البنك المركزي السعودي
SAMA
Saudi Central Bank

ابرز احصاءات أساليب الاحتيال المالي لعام 2021م

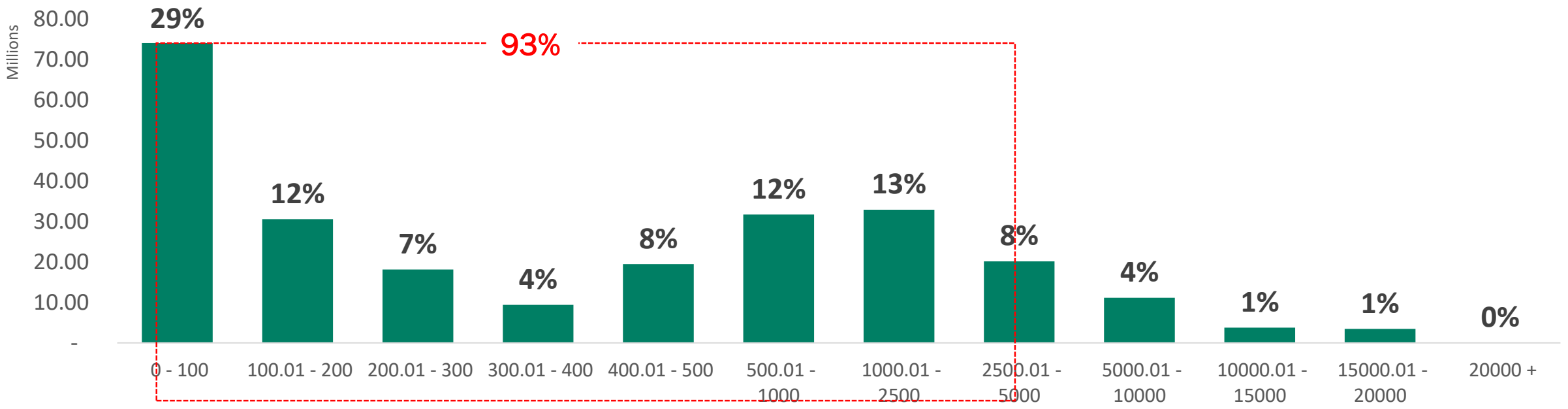
البنك المركزي السعودي

ابريل 2022

SARIE (IPS)

Sarie Transfers Distributions over value slabs

Feb21 – March22



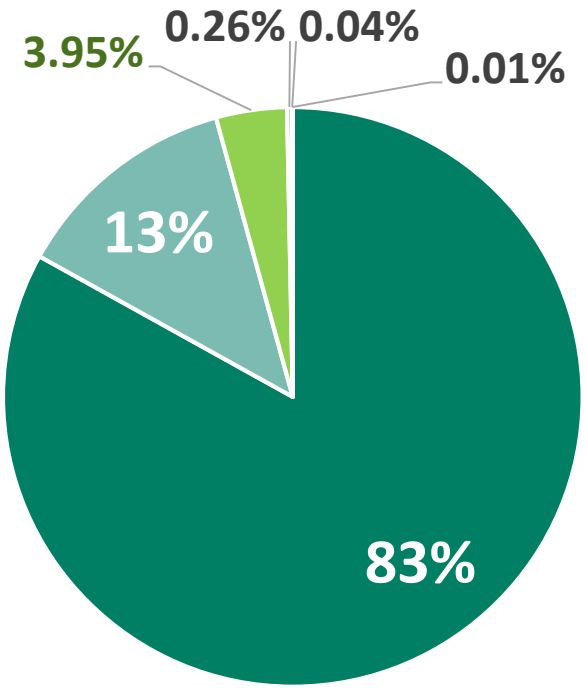
93% of transfers are low value transfers (below 5000 SAR)

2% of transfers are high value transfers (above 10k SAR)

SARIE (IPS)

Accounts Daily Frequency of Transfers

(Sep 2021 – March 2022)



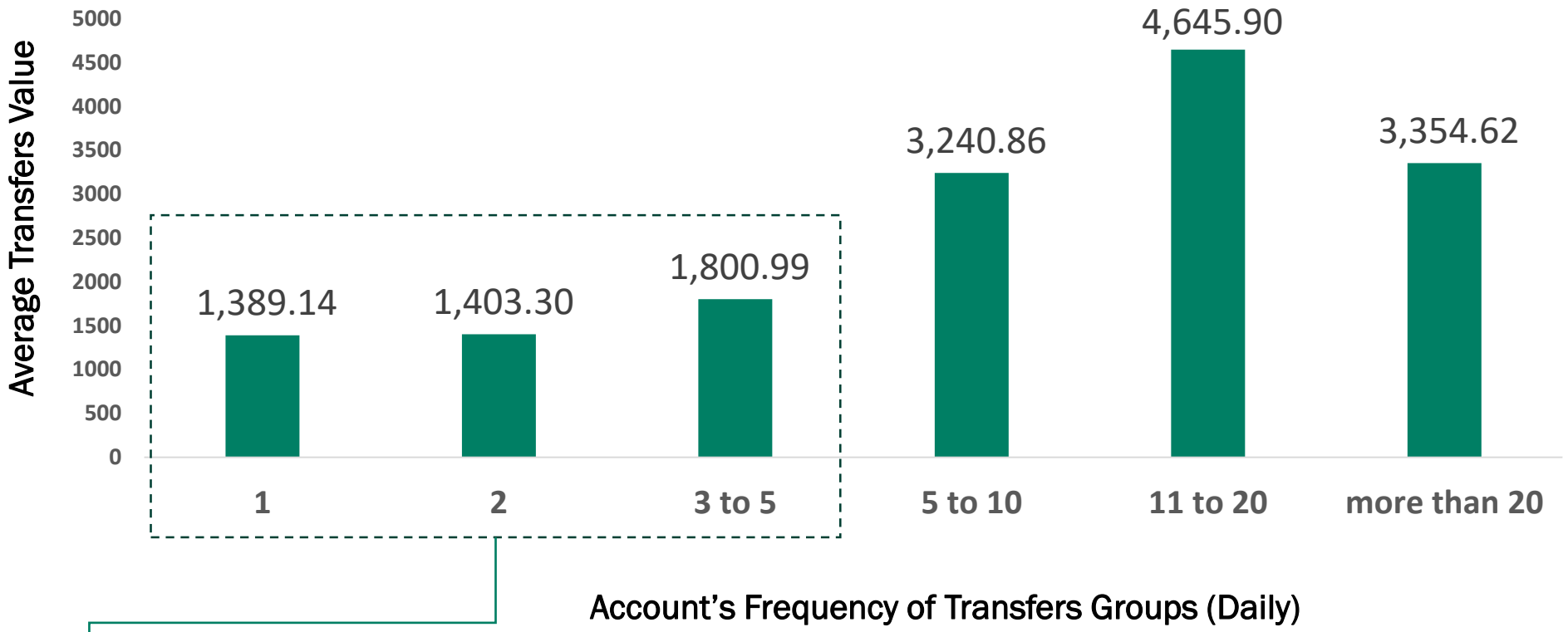
Accounts Frequency of Transfers Groups		Transfers Value
1		150B (60%)
2	During payroll days this group share increase to (18%)	46B (19%)
3 to 5	During payroll days this group share increase to (8% - 9%)	31B (13%)
5 to 10		8B (3%)
11 to 20		3B (1%)
more than 20		3B (1%)

99% of Accounts perform <u>from (1-5) transfers per day</u>

SARIE (IPS)

Average Transfers Value by Account's Daily Frequency of Transfers Groups

September 2021 – March 2022



The average transfers values of the highlighted groups (1 to 5 daily transfers) are within the same range

نبذة عن الاحتيال المالي

نظراً للتطور الكبير والسريع في الخدمات المالية التي تقدمها البنوك عبر القنوات التقليدية والإلكترونية، ازدادت عمليات الاحتيال المالي وتعددت أساليبها وطرقها وتتجدد بين فترة وأخرى وتتخذ أشكالًا وصورًا متغيرة، وهدفها الرئيسي الكسب المالي الغير مشروع، ومن أبرز أساليب عمليات الاحتيال المصرفي هي:

انتحال الشخصية

استخدام أساليب مخادعة لعملاء البنوك من خلال انتحال شخصية (كموظف البنك) واستدراج العميل للحصول على البيانات البنكية

التوظيف الوهمي

استدراج الضحايا عن طريق إعلانات عمل وهمية من خلال شبكات التوظيف واستخدام حسابتهم البنكية لتجميع الأموال الناتجة من عمليات احتيال وتحويلها خارج المملكة

مدارس تعليم القيادة

استدراج المتدربات من خلال انتحال مواقع إلكترونية لمدارس تعليم القيادة للحصول على بيانات الدخول على منصة أبشر وفتح حسابات بنكية دون علمهم واستخدامها في تجميع الأموال الناتجة من عمليات الاحتيال

الاستثمار الوهمي

استخدام مواقع وإعلانات إلكترونية للاستثمار الوهمي مستغلة أسماء جهات أو صناديق حكومية أو مشاهير لإيهام الضحايا بالاستثمار والربح السريع ومن ثم الحصول على المبالغ

صفحات أو منصات إلكترونية وهمية

انتحال منصات إلكترونية لبيع سلع او تقديم خدمات ونحوه بغرض الحصول على بيانات الدخول على الحساب البنكي أو بيانات البطاقة

استغلال الصلاحيات (Internal Fraud):

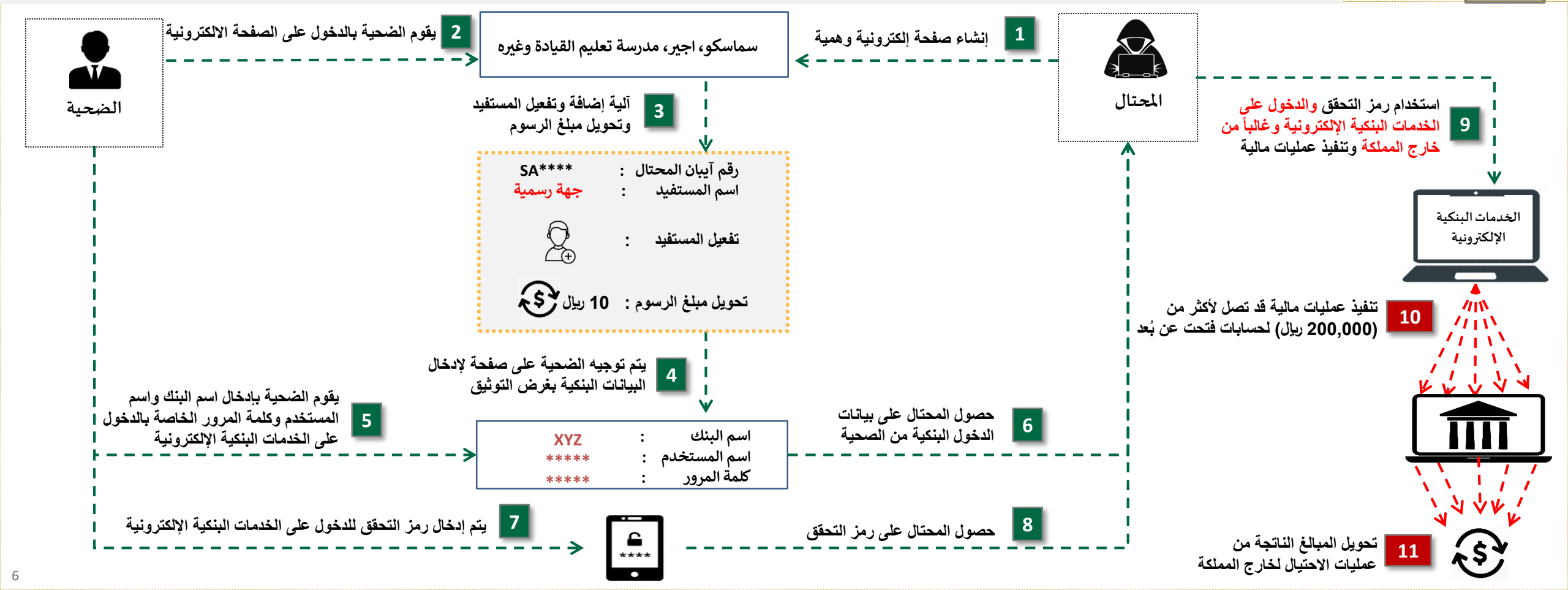
استغلال الصلاحيات في اصدار بطاقات ائتمانية بحد ائتماني عالي أو الحصول على قروض تمويلية وغيرها.

أساليب الاحتيال (مثال)

صفحات ومنصات إلكترونية وهمية

الأساليب المتبعة:

رصد مؤخرا ازدياد في عمليات الاحتيال من خلال انتحال منصات لبيع سلع أو تقديم خدمات تحمل أسماء وهويات جهات رسمية بغرض الحصول على بيانات الدخول على الخدمات البنكية الإلكترونية. وأدناه احد أشهر الأساليب المرصودة :



أبرز التحديات التي ساهمت في ازدياد حالات الاحتيال المالي

- **4,844,564** حساب فُتح عن بُعد دون التحقق من تطابق رقم هوية العميل مع رقم الهوية المستخدم في الجوال، وتشكل بنسبه (55%) من مجموع الحسابات التي فُتحت عن بعُد
- ضعف في أنظمة مراقبة العمليات مما خلق تحدي في اكتشاف والحد من حالات الاحتيال بشكل مبكر
- عدم الاستثمار الكافي في البنية التحتية لأنظمة مكافحة الاحتيال باستخدام الذكاء الاصطناعي ودارسة سلوك العميل
- عدم وجود إجراءات للتحقق من تطابق رقم الآيبان واسم المستفيد
- قصور شديد في تتبع الأموال الناتجة من عمليات الاحتيال لإيقافها قبل خروجها خارج المملكة
- ضعف في إجراءات وآليات تلقي بلاغات الاحتيال والتعامل معها من حيث الرصد والتحقيقات والتقارير
- وجود ضعف في حصر أنواع وأساليب وأعداد واحجام كافة حالات الاحتيال، بما فيها بيانات الضحية والمستفيد من عمليات الاحتيال
- نقص في الكوادر المؤهلة في وحدات مكافحة الاحتيال المالي
- ضعف كفاءة برامج توعوية العملاء من حيث المادة والقنوات المستخدمة، ووضع مؤشرات قياس مدى فاعليتها

التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي والتي يتوجب على البنوك تطبيقها خلال 5 أيام عمل

التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
1. الخدمات الإلكترونية	1.1 عدم تفعيل الخدمات البنكية للحسابات الجديدة التي يتم فتحها عن بُعد ويتوجب على العميل استكمال تفعيل الحساب عن طريق الفرع او الخدمات الذاتية بالبصمة لتفعيل استخدام الخدمات البنكية، وعدم اتاحة الخدمة لغير المواطنين 1.2 تطبيق أكثر من معيار للتحقق من الهوية عند طلب (تأسيس الخدمات الإلكترونية، تغير كلمة المرور، إصدار وتفعيل البطاقات (مدى أو ائتمانيه وغيره)، وتأكيد الطلب عبر قناة أخرى (على سبيل المثال: الاتصال الهاتفي) 1.3 تطبيق متطلبات إضافة وتفعيل المستفيد على التحويلات المالية للمحافظ الإلكترونية بأي طريقة كانت 1.4 تطبيق أكثر من معيار من معايير التحقق (Multi Factor Authentication) لكل عملية تحويل مالية للعملاء المضافين مسبقًا 1.5 يتوجب على العملاء أدخال الرقم السري المؤقت (OTP) يدوياً وايقاف خاصية التعبئة المباشرة (auto fill)

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
2. الحوالات المالية	تعديل سقف مجموع المبالغ لعمليات التحويل حسب الاتي: 2.1 الحسابات المفتوحة عن طريق الفروع / او موثقة عن طريق الفروع يتم : - وضع إجراءات احترازية على عمليات التحويل وتعليق الحوالات لمدة ساعة على الأقل قبل تنفيذها من البنك المصدر عبر نظام RTGS - يكون اجمالي مبالغ الحوالات اليومية عبر نظام (IPS) بحدود مالية يحددها البنك المركزي على سبيل المثال (40,000) ريال كحد أعلى 2.2 الحسابات المفتوحة عن بُعد سابقاً بحيث يكون اجمالي مبالغ الحوالات اليومية لأنظمة المدفوعات (20,000) ريال كحد أعلى 2.3 تطبيق آلية إضافة وتفعيل المستفيد باستخدام قناة أخرى على جميع أنواع الحوالات المالية

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
3. الحوالات الدولية	3.1 عند إضافة مستفيد دولي من الحسابات المملوكة لمقيم، يكون التفعيل عن طريق الفرع أو أجهزة الخدمة الذاتية (بالبصمة) 3.2 تعليق الحوالات الدولية المنفذة عن طريق القنوات الإلكترونية لمدة 24 ساعة إذا كانت للمرة الأولى، ولمدة ساعتين على الاقل للحوالات التالية لنفس المستفيد، وذلك للدول عالية المخاطر 3.3 عدم السماح للحسابات المفتوحة عن بعُد سابقاً ولم يتم توثيقها بإجراء عمليات تحويل دولية

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
4. الحسابات التي تم فتحها عن بُعد سابقاً	4.1 فيما يخص الحسابات المفتوحة عن بُعد سابقاً وتم من خلالها الاستفادة من منتجات بنكية مثل (ربط الراتب، تمويلات، وغيرها)، على البنك أن يضع آلية لتوثيق الحساب إما عن طريق الفرع او الخدمة الذاتية، وأن يتحمل المخاطر الناتجة عن عدم توثيق الحساب 4.2 تقليل مبلغ العمليات الشرائية للحسابات الغير موثقة والمفتوحة سابقاً (20,000) ريال يومياً، وفي حالة الظروف الخاصة على سبيل المثال تواجد العميل خارج المملكة، يمكن للبنك وضع آلية لتوثيق الحساب ورفع الحد على أن يتحمل البنك المخاطر الناتجة عن ذلك

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
5. مراقبة العمليات	5.1 وضع التدابير الاحترازية لإيقاف أو استعادة الحوالات المالية الدولية الإلكترونية بعد تنفيذها من قبل العميل (Remittance)، أخذًا في الاعتبار سلوك العميل في الحوالات الدولية والدول المرسل إليها تلك المبالغ. 5.2 عدم السماح للعملاء بتنفيذ عمليات مالية عند دخول العملاء للحسابات من خلال خاصية السمات الحيوية أو خاصية (M-PIN)، وأن تكون تلك الخدمات للاستعراض فقط دون إجراء عمليات مالية حسب متطلبات البنك المركزي. وفي حال رغبة العميل تنفيذ عمليات مالية يتوجب تطبيق أكثر من معيار من معايير التحقق من الهوية (OTP) لكل عملية مالية، وتطبيق الإجراءات النظامية حيال العمليات المالية. 5.3 عمل مراجعة شاملة للتأكد من عدم وجود أي ثغرات تقنية أو إجرائية تؤدي إلى إظهار أي معلومة حساسة عن العميل (على سبيل المثال: رقم البطاقة البنكية، قائمة البطاقات) 5.4 التحقق من جميع إصدارات تطبيق البنك/المصرف، وعدم وجود أي ثغرات سيبرانية أو تقنية أو إجرائية، وعدم السماح بالدخول للخدمات الإلكترونية من الأجهزة المعدلة (على سبيل المثال: Jailbreak). 5.5 عند دخول العملاء عبر خدمة الهاتف المصرفي، أن تطبق أكثر من معيار من معايير التحقق من الهوية، أخذًا في الاعتبار إمكانية البنك من التعرف على رقم الاتصال ما إذا كان اتصال من رقم حقيقي أو من رقم انتحالي لرقم العميل (Spoofing Caller Ids).

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
6. ضوابط عامة	6.1 إبلاغ العملاء في حال ترقية الحساب إلى فئة أعلى، وأخذ الموافقة على رفع الحدود المالية للعمليات. كما يجب وضع الخيار للعملاء على نحو واضح في حال الرغبة بتقليل الحد اليومي للعمليات المالية. وفي حال رغبة العميل إعادة رفع الحد اليومي، يجب على البنوك استخدام أكثر من معيار من معايير التحقق من الهوية، بالإضافة إلى وضع تدابير آمنة للتحقق تتضمن استخدام قناة أخرى غير المستخدمة في عملية طلب تغيير الحد (على سبيل المثال الاتصال الهاتفي، جهاز الصراف الآلي، الفرع، ...إلخ)، على ألا يتجاوز الحد اليومي لفئة العميل المحددة من قبل البنك مع إرسال رسائل إشعار فورية للعملاء وتحديد وقت يحدده البنك لتفعيل الطلب 6.2 تطبيق الحدود اليومية على الحسابات بما فيها الحسابات الفرعية على سبيل المثال: إذا كان الحد الأعلى للحساب 100,000ريال فأنه يشمل الحسابات الرئيسية والفرعية أي مجموعها لا يتجاوز 100,000 ريال 6.3 تحديد الغرض من جميع أنواع رسائل التحقق (OTP) بشكل واضح وصريح، بما في ذلك عمليات التجارة الإلكترونية، وأن تشمل الغرض، والمبلغ، واسم المتجر حسب قوالب الإشعارات المعتمدة. 6.4 التأكيد على تطبيق خدمة تحقق لجميع الحسابات البنكية حسب التعليمات الصادرة سابقاً 6.5 إشعار العملاء بعمليات تسجيل الدخول التي تتم على الحساب في حال تم تسجيل الدخول من جهاز جديد.

يتبع - التعليمات والإجراءات العاجلة لمكافحة الاحتيال المالي

الموضوع	الإجراءات
7. بلاغات الاحتيال	7.1 وضع إجراءات داخلية فعالة تضمن سرعة التجاوب مع حالات الاحتيال بعد اكتشافها أو بعد شكوى العميل، على أن تشمل جميع الإدارات ذات العلاقة وعلى مدار (24/7). 7.2 وضع إجراءات فعالة وسريعة على مدار (24/7) للتجاوب مع حالات الاحتيال الواردة من البنوك الأخرى، وأن تشمل إجراءات احترازية لتجميد المبالغ المعترض عليها إلى حين التحقق من سلامة مصدرها، وحوكمة تلك الإجراءات. كما يتعين أن تكون ضمن نطاق المراجعة الداخلية لإجراء التقييمات على تطبيق الإجراءات المعتمدة من البنك على نحو دوري. 7.3 دراسة جميع شكاوى العملاء والتي يشتبه بها حالات احتيال وتحليل الأساليب المستخدمة في عمليات الاحتيال وإضافتها في أنظمة مكافحة الاحتيال 7.4 حصر وتحليل كافة أنواع وأساليب وأحجام وأعداد حالات الاحتيال المالي بما فيها بيانات الضحايا والمستفيدين من الأموال الناتجة من عمليات الاحتيال وحفظها في قواعد بيانات وحدة مكافحة الاحتيال المالي 7.5 عند إبلاغ العميل البنك عن التعرض لحالة احتيال ، يتوجب على البنك/ المصرف إيقاف كافة الخدمات المرتبطة بالحساب وجميع القنوات بشكل فوري. وعلى البنك بذل العناية الواجبة للتحقق من هوية العميل قبل إعادة تفعيل الخدمات، وعكس حالات بطاقات مدى والبطاقات الائتمانية ومزامنتها (تاريخ الصلاحية، الحالة، ...إلخ) مع البطاقات المضافة على المحافظ الإلكترونية (مثل Apple Pay) 7.6 تزويد البنوك الاخرى وكذلك الجهات ذات العلاقة بالمواقع والإعلانات الوهمية التي تنتحل أسماء وهويات الجهات الحكومية والخاصة أو شخصيات معرفة بما فيها الحسابات في شبكات التواصل الاجتماعي والأساليب الحديثة عبر لجنة مكافحة الاحتيال المالي بين البنوك

تعليمات وإجراءات مكافحة الاحتيال المالي والتي يتوجب على البنوك تسليم خطة للتطبيق خلال 5 أيام عمل على أن يكون التطبيق خلال شهرين

التعليمات والإجراءات متوسطة المدى

الموضوع	الإجراءات
1.الاستثمار في البنى التحتية	1.1 الاستثمار في البنى التحتية والأنظمة المتقدمة الخاصة بمكافحة الاحتيال المالي، وأن تكون هناك تدابير احترازية كافية وفعالة للتأكد من هوية العميل لتمكينه من إجراء العمليات المالية، مع الأخذ في الاعتبار دراسة سلوك العميل سواءً في العمليات المالية أو ما يتعلق بسلوك العميل في آلية الدخول للخدمات الإلكترونية، وتطوير أنماط وسيناريوهات شاملة وفعالة (Use Cases) لاكتشاف العمليات المشبوهة، ووضع تدابير احترازية للحد من عمليات الاحتيال، على أن يتم تحديث تلك الأنماط والسيناريوهات على نحو دوري أخذًا في الاعتبار أنماط وسيناريوهات الاحتيال المتجددة، ومن ذلك –على سبيل المثال لا الحصر– الآتي: • عند تسجيل الدخول من عدة مناطق جغرافية مختلفة في مدة زمنية قصيرة. • عند تسجيل الدخول من جهاز غير الجهاز الذي يستخدمه العميل. • عند تغيير الرقم السري أو رقم الجوال وتتبعها محاولات إجراء عمليات مالية. • اختلاف سلوك العميل في طريقة كتابة الرقم السري. • تحليل سلوك العميل من ناحية العمليات المالية في حال إجراء عدد من الحوالات المالية في وقت قصير كنتيجة لحوالات مالية واردة لنفس الحساب. • تحليل سلوك العميل من ناحية العمليات المالية التي تتم على حساب العميل وفق حد العمليات اليومي، على أن يتضمن ذلك الحوالات الداخلية والمحلية والخارجية، وربط العمليات المالية بجميع حسابات العملاء والقنوات البنكية المستخدمة من قبلهم، وبحسب سلوك العميل المالي في العمليات المالية (Consumer behavior)، على أن تشمل التدابير العملاء المضافين والمعرفين مسبقًا. • تطوير أنماط وسيناريوهات شاملة ومفصلة للكشف عن عمليات الاحتيال، واتخاذ الإجراءات اللازمة في شأنها، وقياس فعاليتها وتحديثها على نحو دوري.

يتبع - التعليمات والإجراءات متوسطة المدى

الموضوع	الإجراءات
2. تصحيح الحسابات المفتوحة عن بُعد سابقاً	2.1 يتعين على البنك وضع خطة تصحيحية لإجراء التصحيح للحسابات المفتوحة عن بُعد سابقاً وتوثيقها عن طريق الفروع أو أجهزة البنوك الذاتية (بالبصمة) خلال مدة لا تتجاوز شهر

يتبع - التعليمات والإجراءات متوسطة المدى

الموضوع	الإجراءات
3. برامج التدريب والتوعية	3.1 تأهيل وتدريب الكوادر البشرية والصفوف الأمامية لخدمة العملاء على حالات الاحتيال المستحدثة وتطورات عمليات التصيد الاجتماعي، وتزويدهم بالصلاحيات اللازمة لاتخاذ إجراءات إيقاف وتعليق الخدمات البنكية والمصرفية وفق حوكمة تعتمد من البنك. كما يجب عمل العناية الواجبة للوقوف على كل عملية إيقاف أو تعليق الخدمات للعملاء للتحقق من عدم إساءة استخدام الصلاحيات فيما يضر مصلحة العملاء. 3.2 القيام ببرامج توعوية فعالة ومستمرة لغرض توعية العملاء عن أساليب الاحتيال المالي والسيبراني المتجددة، وتكون بطرق مبتكرة وحديثة بعيدًا عن الطرق التقليدية، ويكون لهذه البرامج مؤشرات أداء تقيس فاعليتها. وللبنوك أن تنظم حملات توعوية مشتركة فيما بينها لتحقيق الوعي في عمليات الاحتيال المالي


البنك المركزي السعودي
SAMA
Saudi Central Bank