبراني بالإضافة الى الاطلاع على اهم الاجراءات المتبعة من قبل البنوك المركزية والجهات الدولية. كما قام بإجراء دراسة حول مخاطر القرصنة الإلكترونية لاسيما في ظل التطورات والابتكارات والتطبيقات في الصناعة المصرفية والتقنيات الإلكترونية الحديثة حيث تشتمل القواعد الخاصة لكل من التطبيقات الحديثة التي يتم اطلاقها في القطاع المصرفي بقواعد الحماية والتأمين من مخاطر القرصنة.

- **مصرف الإمارات العربية المتحدة المركزي:** يقوم المصرف المركزي بصفة دورية بدراسة المخاطر التشغيلية لأنظمة الدفع ومنها مخاطر القرصنة الالكترونية، لما لها من تأثير على المعلومات العملاء واستمرارية نظم الدفع. كذلك يقوم المصرف المركزي بالتنسيق المباشر مع الجهات المعنية بأمن المعلومات في الدولة بشأن الامن السيبراني، ومن جهة اخرى يتابع المصرف مع فريق طوارئ الحاسب الآلي بالدولة (aecert)، المستجدات من خلال النشرات التي يصدرها الفريق وبالتالي أخذ الحيطة والحذر حسب درجة التحذير الأمني وباتباع الخطوات المطلوبة. كذلك قام المصرف المركزي بإنشاء ادارة لأمن المعلومات تتبع لدائرة ادارة المخاطر والانضباط.

- **البنك المركزي التونسي:** أعطى البنك المركزي التونسي أهمية كبيرة لضرورة وضع كل التدابير اللازمة لحماية منظومات الدفع بصفة خاصة والقطاع المصرفي بصفة عامة من مخاطر القرصنة الإلكترونية. ونظم العديد من الدورات التدريبية للعاملين في القطاع المصرفي والمدفوعات. كذلك تم تأسيس الوكالة التونسية للسلامة المعلوماتية التي يقع على عاتقها وضع مقاييس خاصة بالسلامة المعلوماتية وإعداد الأدلة الفنية، والعمل على تشجيع تطوير حلول وطنية في مجال السلامة المعلوماتية وإبرازها. وفيما يتعلق بالقطاع المصرفي وأنظمة الدفع، تم اطلاق نظام (BANKING-CERT) الخاص بالقطاع المصرفي تحت اشراف الجمعية المهنية للبنوك والمؤسسات المالية، الى جانب إجراء التدريبات اللازمة للعاملين بمجال أمن المعلومات لمواكبة التطور المطلوب، والاعداد لاستراتيجية وطنية للحماية من مخاطر القرصنة الالكترونية وذلك بمشاركة كل الاطراف المعنية.

- **بنك الجزائر:** تقوم الجهات المختصة ببنك الجزائر بالمراقبة عن كثب لكل الأخطار التي تحوم حول نظام معلوماتها، وتتخذ في كل مرة كل التدابير اللازمة من أجل حماية هذا النظام. من بين الإجراءات التي اتخذت على مستوى بنك الجزائر: منع استعمال وحدات التخزين المتنقلة، ومنع تحميل أية برمجيات غير مرخص بها بالإضافة الى توفير دقة في تتبع مختلف المعاملات. كما أصدر بنك الجزائر تعميم حول أمن أنظمة الدفع، أكد فيه على كافة الشروط التي يجب توفيرها من قبل مشغلي أنظمة الدفع وكذلك المؤسسات المنخرطة فيها بغرض ضمان حسن سير هذه الأنظمة، إلى جانب حماية المعلومات التي تمر عبرها وضمان سريتها وصحتها.

- **مؤسسة النقد العربي السعودي**: قامت مؤسسة النقد العربي السعودي بإصدار استراتيجية موحده لأمن المعلومات للقطاع المالي وفقاً لأفضل المعايير الدولية، حيث يوجد فريق للإشراف على مدى التزام المؤسسات المالية بتنفيذ هذه الاستراتيجية. وعلاوة على ذلك تم اصدار إطار لأمن المعلومات للقطاع المالي. وتم وضع تعاميم تغطي

المؤسسات المصرفية والشركات المالية وذلك استناداً على الأنظمة ذات العلاقة والتي تعطي المؤسسة الصلاحية.

- **بنك السودان المركزي:** تم إعداد دراسة عن المخاطر المحتملة وكيفية التعامل معها. ويتبنى بنك السودان المركزي المعيار ISO 27000 بالنسبة لأنظمة البنك الداخلية عبر قسم أمن المعلومات بالإدارة العامة لتقنية المعلومات أما بالنسبة لنظم الدفع والقطاع المصرفي فهذا يتم عبر التعاميم التي يصدرها البنك والمعايير التي يتم إلزام المصارف بها، ويوجد في السودان قانون المعاملات الإلكترونية للعام 2007 والأن يجرى تعديله لاستيعاب المستجدات الجديدة في الجريمة الإلكترونية والعابرة للحدود.

- **البنك المركزي العراقي:** قام البنك المركزي بإصدار وثيقة سياسة أمن المعلومات والبيانات لتجنب الاضرار الناتجة عن الاختراق أو الفيروسات، بالإضافة الى مجموعة من الاجراءات التقنية لحماية البيانات من الدخول غير المخول وتوفير بيئة امنة من الاختراقات من خلال منظومة حماية متطورة من الجيل الجديد من الجدران النارية وحجب المواقع والتطبيقات المخالفة لسياسة امن المعلومات والبيانات. كما أصدر البنك المركزي القوانين وتعاميم لحماية البيانات والانظمة المصرفية من خطر القرصة الالكترونية.

- **سلطة النقد الفلسطينية:** قامت سلطة النقد في فلسطين بإجراء دراسة حول مخاطر القرصنة الإلكترونية، لاسيما في ظل التطورات والابتكارات والتطبيقات في الصناعة المصرفية والتقنيات الإلكترونية الحديثة، وذلك طبقا لمتطلبات العمل التي تستلزم حماية المعلومات سواء كان ذلك في الخادمات او الشبكات او قاعدة البيانات. ويوجد إطار شامل لإدارة امن المعلومات مبني على المعايير العالمية وأهمها ISO 27000.

- **مصرف قطر المركزي:** يقوم المصرف المركزي بإصدار الإرشادات الأمنية والتعاميم اللازمة للقطاع المالي بشكل مستمر لأخذ الاحتياطات اللازمة من الهجمات الإلكترونية وحماية البيئة المالية. كما يجري العمل على إصدار استراتيجية موحده لأمن المعلومات للقطاع المالي وفقاً لأفضل المعايير الدولية، ويوجد فريق للإشراف على مدى التزام المؤسسات المالية بتنفيذ هذه الاستراتيجية. ويتم مراجعة الأنظمة بشكل دوري والتأكد من تطابقها مع السياسات والإجراءات الأمنية المطلوبة.

- **بنك الكويت المركزي**: قام البنك المركزي في الكويت بوضع نظام مراقبة دقيق مع آلية متابعة امن المعلومات ومكافحة القرصنة. كما قام البنك المركزي بالحث على عدم الرد على رسائل البريد الالكتروني التي تتطلب المعلومات الشخصية، كذلك عدم الدخول على الروابط المشبوهة، إلى جانب التأكيد على استخدام كلمات مرور قوية مع ضرورة تغييرها باستمرار حفاظا على السرية المصرفية.

- **مصرف لبنان:** أعطى مصرف لبنان أهمية كبيرة للعمليات المالية والمصرفية بالوسائل الإلكترونية، وشجع المصارف على اعتماد التكنولوجيا في العمل المصرفي. وأصدر كذلك عدداً من التعاميم المتعلقة بتنظيم العمليات المالية والمصرفية بالوسائل الإلكترونية وبطاقات الدفع، شدد فيها على أهمية توفير عناصر السرعة والأمان والسرية المصرفية، وعمل على اتخاذ إجراءات لحماية نظم المعلومات، وضمان سير التعاملات الإلكترونية واستمراريتها في بيئة تكنولوجية آمنة، كما قرر مصرف لبنان منع استعمال الـ Bitcoin والعملات الافتراضية الأخرى كوسيلة دفع.

- **البنك المركزي المصري:** قام البنك المركزي بدراسة حول مخاطر القرصنة الإلكترونية لاسيما في ظل التطورات والابتكارات والتطبيقات في الصناعة المصرفية والتقنيات الإلكترونية الحديثة حيث تشتمل القواعد الخاصة لكل من التطبيقات الحديثة التي يتم اطلاقها في القطاع المصرفي بقواعد الحماية والتأمين من مخاطر القرصنة. ويتم مراجعة الأنظمة بشكل دوري والتأكد من تطابقها مع السياسات

والإجراءات الأمنية المطلوبة. ومن إجراءات الوقاية التي قام بها البنك المركزي لحماية المعلومات دون المس بالسرية المصرفية هي تفعيل انشاء C-CERT الخاص بالقطاع المصرفي.

- **بنك المغرب:** يقوم بنك المغرب بتطوير مبدأ توجيهي يتعلق بالقدرة على صمود "الفضاء الإلكتروني" للبنية التحتية للأسواق المالية. ففيما يتعلق بأمن المعلومات، تم وضع العديد من التدابير التنظيمية والتقنية تتمثل بإجراء عمليات مراقبة دائمة لأمن نظم المعلومات وتصنيف نظم المعلومات وتنفيذ توصيات الهيئات والسلطات الوطنية والدولية. كما تم إبرام اتفاقية تنسيق بين بنك المغرب والإدارة العامة المغربية لأمن نظم المعلومات بشأن أمن الفضاء الإلكتروني. كذلك يتم إدارة الحوادث الأمنية الإلكترونية وتنسيقها على المستوى الوطني من طرف الإدارة العامة المغربية لأمن نظم المعلومات من خلال خلية متخصصة في هذا الشأن.

خامساً: الخلاصة

بناءً على ما تقدم، تتطلب التدابير المضادة المنطقية التي يتعين اعتمادها لمكافحة الجرائم المالية الالكترونية جهداً وتعاون عالمياً. ولا بد من متابعة وملاحقة مرتكبي الجرائم الإلكترونية. يتطلب الحد من انتشار الجرائم ومكافحتها بشكل فعال تعاون فعال على الصعيد المحلي والإقليمي والدولي.

في هذا الإطار، تؤكد اللجنة العربية لنظم الدفع والتسوية على أهمية إدخال التقنيات الحديثة في مجال أمن الشبكات الإلكترونية لمواجهة مخاطر التجاوز على الشبكة الإلكترونية من قبل القراصنة لما يساهم في تحقيق أمن مقبول لتعاملات الزبائن مع المصارف. كما تؤكد اللجنة على أهمية تعزيز الوعي في هذا الشأن.

سلسلة الكتيبات الصادرة عن
أمانة مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

1. التوجهات الدولية والإجراءات والجهود العربية لمكافحة غسل الأموال – 2002.
2. قضايا ومواضيع في الرقابة المصرفية – 2002.
3. تجربة السودان في مجال السياسة النقدية – 2003.
4. تطورات السياسة النقدية في جمهورية مصر العربية – 2003.
5. الوضعية النقدية وسير السياسة النقدية في الجزائر – 2003.
6. تطوير أسواق الأوراق المالية الحكومية في الدول العربية ودور السلطات النقدية- 2004.
7. الملامح الأساسية لاتفاق بازل II والدول النامية – 2004.
8. تجربة السياسة النقدية في المملكة المغربية -2004.
9. إدارة المخاطر التشغيلية وكيفية احتساب المتطلبات الرأسمالية لها – 2004.
10. التقييم الداخلي للمخاطر الائتمانية وفقاً لمتطلبات (بازل II) – 2005.
11. تجربة السياسة النقدية وإصلاح القطاع المصرفي في الجمهورية اليمنية– 2005.
12. ضوابط عمليات الإسناد الخارجي للمؤسسات المصرفية – 2005.
13. مراقبة الامتثال للقوانين والتعليمات في المصارف – 2005.
14. أنظمة تحويلات العاملين – قضايا وتوجهات – 2005.
15. المبادئ الأساسية لنظم الدفع الهامة نظامياً ومسؤوليات المصارف المركزية – 2006.
16. الدعامة الثالثة لاتفاق (بازلII) " انضباط السوق " – 2006.
17. تجربة مؤسسات نقد البحرين كجهاز رقابي موحد – 2006.
18. ترتيبات الإعداد لتطبيق مقترح كفاية رأس المال (بازل II) – 2006.
19. PAYMENTS AND SECURITIES CLEARANCE AND SETTLEMENT SYSTEM IN EGYPT-2007
20. مصطلحات نظم الدفع والتسوية – 2007.
21. ملامح السياسة النقدية في العراق – 2007.

22. تجربة تونس في مجال السياسة النقدية والتوجهات المستقبلية – 2007.
23. الدعامة الثانية لاتفاق بازل II – المراجعة الرقابية 2007.
24. ضوابط العلاقة بين السلطات الرقابية في الدولة الأم والدول المضيفة – 2007.
25. الإرشادات العامة لتطوير نظم الدفع والتسوية – 2007.
26. تطوير أنظمة الاستعلام الائتماني ومركزيات المخاطر – 2008.
27. استمرارية الأعمال في مواجهة الطوارئ – 2008.
28. نظم الدفع الخاصة بعرض وسداد الفواتير الكترونياً – 2008.
29. مبادئ الإشراف على أنظمة الدفع والتسوية ومسؤوليات المصارف المركزية- 2008.
30. مقاصة الشيكات في الدول العربية – 2008.
31. برنامج إصلاح إدارة سوق الصرف والسياسة النقدية في مصر – 2008.
32. Information Sharing and Credit Reporting System in Lebanon
33. أنظمة الإنذار المبكر للمؤسسات المالية – 2009.
34. تنميط أرقام الحسابات المصرفية – 2009.
35. التمويل متناهي الصغر ودور البنوك المركزية في الرقابة والإشراف عليه – 2009.
36. برنامج الاستقرار المالي لمواجهة تداعيات الأزمة المالية في دولة الكويت – 2009.
37. تطوير السياسة النقدية والمصرفية في ليبيا 2010.
38. Information Sharing and Credit Reporting System in Syria-2010
39. Information Sharing and Credit Reporting System in Yemen-2010
40. Information Sharing and Credit Reporting System in Oman-2010
41. Information Sharing and Credit Reporting System in Tunisia-2010
42. مبادئ إدارة مخاطر الائتمان - 2011.
43. قواعد ممارسات منح المكافآت المالية - 2011.
44. الإدارة السليمة لمخاطر السيولة والرقابة عليها - 2011.
45. إطار ربط محولات الدفع الوطنية في الدول العربية - 2011.
46. الإطار القانوني لنظم الدفع وتسوية الأوراق المالية - 2012.

47. تجربة البنك المركزي التونسي في التعامل مع التداعيات الاقتصادية للتطورات السياسية الأخيرة - 2012.
48. السياسات النقدية والمصرفية لمصرف قطر المركزي في مواجهة تداعيات الأزمة العالمية - 2012.
49. توسيع فرص الوصول للتمويل والخدمات المالية في الدول العربية ودور المصارف المركزية - 2013.
50. مبادئ اختبارات الجهد للمؤسسات المصرفية - 2013.
51. نظم الدفع عبر الهاتف المحمول- الأبعاد والقواعد المطلوبة - 2013.
52. تجربة بنك المغرب في مجال تعزيز الولوج إلى الخدمات المالية - 2013.
53. قضايا تطوير نظم الحفظ المركزي للأوراق المالية ودور المصارف المركزية.
54. أهمية ودور مجلس المدفوعات الوطني – تجارب الدول العربية.
55. حماية المستهلك (العميل) في الخدمات المصرفية.
56. مبادئ حوكمة المؤسسات المصرفية.
57. التجربة الفلسطينية في مجال تطوير البنية التحتية للقطاع المالي والمصرفي.
58. الترجمة العربية للمبادئ الأساسية للرقابة المصرفية الفعّالة – 2014.
59. التعامل مع المؤسسات المصرفية ذات المخاطر النظامية محلياً ودور المصارف المركزية – 2014.
60. الرقابة على صيرفة الظل – 2014.
61. تطبيق آلية الوسيط المركزي لتسوية معاملات الأسواق المالية – تجربة بنك المغرب – 2014.
62. مبادئ البنية التحتية لأسواق المال وإطار الإفصاح ومنهجية التقييم لهذه المبادئ – 2014.
63. إصلاح القطاع المصرفي والاستقرار المالي في الجزائر – 2014.
64. قاموس مصطلحات الرقابة المصرفية – 2015.
65. المستجدات الرقابية في مكافحة عمليات غسل الأموال وتمويل الإرهاب وأهمية الاستعداد للجولة الثانية من عملية التقييم المتبادل – 2015.
66. التعامل مع مخاطر التعرضات الكبيرة وتجارب الدول العربية – 2015.

67. العلاقة المتداخلة بين الاستقرار المالي والشمول المالي – 2015.
68. متطلبات تبني استراتيجية وطنية شاملة لتعزيز الشمول المالي في الدول العربية – 2015.
69. متطلبات رأس المال الإضافي للحد من مخاطر التقلبات في دورات الأعمال ومنح الائتمان – 2015.
70. احتياجات الارتقاء بنظم الدفع صغيرة القيمة – 2015.
71. المعايير الدولية للتقارير المالية وانعكاساتها على الرقابة المصرفية – تطبيق المعيار رقم تسعة – 2017.
72. سلامة وأمن المعلومات المصرفية الإلكترونية – 2017.
73. مبادئ حوكمة المؤسسات المصرفية (ورقة محدثة) – 2017.
74. Financial Inclusion Measurement in the Arab World.
75. تطوير خدمات نظم الاستعلام والتصنيف الائتماني لقطاع المنشآت الصغيرة والمتوسطة في الدول العربية – 2017.
76. Financial Education Initiatives in the Arab Region.
77. نشرة تعريفية بمفاهيم الشمول المالي – 2017.
78. كتيب تعريفي بمجلس محافظي المصارف المركزية ومؤسسات النقد العربية – 2016.
79. إدارة مخاطر السيولة في نظم الدفع والتسوية اللحظية – تجربة مؤسسة النقد العربي السعودي – 2017.
80. الإطار القانوني لحماية مستهلكي الخدمات المالية – 2017.
81. توافق السياسات الاحترازية والسياسات الاقتصادية الكلية – 2017.
82. Payment and Securities Settlement Systems in Lebanon- 2017
83. المعالجة الرقابية لمخاطر الديون السيادية – 2018.
84. الإطار الإشرافي لمخاطر الائتمان والمحاسبة لخسائر الائتمان المتوقعة – 2018.
85. قضايا الإسناد الخارجي في الخدمات المالية والمصرفية – 2018.
86. التطورات الرقابية في الدول العربية وتنفيذ متطلبات بازل III – 2018.
87. Regulatory Developments and Basel II Implementation in the Arab Region in 2018.

88. De-Risking and Financial Inclusion: Global trends and thoughts for policy debate for the Arab region – 2018.

89. العلاقة بين إجراءات البنوك المراسلة العالمية والشمول المالي – 2018.

90. المنهجيات الحديثة لاختبارات الأوضاع الضاغطة – 2018.

91. الإطار العام للاستقرار المالي وإدارة المخاطر العابرة للحدود – 2018.

92. دور المعلومات الائتمانية في الحد من مخاطر الإفراط في الاستدانة – 2018.

93. تطبيق مبادئ إدارة التعثر في إطار مبادئ البنية التحتية المالية – 2018.

94. الإطار الرقابي للقيم المخزنة وعمليات الدفع الإلكتروني – تجربة مصرف الإمارات المركزي – 2018.

95. إدارة مخاطر السيولة وفق متطلبات بازل III في الدول العربية.

96. تحديد وإدارة مخاطر دعم الشركات المرتبطة.

97. الإجراءات الرقابية والإشرافية للتعامل مع البنوك الضعيفة.

98. تطبيق صافي التمويل المستقر (NSFR) وفقاً لبازل III.

99. تمكين المرأة مالياً ومصرفياً.

100. استخدام أدوات الدفع الإلكترونية لتعزيز الشمول المالي.

101. تحفيز البنوك لتمويل الشركات الناشئة – تجربة مصرف لبنان.

102. الثورة الرقمية وتداعياتها على النظام المصرفي والاستقرار المالي: مخاطر الابتكارات المالية.

103. متطلبات إصدار مؤشر محلي للاستقرار المالي في الدول العربية – تجربة المملكة الأردنية الهاشمية.

104. مخاطر الجرائم المالية الإلكترونية وآثارها على نظم الدفع.

105. تطبيقات التحويلات الفورية في المدفوعات الصغيرة.

106. قضايا تطبيق الشيك والتوقيع الإلكتروني.

107. إرشادات حول حقوق مستخدمي خدمات الاستعلام الائتماني.

108. استخدام المعلومات الائتمانية لأغراض الإشراف والرقابة في الدول العربية.

للحصول على مطبوعات صندوق النقد العربي

يرجى الاتصال بالعنوان التالي:

صندوق النقد العربي

ص.ب. 2818

أبوظبي - الإمارات العربية المتحدة

هاتف رقم: 6215000 (9712+)

فاكس رقم: 6326454 (9712+)

البريد الإلكتروني: centralmail@amfad.org.ae

موقع الصندوق على الإنترنت: http://www.amf.org.ae

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors