الدليل الإرشادي

مكافحة الاحتيال المالي

في نظام المدفوعات الوطني

البنك المركزي الأردني
دائرة الإشراف والرقابة على نظام المدفوعات الوطني
أيـــار، 2023

تم إعداد هذا الدليل بعنوان "مكافحة الاحتيال المالي في نظام المدفوعات الوطني" من قبل قسم الدراسات والسياسات/ دائرة الإشراف والرقابة على نظام المدفوعات الوطني في البنك المركزي الأردني، حيث أعده م. إيمان بني عطية/ أخصائي الدراسات والسياسات، وفي التحرير والمراجعة والإشراف إبراهيم الرمضان رئيس قسم الدراسات والسياسات. كما تم مشاركة وعرض هذا الدليل لغايات التشاور على كل من لجنة مراقبة الامتثال في شركات الدفع والتحويل الإلكتروني للأموال، ولجنة متابعة حالات الاحتيال المالي في القطاع المالي، وأيضًا على جميع البنوك العاملة في المملكة بالتعاون والتنسيق مع جمعية البنوك الأردنية.

البنك المركزي الأردني
دائرة الإشراف والرقابة على نظام المدفوعات الوطني
قسم الدراسات والسياسات
هاتف: 0096264630301
فاكس: 0096264600521
ص. ب 37 عمان 11118 الأردن
الموقع الالكتروني: www.cbj.gov.jo
البريد الالكتروني: studies.oversight@cbj.gov.jo

المحتويات

مقدمة	3
الهدف من الدليل الإرشادي	4
الإطار التشريعي	5
نطاق التطبيق	6
أولاً: مدخل إلى الاحتيال المالي	7
مفهوم الاحتيال المالي	7
أبرز أشكال الاحتيال المالي	8
ثانياً: إطار الحاكمية المؤسسية	11
مجلس الإدارة	12
لجنة مكافحة الاحتيال المالي	14
الإدارة التنفيذية العليا	16
وحدة مكافحة الاحتيال المالي	17
ثالثًا: إدارة مخاطر الاحتيال المالي	22
سياسة مكافحة الاحتيال المالي	23
تقييم مخاطر الاحتيال المالي	25
إجراءات الرقابة الداخلية	30
الإبلاغ عن الاحتيال المالي	45
التحقيق في عمليات الاحتيال المالي	47
معالجة حالات الاحتيال المالي	49
نشر التوعية والتثقيف	51
ملحق (1): أمثلة على أبرز حالات الاحتيال المالي في نظام المدفوعات الوطني	53
ملحق (2): إرشادات عامة للعملاء للحماية من مخاطر الاحتيال المالي	58

مقدمــة:

اتســمت العقود الأخيرة بتنامي التطور التكنولوجي، وتســارع الابتكارات التقنية التي تســتهدف جميع نواحي الحياة ومنها الاقتصــادية، حيث ازداد اعتماد المؤسـسـات المالية على التكنولوجيا وابتكاراتها في تقديم خدماتها ومنتجاتها المالية والمصـــرفية، وفق نماذج أعمال جديدة قائمة على منصـــات الانترنت وتطبيقات الهواتف النقالة، ما فتح المجال أمامها لتقديم فرص عمل هائلة خصـوصـًا للمؤسـسـات الناشـئة، ومنها إنشـاء علاقة العمل أو العلاقة المصرفية مع العملاء إلكترونيًا، بالتالي التوسع في نطاق أعمالها والمساهمة في خلق بيئة تنافسية كبيرة في أسواقها.

ومع تزايد اعتماد المؤسـســـات المالية على الوســـائل الإلكترونية في قبول العملاء وتقديم الخدمات والمنتجات المالية والمصـرفية لهم، تزايد انتشـار الجرائم المالية الإلكترونية، وباتت هذه الجرائم تشـكل تهديدًا قويًا للمؤسسات المالية، من حيث الخسائر المالية التي تتكبدها أو مخاطر أمن المعلومات وسرقتها أو المخاطر التشـغيلية المرتبطة بالهجمات الإلكترونية من حيث إيقاف عمل أنظمة المؤسـسـة المالية وحجب خدماتها عن العملاء، إلى جانب المخاطر الأخرى التي تشـكلها هذه الجرائم كمخاطر السـمعة والمخاطر القانونية التي قد تنشأ عن ذلك.

وقد تتعرض المؤسسات المالية لمخاطر جديدة جراء اعتماد واستخدام التقنيات الحديثة وابتكاراتها، بعيداً عن الاسـتخدام غير المدروس وغير المحكم لتقنية المعلومات والاتصـالات؛ والذي يمكن أن يؤدى إلى تعطيل الخدمات الماليـة والمصرفية الضروريـة سواء للأنظمة المالية الوطنية أو الدولية، وتقويض الأمن والثقة في النظام المالي والمصرفي ونزاهته، وتعريض الاستقرار المالي للخطر. ولكون المؤسسات المالية ليست بمنأى عن مخاطر الجرائم المالية الإلكترونية، فلا بد من تكاتف الجهود للوقوف على مخاطر هذه الجرائم وتحديدها وتقييمها وفهمها بالشكل المناسب، وصـولاً إلى وضـع التدابير اللازمة لصـدها والتخفيف منها والتعافي منها حال وقوعها.

هذا ويعد الاحتيال أحد أهم التحديات التي تواجه المؤسـســات المالية وعملائها على حد ســواء، فعواقبه وخيمة، وقد يُلحق الأذى بالمؤسسـة المالية متجاوزًا الخسـائر المالية التي قد تترتب عنه إلى الإضـرار بسمعة المؤسـسـة المالية والذي قد يتناقل أثره إلى القطاع المالي والمصـرفي ككل، إلى جانب تقليل الثقة لدى العملاء والجمهور عامة في اعتماد واستخدام الوسائل الإلكترونية لتنفيذ العمليات المصرفية والمالية ومنها المدفوعات والتحويلات الإلكترونية.

ويكمن خطر الاحتيال بأن أثره لا يقتصر على مؤسسة مالية بعينها، بل قد يمتد ليشمل القطاع بأكمله كما تم الإشارة إلى ذلك سابقًا، أضف إلى ذلك الديناميكية المتغيرة لأساليب الاحتيال، فهو يتطور بسرعة ويتكيف مع التطورات التكنولوجية والتغييرات التي تطرأ على نماذج عمل القطاع المالي والمصـــرفي وعلى وجه الخصـوص جانب المدفوعات، فبالرغم من تطور الآليات وضـوابط الحماية المطبقة لدى المؤسـسـات المالية لمكافحة الاحتيال، إلا أنه لا تزال عمليات الاحتيال الناجحة في جانب المدفوعات بتزايد.

وعادة ما يصـعب تقييم حجم الخسـائر التي قد تترتب على المؤسـسـة المالية نتيجة وقوع عملية احتيال ناجحة على خدماتها، فالأمر يتجاوز الخسـائر المالية التي يمكن تقديرها بسـهولة إلى خسـائر أخرى يصـعب تقديرها؛ كالتأثير على السمعة والقيمة التنافسية في السوق، وتراجع ثقة العملاء، وصولاً إلى احتمالية تنشيط جرائم غســل الأموال وتمويل الإرهاب التي تؤثر على نزاهة النظام المالي ككل، ناهين عن أية عقوبات أو غرامات قد تفرض من البنك المركزي بسـبب عدم الامتثال للأنظمة والتشـريعات في حال ثبت ذلك، ما يدفع المؤسسات المالية إلى ضخ المزيد من الاستثمارات في تطوير واستخدام الأنظمة والبرامج اللازمة لمراقبة ومكافحة عمليات الاحتيال وردعها، والتي قد تكون أقل كلفة من محاولات التعافي من عمليات الاحتيال حال حدوثها.

الهدف من الدليل الإرشادي:

يأتي هذا الدليل حرصـاً من البنك المركزي الأردني على تمكين ومسـاعدة الشـركات – بما يشـمل البنوك وشركات الصرافة - المرخص لها من البنك المركزي الأردني لممارسة أعمال تقديم خدمات الدفع الإلكتروني وإدارة وتشـغيل أنظمة الدفع الإلكترونية من إدارة مخاطر الاحتيال المالي في نظام المدفوعات الوطني بكفاءة وفاعلية، ســواء كان الاحتيال متأتي من قبل موظفي الشــركة أو بمســاعدتهم أو من قبل العملاء أو الغير، وتعزيز الفهم السليم والمعرفة الجيدة للتدابير والإجراءات المناسبة لديها بشأن منع ومكافحة عمليات الاحتيال المالي والتعامل معها بالشـكل المناسـب ورصـد الأسـاليب الجديدة والطرق المبتكرة لحالات الاحتيال، وكذلك تمكين الشــركات من تكييف هذه الإجراءات والتدابير مع طبيعة عملها وأنشــطتها وتعزيز القدرة لديها على تطوير وتبني البرامج اللازمة لمكافحة الاحتيال وفق النهج القائم على المخاطر.

حيث يتضمن هذا الدليل إرشادات عامة لأسس الحوكمة الفعّالة لدى الشركة في مكافحة عمليات الاحتيال التي قد تتعرض لها، بما في ذلك تحديد أدوار ومسـؤوليات كافة الطبقات الإشـرافية والوظيفية داخل الشـركة في وضـع وتنفيذ الضـوابط الوقائية والكشـفية والتصـحيحية لكشـف ومكافحة عمليات الاحتيال والتعافي منها

بالوقت المناسب، بدءًا من مجلس الإدارة ومروراً بالإدارة التنفيذية العليا خصوصًا المدققين الداخليين وموظفي الامتثال وإدارة المخاطر وصولاً إلى بقية العاملين في الشركة، إلى جانب دور ومسؤوليات العميل الذي قد يكون سببًا في إنجاح عملية الاحتيال، بالإضافة إلى إجراءات نشر وتعزيز التوعية اللازمة تجاه مكافحة الاحتيال وخلق ثقافة جيدة بالخصوص.

تجدر الإشارة إلى أن الإجراءات والتدابير الواردة في هذا الدليل تمثل الحد الأدنى من القواعد الإرشادية تجاه مكافحة الاحتيال المالي التي يمكن للشركات اللجوء إليها والاستفادة منها في تطوير سياساتها وإجراءات عملها وضوابطها الرقابية، في حين يترك للشركات وضع تدابير وإجراءات إضافية ملائمة وبما يتناسب مع نتائج تقييم المخاطر لديها وطبيعة أعمالها وأنشطتها.

الإطار التشريعي:

يأتي وضع هذا الدليل الارشادي انطلاقًا من الصلاحيات المخولة للبنك المركزي الأردني بموجب أحكام المادة (4/ب) من قانونه رقم (23) لسنة 1971 وتعديلاته التي تم بموجبها تحديد المهام المناطة بالبنك المركزي ومنها تنظيم نظام المدفوعات الوطني وتطويره بما يضمن توفير نظم آمنة وكفؤة للدفع والتقاص والتسوية في المملكة، وذلك في سبيل تحقيق أهدافه التي شملت المساهمة في تحقيق الاستقرار المصرفي والمالي في المملكة ضمن الفقرة (أ) من المادة أعلاه. كذلك انطلاقًا من دور البنك المركزي الإشرافي والرقابي على نظام المدفوعات الوطني بموجب أحكام المادة (50/أ) من القانون أعلاه. كما يأتي هذا الدليل لينسجم مع المقتضيات التشريعية ذات العلاقة بمكافحة عمليات الاحتيال وإدارة المخاطر ذات الصلة، ولتعزيز قدرة الشركات في الامتثال إلى أحكام التشريعات النافذة دون إخلال أو قصور في الإجراءات المتخذة بالخصوص، حيث أن أبرز التشريعات الناظمة للشركات ذات الصلة بمكافحة الاحتيال على النحو التالي:

أ. نصت أحكام المادة (93/أ) من قانون البنوك رقم (28) لسنة 2000 وتعديلاته على "إذا علم البنك أن تنفيذ أي معاملة مصرفية أو أن تسلم أو دفع أي مبلغ يتعلق أو يمكن أن يتعلق بأي جريمة أو بأي عمل غير مشروع، فعليه أن يقوم فوراً بإشعار البنك المركزي بذلك".

ب. تم بموجب أحكام المادة (5/و) من نظام الدفع والتحويل الإلكتروني للأموال رقم (111) لسنة 2017 الصادر بمقتضى أحكام المادتين (21) و (22) من قانون المعاملات الإلكترونية رقم (15) لسنة 2015؛ وجوب أن يتوفر لدى الشركات قواعد وأنظمة واضحة وسريعة للرد على استفسارات

وشكاوى العملاء وحماية مصالحهم وحل النزاعات التي قد تنشأ عن الخدمات المقدمة لهم وإجراءات الإبلاغ عن سرقة أو فقدان أو اختراق بيانات استخدامهم للخدمات واسترداد الأموال.

ج. ألزمت أحكام المادة (35) من نظام الدفع والتحويل الإلكتروني للأموال رقم (111) لسنة 2017 مقدمي خدمات الدفع من الشركات التأكد من أن البيانات الأمنية الشخصية التي تستخدم لغايات التوثق من شخص العميل غير متاحة لغيره، وتوفير الوسائل المناسبة لتمكين العميل من الاخبار عن فقدان أو سرقة أو اختراق البيانات الأمنية الشخصية.

د. كما تلتزم الشركات سندًا لأحكام المادة (36) من نظام الدفع والتحويل الإلكتروني للأموال رقم (111) لسنة 2017 بإخطار البنك المركزي والجهات والأخرى ذات العلاقة عن أي حالات اختراق أو احتيال قد تتعرض لها الشركة أو أي طرف ثالث متعاقدة معه فور حدوثها.

تنويـــــه:

تم إصدار هذا الدليل لأغراض الاسترشاد به من قبل الشركات التي تمارس أي من أنشطة تقديم خدمات الدفع الإلكتروني و/أو إدارة وتشغيل أنظمة الدفع الإلكتروني في مكافحة عمليات الاحتيال المالي، ولا يقع هذا الدليل ضمن نطاق الإلزامية ما لم تقرر أوامر البنك المركزي خلاف ذلك. هذا وفي حال وجود أو نشوء أي تعارض بين أي من الإجراءات الواردة في هذا الدليل مع أي من الأحكام الواردة في التشريعات النافذة فتطبق الأحكام الواردة في تلك التشريعات، على أن يتم إخطار البنك المركزي من قبل الشركات عن هذا التعارض لمعالجته بشكل المناسب.

نطاق التطبيق:

تم إصدار هذا الدليل الإرشادي للشركات المرخص لها من البنك المركزي الأردني – بما يشمل البنوك وشركات الصرافة - لممارسة أعمال تقديم خدمات الدفع الإلكتروني وإدارة وتشغيل أنظمة الدفع الإلكترونية؛ لغايات الاستئناس به في مكافحة عمليات الاحتيال المالي التي قد تتعرض لها أي من مكونات نظام المدفوعات الوطني، مع مراعاة عدم إخلال الشركات بأحكام التشريعات النافذة ذات العلاقة بالاحتيال، وللبنك المركزي الأردني أن يوجه هذا الدليل للاسترشاد به من قبل المؤسسات المالية الأخرى الخاضعة لإشرافه ورقابته بموجب أوامر خاصة تصدر لهذه الغاية.

أولاً: مدخل إلى الاحتيال المالي

1. مفهوم الاحتيال المالي

يستخدم مصطلح الاحتيال بشكل شائع لوصف مجموعة واسعة من السلوكيات السيئة، بما في ذلك السرقة والفساد والاختلاس والرشوة والتزوير والتضليل والتواطؤ وغسل الأموال وإخفاء الحقائق المادية، وغالبًا ما ينطوي ذلك على الأعمال غير القانونية التي تتسم بالخداع أو الاخفاء أو انتهاك الثقة؛ لتحقيق مكاسب شخصية لمصلحة فرد أو طرف ثالث.

ويعرف الاحتيال بأنه "استخدام الخداع للحصول على منفعة دون وجه حق" أو "أي ممارسة تنطوي على استخدام الخداع للحصول المباشر أو غير المباشر على شكل من أشكال الاستفادة المالية لمرتكب الجريمة، أو تسهيل ذلك لغيره لتؤدي إلى شكل من أشكال الخسارة للطرف الذي تعرض للاحتيال".

أما على صعيد المشرع الأردني، فقد نصت أحكام المادة (417) من قانون العقوبات النافذ على أن الاحتيال "كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو اسنادًا يتضمن تعهدًا أو إبراء، فاستولى عليه احتيالاً". ومن خلال هذا النص فإنه يمكن تعريف الاحتيال بأنه استيلاء على أموال منقولة أو غير منقولة أو سندات باستعمال طرق ووسائل احتيالية تجعل الطرف الآخر يذعن له ويقوم بتسليمها له.

ولكي تقوم جريمة الاحتيال لا بد من قيام الجاني بفعل مادي يتمثل بالاستيلاء على مال الغير بطرق احتيالية، بالإضافة إلى القصد الجرمي وهو أن تتجه إرادة الجاني للاستيلاء على مال الغير من خلال الوسائل الاحتيالية التي قام باستخدامها.

ويقوم الاحتيال على الغش والخداع، وقد حدد المشرع الأردني بموجب المادة (417) من قانون العقوبات النافذ الوسائل الاحتيالية؛ باستعمال طرق احتيالية من شأنها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو بتسديد المبلغ الذي أخذ بطريق الاحتيال أو الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزور، وبالتصرف في مال منقول أو غير منقول وهو يعلم أنه ليس له صفة للتصرف به، وباتخاذ اسم كاذب أو صفة غير صحيحة.

وبذات السياق، يمكن تعريف الاحتيال الإلكتروني وفقًا للمادة (11) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنه "التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق؛ إدخال أو تعديل أو

محو أو حجب للمعلومات والبيانات، أو التدخل في وظيفة أنظمة التشـــغيل وأنظمة الاتصـــالات أو محاولة تعطيلها أو تغييرها، أو تعطيل الأجهزة والبرامج والمواقع الإلكترونية".

الاحتيال المالي وغسل الأموال:

تعد جريمة الاحتيال أحد الجرائم الأصـلية لجريمة غسـل الأموال، وهناك علاقة وثيقة بين غسـل الأموال والاحتيال المالي، ففي غالب الأحوال يلجأ المحتالون إلى غسل الأموال الناتجة عن عمليات الاحتيال المالي لإخفاء مصـادرها غير المشـروعة، لذلك فإن هناك تداخل في التدابير المتخذة لمكافحة الاحتيال المالي من جهة وتدابير مكافحة غسل الأموال من جهة أخرى.

2. أبرز أشكال الاحتيال المالي

مع التطور التكنولوجي الذي شهده العالم في العقود الأخيرة، والذي نتج عنه تقديم خدمات مالية باستخدام هذه التقنيات، تزايد بذلك اعتماد الأفراد والشركات على عمليات الدفع الإلكتروني، ومع تطور الوسائل التقنية التي يمكن من خلالها الحصـول على الخدمات والمنتجات المالية، تتطور أسـاليب الاحتيال المالي وتتجدد بين فترة وأخرى متخذة أشـكالًا وصـورًا متعددة؛ إلا أن هدفها واحد وهو الاحتيال على الأفراد للحصـول على بياناتهم المالية والشـخصـية لسـرقة أموالهم ومدخراتهم، ولكن مهما تعددت أسـاليب الاحتيال، من الضـروري معرفة أن الحيطة والحذر خير وسـيلة للحماية ضـد أي عملية احتيال مالي، وفي هذا القسـم سـوف نسـتعرض أبرز أشكال الاحتيال وكيفية التحصن منها.

بذات السياق، تتصـف أسـاليب الاحتيال في المدفوعات الإلكترونية بديناميكية متغيرة، إلا أنها وليدة عدد من الأشكال الرئيسية، وقد تتضمن عملية احتيال مالي واحدة استخدام أكثر من نوع من هذه الأشكال الرئيسية والتي ندرجها على النحو التالي:

الهندسة الاجتماعية:

الاحتيال باستخدام أسـاليب الهندسـة الاجتماعية مصـطلح عام يشـير إلى أسـاليب الاحتيال التي يسـتخدمها المجرمون لاستغلال ثقة الشخص من أجل الحصول مباشرة على المال أو المعلومات السرية التي تمكنهم من ارتكاب جريمة لاحقة، ويسـتخدم المجرمون تكتيكات الهندسـة الاجتماعية لأنه عادةً ما يكون من الأسـهل اسـتغلال ميل الفرد الطبيعي للثقة، بدلاً من اكتشـاف طرق لمهاجمة الأنظمة أو الأجهزة الخاصـة بالشـركة بشكل مباشر.

وعلى الرغم من أن وسائل التواصل الاجتماعي هي القناة المفضلة في هذا الشكل من أساليب الاحتيال المالي، إلا أنه يمكن أن تتم محاولات الهندسة الاجتماعية عبر العديد من الوسائل الإلكترونية وغير الإلكترونية، بما في ذلك البريد الإلكتروني والرسائل القصيرة والمكالمات الهاتفية بالإضافة إلى مواقع التواصل الاجتماعي، وأي قناة تستخدم للتواصل مع العملاء يمكن أن يستغلها المهاجم بدرجات متفاوتة من التطور المطلوب لتنفيذ الهجوم.

ومن أشكال الهندسة الاجتماعية في الاحتيال المالي؛ التصَّيد (Phishing) وهو أسلوب احتيالي يقوم فيه المجرم بإرسال رسالة احتيالية تخدع المستلم للتخلي عن معلوماته الخاصة، وقد تتضمن المعلومات التي يطلبونها تفاصيل بطاقة الدفع أو تفاصيل الحساب المصرفي أو حسابات الدفع الإلكترونية أو مجموعة من المعلومات الشخصية الأخرى، وهو يأتي غالباً على ثلاثة أنواع هي:

- **التصَّيد الاحتيالي عبر البريد الإلكتروني:** يتم تنفيذ أكثر أشكال هجمات التصيد الاحتيالي عبر رسائل البريد الإلكتروني، وعادةً ما يتضمن هذا النوع من الهجوم محتالًا يرسل بريداً إلكترونياً يخبر المستلم أن حسابه قد تم اختراقه، وأنهم بحاجة إلى إعادة تعيين كلمة المرور الخاصة به، الهدف من التصيد الاحتيالي عبر البريد الإلكتروني هو جعل المستلم يكشف عن طيب خاطر بيانات اعتماد تسجيل الدخول الخاصة به أو أي معلومات حساسة أخرى يحتاجها المحتال لإتمام هجمته.

- **التصَّيد عبر القنوات الصوتية (Vishing):** يتم هذا النوع من التصيد عبر مكالمة صوتية يتلقى المستلم مكالمة تخبره بانتهاء صلاحية بطاقة الدفع الخاصة به مثلاً، ويحتاج إلى الكشف عن بيانات الاعتماد المصرفية الخاصة به لضمان إعادة تفعيلها بشكل صحيح. ومن الأمثلة على التصيد الذي يتم من خلال قناة الصوت، أن يتصل المحتال بالضحية يدعي أنه أحد موظفي الشركة وأن هناك حالة طارئة ويقوم بترهيب العميل بأن أمواله يمكن أن تُفقد، ومن ثم يعرض عليه المساعدة وعلى الضحية فقط أن يتوثق من خلال بياناته الأمنية (Credential information)، وبالتالي يستطيع المحتال الحصول على البيانات الأمنية تلك لاستخدامها في تنفيذ عملية من خلال قناة (On-line Banking) أو أي شكل من أشكال إساءة الاستخدام.

- **التصَّيد الاحتيالي عبر الرسائل النصية (Smashing):** نوع من هجمات التصَّيد الاحتيالي الذي يستخدم الرسائل النصية القصيرة لاستهداف الضحايا غير المعروفين، الأساليب المستخدمة هنا تشبه إلى حد بعيد كيفية تنفيذ هجوم التصَّيد عبر البريد الإلكتروني؛ حيث يتلقى المستلم رسالة نصية

تخبره أن حسابه (الخدمات المصرفية عبر الإنترنت مثلاً) قد تم اختراقه ويحتاج إلى مشاركة معلومات تسجيل الدخول الحالية للوصول إلى الحساب، بمجرد حصول المحتال على بيانات تسجيل الدخول، يمكنه تغيير كلمة المرور ومنع الضحية من الوصول إلى الحساب. وقد يكون المستهدف في عملية الاحتيال هنا عميل الشركة، وقد يكون موظف لدى الشركة يتم استغلاله للوصول إلى أنظمة الشركة وبياناتها والحصول على الموارد المالية بشكل مباشر لتنفيذ عمليات دفع من خلال الأنظمة الخاصة بالشركة، أو حتى إيقاف عمل أنظمة الشركة، وهنا تكون الشركة قد تعرضت لعملية اختراق أمني ولا بد لها من أخذ الإجراءات اللازمة لمعالجة هذا الاختراق.

سرقة بيانات هوية العميل:

في هذا النوع من أنواع الاحتيال يقوم المحتال باستخدام هوية العميل لإجراء عملية دفع، وفي العديد من عمليات الاحتيال في هذا النوع تكون نقطة الدخول إلى الضحية من أشكال مختلفة من التصيد الاحتيالي للحصول على بيانات اعتماد الخدمات المصرفية عبر الإنترنت ويتم سحب الأموال من خلال عمليات الدفع عبر البطاقات.

ويمكن استخدام بيانات الشخص وسرقة هويته لاستغلالها في التسجيل وفتح حساب لدى شركة ما، لذا يتطلب من الشركة بذل العناية الواجبة للتأكد والتوثق من قيامها بتسجيل العميل والتوثق من أنه من يدعي حقيقة، وأن لا يكون هناك انتحال لشخصية أو تزوير لأي معلومات، كون أن كل ما سيلحق عملية تسجيل العميل من معاملات مالية ستعتمد في دقتها وحقيقتها على مدى دقة عملية التسجيل.

تزوير هوية التاجر:

يشبه إلى حد كبير الاحتيال في هوية العميل، وينطوي الاحتيال في هوية التاجر على مجرمين يقومون بإنشاء حساب تاجر احتيالي بعد الحصول بشكل غير قانوني على معلومات تعريف الشركة، ويستخدم المحتال هذا "العمل" الذي تم إنشاؤه حديثًا لفرض عمولات على بطاقات ائتمان العملاء، ثم إنهاء الحساب والابتعاد، تاركًا وراءه عدد كبير من عمليات رد المبالغ المدفوعة وشكاوى العملاء وتقارير الاحتيال.

إضافةً إلى تعدد أنواع الاحتيال، فإن احتيال ببطاقات الدفع دائم التغير، إذ تدفع التقنيات الجديدة الجرائم الإلكترونية إلى تطوير أساليبها، فيستحيل تقريبًا حصرها في قائمة واحدة، ولكن توجد فئتان رئيسيتان هما:

- **الاحتيال دون وجود البطاقة (Card Non-Present):** هو النوع الأكثر شيوعًا، ويحدث عندما تُسرق معلومات صاحب البطاقة وتُستخدم استخدامًا غير قانوني دون الحاجة إلى وجود البطاقة فعليًا. يحدث هذا النوع عادةً على الإنترنت، وقد يكون نتيجة ما يسمى رسائل التصَّيد الاحتيالية الإلكترونية التي تُرسل من محتالين ينتحلون شخصية مؤسسات موثوقة بغرض سرقة التفاصيل الشخصية أو المالية عبر رابط احتيالي.

- **احتيال بوجود البطاقة (Card Present):** يأخذ غالبًا شكل سرقة معلومات البطاقة باستخدام جهاز إلكتروني للاستنساخ الاحتيالي للبيانات، هذه النوع أقل شيوعًا حاليًا لكن يبقى الحذر واجبًا، حيث يمرر البائع المخادع البطاقة عبر جهاز يخزن معلومات البطاقة، وتستخدم هذه المعلومات في أي عملية شراء، وتُحمَّل التكلفة على حساب صاحب البطاقة.

ثانياً: إطار الحاكمية المؤسسية

يقع على عاتق الشركات للتمكن من مكافحة حالات الاحتيال المالي بكافة مصادرة والتعامل معها بالشكل والتوقيت المناسبين وضمن مستويات الكفاءة والفاعلية؛ وضع إطار حاكمية شامل وفعال يحدد مستوى الصلاحيات وطبيعة الأدوار ونطاق المسؤوليات تجاه تنفيذ سياسة الشركة في مكافحة الاحتيال المالي وبما ينسجم مع أحكام التشريعات النافذة بالخصوص، حيث كلما كانت الصلاحيات والأدوار والمسؤوليات محددة بشكل واضح وشمولي لجميع المستويات الإشرافية والإدارية والوظيفية في الشركة، كلما ساهم ذلك في ضمان فاعلية تنفيذ خطط الشركة وبرامجها في مكافحة الاحتيال المالي.

ولضمان تنفيذ الشركات للممارسات السليمة للحاكمية المؤسسية، فإنه يتوجب عليها لدى تطوير ووضع إطار الحاكمية الخاص بمكافحة الاحتيال المالي مراعاة المتطلبات التالية:

أ. أن تقوم الشركة بوضع سياسة خاصة لمكافحة الاحتيال المالي بكافة مصادره، أو تضمين سياساتها الداخلية بالإجراءات والمتطلبات اللازمة لمكافحة الاحتيال المالي، بحيث تحدد هذه السياسات الصلاحيات والأدوار والمسؤوليات المتعلقة بمكافحة الاحتيال.

ب. أن تقوم الشركة بتحديد وتقييم وفهم مخاطر الاحتيال المالي التي قد تتعرض لها، مع ضرورة تبني النهج المستند على المخاطر في التعامل مع حالات الاحتيال المالي ومكافحته، إلى جانب تضمين

متطلبات مكافحة الاحتيال المالي ضمن استراتيجية الشركة أو الإطار الشامل لإدارة المخاطر؛ للتخفيف من المستويات الحدية لمخاطر الاحتيال المالي والآثار المترتبة عليه حال حدوثه.

ج. أن تقوم الشركة بتحديد وحدة تنظيمية لديها مسؤولة عن وظيفة إدارة عمليات مكافحة الاحتيال المالي، ويمكن للشركة بهذا الخصوص أن توجد وحدة تنظيمية مستقلة خاصة بتنفيذ هذه الوظيفة، أو من خلال تأسيس قسم معني بذلك يتبع إلى وحدة إدارة الامتثال و/أو وحدة إدارة المخاطر، على أن يتم تقدير ذلك وفقًا لحجم أعمال الشركة وتنوع خدماتها وطبيعتها ومستوى التعقيد فيها.

د. أن تقوم الشركة في سبيل تعزيز حوكمة إدارة مخاطر الاحتيال لديها بتشكيل لجنة منبثقة عن مجلس إدارتها؛ لغاية متابعة إدارة عمليات الاحتيال المالي ونتائج التحقيق بها، وقد توكل مهام اللجنة المنبثقة عن مجلس الإدارة بالخصوص إلى لجنة الامتثال أو لجنة إدارة المخاطر.

هذا وتقع مسؤولية مكافحة عمليات الاحتيال المالي على عاتق جميع العاملين في الشركة بمختلف المستويات الوظيفية فيها، جنبًا إلى جنب مع مجلس إدارة الشركة، وبحيث تكون الصلاحيات والمسؤوليات والأدوار وفقًا لما يلي:

1. مجلس الإدارة

يتحمل مجلس إدارة الشركة المسؤولية العامة للإشراف والرقابة على مكافحة الاحتيال المالي في الشركة ولكافة مصادره، وضمن هذا النطاق تكون مهام ومسؤوليات مجلس الإدارة بحد أدنى ما يلي:

أ. اعتماد سياسة مكافحة الاحتيال المالي ومراجعتها عند إجراء أي تغييرات تطرأ عليها، والتأكد من مدى ملاءمة السياسة لمخاطر الاحتيال المالي في الشركة، سواء كانت سياسة خاصة بحد ذاتها أو جزء من السياسات الأخرى في الشركة.

ب. مراقبة ومتابعة تقييم سياسة مكافحة الاحتيال المالي بشكل دوري للتحقق من تطبيقها على نحو فعال، بما في ذلك التأكد من أن جميع حالات الاحتيال المالي التي تعرضت لها الشركة قد تم معالجتها وإدارتها بالشكل والوقت المناسب من قبل الإدارة التنفيذية العليا، وتقييم درجة الفاعلية التي تدير بها الشركة مخاطر الاحتيال المالي مرة واحدة في السنة على الأقل.

ج. اعتماد وثيقة رسمية يتم بموجبها الموافقة على تحديد وحدة تنظيمية دائمة وفعالة داخل الشركة؛ تعنى بالقيام بوظيفة إدارة عمليات مكافحة الاحتيال المالي، سواء كانت هذه الوحدة التنظيمية مستقلة

بحد ذاتها، أو قسم يتبع تنظيميًا لوحدة إدارة الامتثال أو وحدة إدارة المخاطر في الشركة، بالقدر الممكن عمليًا ووفق ما تقتضيه الظروف.

د. اعتماد إطار شامل لإدارة مخاطر الاحتيال المالي أو تضمينها في الإطار العام للمخاطر الكلية في الشركة، ووضع الاستراتيجيات الرئيسية لإدارة تلك المخاطر، وبشكل يمكن الشركة وبجميع الأوقات من الاستجابة لمخاطر الاحتيال المالي التي قد تنشأ، والتقليل من احتمالية حدوث تلك المخاطر وإدارتها بشكل فعال ضمن نطاق المنهج المستند على المخاطر.

ه. التأكد من توفر الموارد المالية الكافية والكوادر البشرية المؤهلة والمناسبة لوحدة مكافحة الاحتيال المالي، وتحديد مسؤولياتها وصلاحياتها بدقة بما في ذلك الصلاحيات التي تخولها إجراء عمليات التحقيق في حالات الاحتيال المالي مع أي من العاملين في الشركة بمختلف مستوياتهم الوظيفية والوصول إلى جميع المعلومات والمستندات اللازمة لتنفيذ أعمالها مع ضمان عدم الإخلال بمتطلبات السرية، ومراعاة إخضاع نشاطها للمراجعة الدورية من قبل وظيفة التدقيق الداخلي في الشركة.

و. عقد اجتماعات دورية بحد أدنى ربع سنوية أو أينما استدعى الأمر ذلك؛ لمناقشة حالات الاحتيال المالي التي تعرضت لها الشركة - بما في ذلك محاولات الاحتيال المالي أو الحالات المحتملة - والأساليب المستخدمة في ذلك والإحصائيات التابعة لها وعرض نتائجها وحجم الأثر المترتب عليها أو المتوقع والإجراءات المتخذة للإبلاغ الفوري عن تلك الحالات للبنك المركزي والجهات الأخرى ذات العلاقة، وصولاً إلى الإجراءات التصحيحية والضوابط الرقابية الموصى بها من وحدة مكافحة الاحتيال المالي للموافقة عليها، مع وضع آلية لمتابعة تنفيذ تلك الإجراءات التصحيحية والضوابط الرقابية المعتمدة من قبله.

ز. مراجعة ومناقشة التقرير السنوي لمكافحة الاحتيال المالي، والتأكد من تنفيذ كافة التوصيات الواردة فيه بالشكل والوقت المناسبين.

ح. اتخاذ التدابير اللازمة لتعزيز قيم الاستقامة والنزاهة والممارسة المهنية السليمة داخل الشركة بالشكل الذي يجعل من عمليات مكافحة الاحتيال المالي هدفًا أساسيًا واجب التحقيق، بما في ذلك توفير بيئة مواتية داخل الشركة لتعزيز ثقافة مكافحة عمليات الاحتيال المالي وصدها والوقاية منها والإبلاغ عنها بسهولة ويسر وبما يضمن نطاق الحفاظ على السرية.

قد يختار مجلس الإدارة تفويض القيام بالمهام والمسؤوليات الواردة في الفقرات (ب) و (هـ) و (و) و (ز) و (ح) أعلاه إلى جانب مراجعة سياسة مكافحة الاحتيال المالي وإجراءات إدارة مخاطر الاحتيال المالي

والتأكد من درجة فاعليتها وتقديم التوصيات اللازمة بشأنها إلى لجنة مستقلة منبثقة عنه يتم تشكيلها لهذه الغاية أو إلى لجنة مراقبة الامتثال (إن وجدت) أو لجنة إدارة المخاطر.

2. لجنة مكافحة الاحتيال المالي

حال قرر مجلس الإدارة الذهاب باتجاه حوكمة إدارة مخاطر الاحتيال المالي من خلال تشكيل لجنة منبثقة عنه أو أيكال ذلك إلى لجنة الامتثال أو لجنة إدارة المخاطر، فيراعى أن تتضمن مهام ومسؤوليات اللجنة بما يلي:

أ. القيام بالمهام والمسؤوليات المحددة لمجلس الإدارة ضمن الفقرات (ب) و (هـ) و (و) و (ز) و (ح) من البند (1) أعلاه.

ب. مراجعة سياسة مكافحة الاحتيال المالي بما في ذلك التأكد من انسجامها مع السياسات الأخرى في الشركة وعلى وجه الخصوص سياسة مكافحة غسل الأموال وتمويل الإرهاب والإطار الشامل لإدارة المخاطر في الشركة، وكذلك مراجعة إجراءات إدارة مخاطر الاحتيال المالي والضوابط الرقابية الوقائية أو الكشفية أو التصحيحية والتأكد من كفايتها ودرجة فاعليتها، ورفع النتائج والتوصيات بخصوصها لمجلس الإدارة.

ج. مراجعة نتائج عملية تقييم مخاطر الاحتيال المالي، وبما يشمل التأكد من أن الشركة قامت بتحديد المخاطر المحتملة والتعرف عليها وتقييمها بالشكل المناسب وصولاً إلى وضع الإجراءات والضوابط الرقابية اللازمة وعلى نحو يجعل من المخاطر المتبقية مقبولة وفقاً لسياسة الشركة في إطار إدارة المخاطر وشهيتها في قبول المخاطر، ورفع النتائج والتوصيات بالخصوص إلى مجلس الإدارة.

د. متابعة عمليات التحقيق في حالات الاحتيال المالي سواء نتج عنها خسائر مالية أم لم ينتج، إلى جانب متابعة البلاغات مع الجهات ذات العلاقة بخصوص تلك الحالات.

ه. التعرف على الثغرات التي ساهمت في حدوث عمليات الاحتيال المالي والتأكد من وضع التدابير اللازمة لحلها والضوابط الرقابية للحيلولة دون تكرارها، بما في ذلك تحديد الأسباب التي أدت إلى التأخر في الكشف عن عمليات الاحتيال المالي التي تعرضت لها الشركة (إن وجدت).

و. متابعة حالات الإبلاغ للبنك المركزي ووحدة مكافحة غسل الأموال وتمويل الإرهاب والجهات المختصة الأخرى (سلطات انفاذ القانون) عن أية عمليات احتيال مالي مثبتة تتعرض لها الشركة

سـواء كان الاحتيال داخلي أو خارجي بما في ذلك على عملاء الشـركة أو أي طرف ثالث متعاقدة معه، وبما يتفق مع أحكام التشريعات النافذة.

ز. تقديم توصيات اللجنة وتقاريرها بشكل دوري أو عند اللزوم إلى مجلس الإدارة، مع مراعاة تضمين تلك التقارير بما يلي:

1. تفاصيل حالات الاحتيال المالي التي تعرضت لها الشركة متضمنة على سبيل المثال ما يلي:
   - إجمالي عدد عمليات الاحتيال المالي (وقيمها) سواء التي تم كشفها/ المبلغ عنها.
   - الآلية المستخدمة في تنفيذ عملية الاحتيال المالي.
   - نتائج التحقيق لحالات الاحتيال المالي بما في ذلك وضع حالة الاحتيال المالي.
   - الثغرات التي تم استغلالها لتنفيذ عمليات الاحتيال المالي.
   - الخسارة المالية التي ستتكبدها الشركة (إن وجدت) أو أية خسائر أخرى مادية أو معنوية.
   - معدل الوقت المستغرق للكشف عن عمليات الاحتيال المالي ومعالجتها وأسباب الانحراف عن المستهدف في تحقيق ذلك.
   - عدد العمليات التي تم البت بها والأخرى قيد التحقيق والدراسة.
   - الإجراءات التصـحيحية المتخذة أو الوقائية التي تم تطبيقها لعدم تكرار مثل هذه الحالات مستقبلاً.
2. نتائج عمليات تقييم مخاطر الاحتيال المالي متضمنة على سبيل المثال ما يلي:
   - نتائج تحديد وتقييم مخاطر الاحتيال المالي.
   - مدى فاعلية وكفاية الضوابط الرقابية لمكافحة عمليات الاحتيال المالي.
   - نتائج أداء المؤشرات الرقابية وسيناريوهات الاشتباه لرصد وكشف عمليات الاحتيال المالي.
   - نتائج تنفيذ خطة التوعية والتثقيف تجاه مخاطر الاحتيال المالي.
   - مؤشر التزام موظفي الشركة بإجراءات مكافحة عمليات الاحتيال المالي.
   - نتائج تقييم قوائم الصلاحيات ومدى فاعليتها في مكافحة الاحتيال المالي الداخلي.
   - مدى مناسبة الإجراءات الإدارية والتأديبية المتخذة لحالات الاحتيال المالي الداخلي.

ح. التأكد من تنفيذ البرامج التوعوية اللازمة لتعزيز ثقافة مكافحة عمليات الاحتيال المالي على كافة المستويات الوظيفية في الشركة بما في ذلك البرامج التوعوية المعدة للعملاء.

ط. التعاون مع اللجان الأخرى المنبثقة عن مجلس الإدارة لتبادل المعلومات اللازمة لتنفيذ مهامها.

ي. أية مهام أخرى يكلفها بها مجلس الإدارة.

لغايات تمكين لجنة مكافحة الاحتيال المالي من تنفيذ مهامها ومسؤوليات بكفاءة وفاعلية، فإنه يتطلب من مجلس الإدارة وضع واعتماد الترتيبات اللازمة لإعطاء اللجنة حق الاتصال المباشر مع كافة العاملين في الشركة وحرية الوصول لكافة الوثائق والمستندات والسجلات والكشوفات والأجهزة، إلى جانب تمكينها من طلب الاستشارات الخارجية بهدف المساعدة والنصح في تنفيذ مهامها، والنظر في أية أمور عالقة بين وحدة مكافحة الاحتيال المالي والوحدات التنظيمية الأخرى بما في ذلك مدير عام الشركة لمعالجتها بهدف تمكين وحدة مكافحة الاحتيال المالي من تنفيذ مهامها.

3. الإدارة التنفيذية العليا

تتحمل الإدارة التنفيذية العليا في الشركة المسؤولية الكاملة عن تطبيق الإجراءات اللازمة لغايات مكافحة عمليات الاحتيال المالي بكافة مصادره، ولها في سبيل تحقيق ذلك القيام بالمهام والمسؤوليات التالية كحد أدنى:

أ. إدارة وتنظيم وظيفة مكافحة الاحتيال المالي من خلال؛ إنشاء الوحدة التنظيمية المعنية بذلك وترشيح/ تعيين مديرها/ رئيسها، ورفدها بالكوادر البشرية المؤهلة والمناسبة على أساس الكفاءة ومعايير الملاءمة، وتخصيص الموارد المالية اللازمة لتمكينها من تنفيذ مهامها وبما يشمل تغطية الاحتياجات التدريبية اللازمة للعاملين فيها باستمرار وتوفير الأنظمة المعلوماتية الإلكترونية المساندة لها.

ب. وضع سياسة مكافحة الاحتيال المالي واعتمادها من مجلس الإدارة، واتخاذ التدابير اللازمة لضمان تطبيقها والالتزام بها، إلى جانب مراجعتها وتحديثها بشكل دوري وكلما لزم الأمر، وتعميمها على جميع الوحدات التنظيمية والعاملين في الشركة للالتزام بها بما في ذلك الإبلاغ عن أية حالات احتيال مالي يتم اكتشافها أو يشتبه بها لرئيس وحدة مكافحة الاحتيال المالي وفق قنوات تواصل مخصصة ومهيأة لذلك، وصولاً إلى التأكد من أنه يتم تطبيق الإجراءات والضوابط اللازمة للكشف عن وقوع حالات احتيال مالي أو الاشتباه بها سواء من داخل الشركة أو خارجها ومعالجتها وردعها بالشكل والوقت المناسبين، أو التأكد من كفاية تلك الإجراءات والضوابط.

ج. وضع برنامج سنوي على الأقل لإدارة مخاطر الاحتيال المالي بالتعاون مع وحدة مكافحة الاحتيال المالي، بحيث يأخذ البرنامج بالاعتبار التعرف على مخاطر الاحتيال المالي بكافة مصادرها

وتحديدها وتقييمها ووضع الخطط التصحيحية في حال وجود أي قصور في الإجراءات والضوابط الرقابية اللازمة لمكافحة أية عمليات احتيال مالي محتملة والتأكد من تطبيقها.

د. وضع الإجراءات الكفيلة للتأكد من أن كافة المستويات الوظيفية داخل الشركة تتيح الإمكانيات المناسبة لموظفي وحدة مكافحة الاحتيال المالي للقيام بتنفيذ المهام المناطة بهم بكفاءة وفاعلية وضمن نطاق الثقة والتجانس في العلاقة بينهم، وعلى وجه الخصوص أثناء قيامهم بإجراء عمليات التحقيق في حالات الاحتيال المالي والوصول إلى المعلومات والمستندات اللازمة لتنفيذ أعمالهم.

ه. تحديد خطوط الإبلاغ سواء لمجلس الإدارة أو البنك المركزي أو أي من السلطات المختصة الأخرى ذات العلاقة عن أية حالات احتيال مالي تتعرض لها الشركة أو أي من الأطراف الثالثة التي تتعاقد معها، وكذلك حالات الإبلاغ لوحدة مكافحة غسل الأموال وتمويل الإرهاب حال كانت عملية الاحتيال المالي يشتبه ارتباطها بعمليات غسل أموال أو تمويل إرهاب.

و. وضع وضمان تنفيذ البرامج التثقيفية والتوعوية الموجهة لجميع المستويات الإشرافية والوظيفية في الشركة بدءًا من قمة الهرم ووصولاً إلى القاعدة (Tone at The Top)؛ لبيان أهمية وواجبات ومسؤوليات مكافحة عمليات الاحتيال المالي والإبلاغ عنها وصدها.

4. وحدة مكافحة الاحتيال المالي

تم الإشارة مسبقًا إلى ضرورة قيام الشركة بتحديد وحدة تنظيمية لديها مسؤولة عن وظيفة إدارة عمليات مكافحة الاحتيال المالي، ويمكن للشركة بهذا الخصوص أن توجد وحدة تنظيمية مستقلة خاصة بتنفيذ هذه الوظيفة، أو من خلال تأسيس قسم معني بذلك يتبع إلى وحدة مراقبة الامتثال أو وحدة إدارة المخاطر، على أن يتم تقدير ذلك وفقًا لحجم أعمال الشركة وتنوع خدماتها وطبيعتها ومستوى التعقيد فيها. وتتولى الوحدة التنظيمية المسؤولة عن القيام بمهام مكافحة الاحتيال المالي بشكل عام بمساعدة الإدارة التنفيذية العليا في الشركة في إدارة مخاطر الاحتيال المالي ومراقبته ومكافحته، بالإضافة المهام التالية:

أ. اقتراح السياسات والخطط التنفيذية وإجراءات العمل والضوابط الرقابية اللازمة للشركة في سبيل مكافحة عمليات الاحتيال المالي ومراجعتها وتقييمها بشكل دوري وتحديثها أينما لزم الأمر.

ب. استخدام الأنظمة الرقابية الإلكترونية لرصد والكشف والحد من عمليات الاحتيال المالي سواء من داخل الشركة أو خارجها، وقياس مدى فعالية وكفاءة تلك الأنظمة بشكل دوري، والالتزام بتحديث السيناريوهات والمؤشرات التحذيرية لرصد عمليات الاحتيال المالي المحتملة وبما يتوافق مع

المستجدات التي تطرأ على الأساليب المستخدمة في عمليات الاحتيال المالي، أخذًا بالاعتبار تضمين تلك الأنظمة الرقابية بما يلي:

1. سيناريوهات ومؤشرات تحذيرية مبنية على إجراءات واضحة لحالات الاحتيال المالي.
2. تحليل سلوك العملاء على مستوى كافة القنوات المتاحة لكشف العمليات غير المعتادة ذات الصلة بالاحتيال المالي.
3. وضع سيناريوهات خاصة لمراقبة حسابات العاملين في الشركة وتحليل سلوكهم.

ج. تقصي حالات الاحتيال المالي المحتملة ضد الشركة، أو اتخاذ الإجراءات اللازمة حال تعرضت الشركة لأي عملية احتيال (داخلي أو خارجي) منها على سبيل المثال لا الحصر:

1. التحقيق في حالات الاحتيال المالي المرتكبة من قبل أي من العاملين في الشركة أو التي تتعرض لها الشركة من الغير، على أن يتم تشكيل لجنة من داخل الشركة يرأسها ويشارك في عضويتها وحدة مكافحة الاحتيال المالي للقيام بمهام التحقيق في عمليات الاحتيال المالي مع مراعاة تجنب تضارب المصالح لدى إنشاء هذه اللجنة.
2. تتبع العمليات وتبادل المعلومات ذات الصلة بأية حالات احتيال مالي تكون الشركة طرفًا فيه بما في ذلك عملائها وبما يراعي أحكام التشريعات النافذة.
3. حجز المبالغ محل الاشتباه بعملية احتيال مالي بناء على طلب أصولي من قبل الجهات المختصة.
4. إخطار البنك المركزي والجهات الأخرى المختصة (سلطات إنفاذ القانون) -دون توانٍ أو تأخير- عن كافة عمليات الاحتيال المالي (سواء داخلي أو خارجي) فور وقوعها أو اكتشافها والتي تكون الشركة أو أي من إداريها طرفاً فيها سواء تمت تسويتها أو لم يترتب عليها خسائر مادية.
5. إخطار البنك المركزي عن كافة الحالات التي لا تكون الشركة أو أي من إداريها طرفاً فيها ويقع على عاتق الشركة مسؤولية اتخاذ الإجراءات القانونية اللازمة بما في ذلك تقرير إبلاغ أو عدم إبلاغ الجهات المختصة الأخرى (سلطات إنفاذ القانون) ووفق رأي مستشارها القانوني بشأن كل حاله ووفقاً لما تقتضيه التشريعات ذات العلاقة.
6. أن يكون إخطار البنك المركزي بالحالة مستقلة عن عملية إخطار الجهات المختصة الأخرى (كسلطات إنفاذ القانون)، وعلى أن يتم توضيح (تاريخ حدوث العملية، وأطرافها، الوحدات التنظيمية المعنية من داخل الشركة، الإجراءات التصحيحية المتخذة، الخسائر إن وجدت،

الأساليب المستخدمة)، مع تزويد البنك المركزي بشكل لاحق بما يُفيد إبلاغ الجهات المختصة الأخرى (سلطات إنفاذ القانون) بالحالة وتوضيح تاريخ الإخطار.

7. إخطار وحدة مكافحة غسل الأموال وتمويل الإرهاب وفق الإجراءات والقنوات والآليات المحددة بالخصوص وبما ينسجم ومتطلبات قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (20) لسنة 2021.
8. مراجعة السياسات وإجراءات العمل لتحديد أوجه القصور فيها والتي كانت سببًا أو ساهمت في إحداث عملية الاحتيال المالي، وتعزيز الضوابط الرقابية للحيلولة دون تكرار حالات الاحتيال المالي.
9. جمع البيانات والمعلومات والوثائق اللازمة لمساندة الإجراءات الإدارية أو التأديبية أو غيرها من الإجراءات والملاحقة القضائية ومحاولة استرداد الأموال موضع عملية الاحتيال المالي.

د. تطبيق إجراءات العناية الواجبة المشددة المحددة لمكافحة عمليات غسل الأموال وتمويل الإرهاب تجاه حالات الاحتيال المالي وفقًا لطبيعة الاشتباه بها، وعلى أن تنفذ تلك الإجراءات في الحالات التالية:

1. عند الاشتباه بحدوث حالة احتيال.
2. عند الشك في صحة المستندات المقدمة من العملاء أو الموظفين.
3. عند تلقي مراسلة تتعلق بشبهة احتيال مالي سواء من العاملين في الشركة أو العملاء أو المؤسسات المالية أو الأطراف الثالثة أو أية جهات أخرى.
4. عند ظهور إنذار أو مؤشر تحذيري في نظام الرقابة الإلكتروني.
5. عند الوصول إلى المستفيدون من المبالغ الناتجة عن عمليات الاحتيال المالي ما أمكن ذلك.

ه. تحديد وتقييم وتوثيق مخاطر الاحتيال المالي المحتملة ذات الصلة بأنشطة الشركة وعملياتها بما في ذلك المرتبطة بتطوير منتجات أو خدمات جديدة بما في ذلك الآليات الجديدة لتقديم الخدمات أو التي قد تنشأ عن استخدام التقنيات التكنولوجية الحديثة أو قيد التطوير فيما يتعلق بكل من المنتجات الحالية والجديدة، وأيضًا المتصلة بالأطراف الثالثة المنوي التعاقد معها خصوصًا المسند لها مهام ذات طبيعة حساسة، وذلك وفق أسس مدروسة وطرق قياس كمية ونوعية ضمن نطاق العمل التعاوني مع الوحدات التنظيمية ذات العلاقة في الشركة، واقتراح الضوابط الرقابية للحد والتخفيف منها على نحو مقبول.

و. تنفيذ البرنامج السنوي لإدارة مخاطر الاحتيال المالي بالتعاون مع جميع الوحدات التنظيمية داخل الشركة، بحيث يأخذ البرنامج بالاعتبار ما يلي:

1. التعرف على مخاطر الاحتيال المالي المحتملة بكافة مصادرها وتحديدها وتقييمها.
2. التأكد من مدى التقيد بسياسة مكافحة الاحتيال المالي المعتمدة وبما يشمل التزام الأطراف الثالثة بها، وذلك من خلال إجراء الاختبارات لتقييم مدى كفاية وملاءمة الضوابط الداخلية المطبقة لإدارة مخاطر الاحتيال المالي في الشركة.
3. وضع الخطط التصحيحية في حال وجود أي قصور في الإجراءات والضوابط الرقابية اللازمة لمكافحة أية عمليات احتيال مالي محتملة والتأكد من تطبيقها بكفاءة وفاعلية.

ز. متابعة الملاحظات الواردة في تقارير البنك المركزي والسلطات التنظيمية الأخرى والمدقق الخارجي ووحدة التدقيق الداخلي وأية جهات رقابية أخرى داخل الشركة ذات صله بعمليات الاحتيال المالي واتخاذ الإجراءات اللازمة بخصوصها.

ح. نشر وتعزيز التوعية تجاه أساليب الاحتيال المالي سواء على صعيد عملاء الشركة أو العاملين فيها بشكل مستمر، بما في ذلك إعداد الأدلة أو النشرات التوعوية وعقد البرامج التدريبية للعاملين في الشركة حول مواضيع مخاطر الاحتيال المالي ومكافحته، وتعزيز قيم الاستقامة والممارسة المهنية السليمة لديهم بالشكل الذي يجعل مكافحة الاحتيال المالي هدفًا أساسيًا واجب التحقيق.

ط. الاطلاع المستمر على التقارير الصادرة عن المنظمات الدولية ذات الصلة بمكافحة الاحتيال المالي والاستفادة من الإجراءات الموصى بها وأفضل الممارسات المطبقة بالخصوص.

ي. رفع التقارير الفورية للإدارة التنفيذية العليا (بحسب مقتضى الحال) حول أي من الحالات التالية، وعلى أن تلتزم الإدارة التنفيذية العليا برفع نسخة من هذه التقارير لمجلس الإدارة أو اللجنة المنبثقة عنه التي تتولى مهام إدارة مخاطر الاحتيال المالي (إن وجدت) بشكل فوري:

1. أية عملية احتيال تعرضت لها الشركة متضمنة نتائج التحقيق والإخفاقات أو أوجه القصور التي تسببت أو ساهمت في إنجاح عملية الاحتيال المالي، والتوصيات والإجراءات التصحيحية الموصى بها.
2. اكتشاف أسلوب احتيالي أو ظاهرة احتيال جديدة والإجراءات الموصى بها لحماية الشركة من التعرض لها.

3. الكشف عن أية إخفاقات أو أوجه قصور في إدارة مخاطر الاحتيال المالي قد ينجم عنها خطورة عالية أو إجراءات قضائية أو عقوبات رقابية أو خسارة مالية أو إساءة سمعة، والتوصيات اللازمة للحد من المخاطر المترتبة على ذلك.

ك. رفع تقرير سنوي للإدارة التنفيذية العليا والتي تلتزم بدورها برفع التقرير إلى مجلس الإدارة أو اللجنة المنبثقة عنه التي تتولى مهام إدارة مخاطر الاحتيال المالي (إن وجدت)، مع مراعاة أن يتضمن هذا التقرير بحد أدنى ما يلي:

1. نتائج تنفيذ البرنامج السنوي لإدارة مخاطر الاحتيال المالي، بما في ذلك نتائج الاختبارات التي تم إجراؤها خلال فترة تنفيذ البرنامج.
2. ملخص تقرير احصائي لحالات الاحتيال المالي التي تعرضت لها الشركة، وأوجه القصور الحاصلة في إدارة مخاطر الاحتيال المالي على مستوى كافة الوحدات التنظيمية في الشركة بما في ذلك الأطراف الثالثة المتعاقدة مع الشركة.
3. تقييم مستويات الأثر لمخاطر الاحتيال (المالية وغير المالية) على الشركة.
4. الإجراءات والتدابير التصحيحية المتخذة ومدى كفايتها والتوصيات المحددة لمعالجة أوجه القصور التي تم الكشف عنها، بما في ذلك الإجراءات التأديبية الموصي بها بحق موظفي الشركة أو الإجراءات المتخذة بحق الأطراف الثالثة المتعاقدة مع الشركة.
5. التوصيات المتعلقة بمستويات التوعية تجاه مكافحة عمليات الاحتيال المالي وإدارة مخاطره على صعيد العملاء أو العاملين في الشركة بما في ذلك مدى كفاية البرامج التدريبية المخصصة للعاملين في الشركة وجودتها، وكفاية الموارد البشرية والمالية المخصصة لمكافحة عمليات الاحتيال المالي.

ل. تزويد البنك المركزي من خلال الإدارة التنفيذية العليا بنسخة من التقرير السنوي المشار إليه في الفقرة (ك) أعلاه، على أن يكون التقرير معتمد من مجلس الإدارة أو المدير الإقليمي بالنسبة لفروع الشركات الأجنبية.

م. إنشاء قاعدة بيانات (سرية ومقيدة الوصول ضمن صلاحيات محددة) تتضمن كافة التفاصيل عن حالات الاحتيال المالي الفعلية والمشتبه بها وفق تصنيفات وفئات يمكن الاستفادة منها في دراسة تلك الحالات وسبل مكافحتها، بحيث تشمل المعلومات بالحد الأدنى ما يلي:

1. الرقم المرجعي لعملية الاحتيال.

2. الوضع الراهن لعملية الاحتيال فيما إذا انتهت أو قيد التحقيق والدراسة أو نشطة وما إلى ذلك.
3. المعلومات ذات الصلة بعملية الاحتيال مثل تاريخ وقوعها، وفترتها، أسماء المحتالين والأشخاص ذوي العلاقة، الشخص المسؤول عن متابعة الحالة ضمن وحدة مكافحة الاحتيال المالي، الوحدة التنظيمية ذات العلاقة.
4. تقدير الخسائر الناتجة عن عملية الاحتيال سواء المادية أو غيرها كحجم الأثر الشامل للاحتيال على عمليات الشركة أو أداؤها.
5. طبيعة أو الهدف من عملية الاحتيال.
6. وسيلة ارتكاب عملية الاحتيال ونمطها.
7. الإجراءات التي تمت للتحقيق في عملية الاحتيال، ونتائج التقصي والتحقيق.
8. الإجراءات التصحيحية أو التأديبية، أو الملاحقات القضائية التي تمت.
9. التدابير التي تم اتخاذها لمكافحة الحالات المشابهة.

ثالثاً: إدارة مخاطر الاحتيال المالي

تعتبر جريمة الاحتيال المالي من أخطر الجرائم التي تعصف بالمجتمعات والتي تنامت مع التطورات التكنولوجية، وتعتمد هذه الجريمة على حنكة ودهاء الجاني في اتباع الأساليب والوسائل المتنوعة للإيقاع بالضحايا، وجعلهم يخضعون له ويسلموا أموالهم دون أدنى شك بأنه محتال. ويمكن أن يكون الاحتيال المالي من داخل المؤسسة المالية أو من خارجها، كما يمكن أن يكون خارجيًا وينطوي على مشاركة أو مساعدة من الداخل، فمعظم الخسائر الناتجة عن عمليات الاحتيال المالي قد تكون بسبب أشخاص يعملون لدى تلك المؤسسات في جميع المستويات الوظيفية، لذلك يتعين على المؤسسة المالية أن تأخذ بالاعتبار لدى إعداد استراتيجياتها تجاه إدارة مخاطر الاحتيال المالي أن تكون شمولية وأن تركز بصورة أساسية على الاحتيال المالي في مكان العمل بذات الأهمية التي تركز فيها على الاحتيال المالي من العميل أو الاحتيال من الغير بما يشمل الأطراف الثالثة.

الخطوة الأولى في مكافحة الاحتيال المالي تتمثل بالاقتناع بأهمية إدارة مخاطره، لذا من الضرورة بمكان أن يكون لدى الشركة خطة استراتيجية متكاملة للحماية ضد عمليات الاحتيال المالي، وذلك بالاستناد إلى أفضل الممارسات بهذا الخصوص، بحيث تشمل هذه الخطة العناصر الأساسية التالية:

1. سياسة مكافحة الاحتيال المالي.

2. تقييم مخاطر الاحتيال المالي.
3. أنظمة الرقابة الداخلية.
4. الإبلاغ عن الاحتيال المالي.
5. التحقيق بعمليات الاحتيال المالي
6. معالجة حالات الاحتيال المالي
7. نشر التوعية والتثقيف.

1. سياسة مكافحة الاحتيال المالي

لإدارة مخاطر الاحتيال المالي على نحو كفؤ وفعال، فإنه يتطلب من الشركة وضع سياسة مكتوبة وشاملة ومعتمدة من مجلس إدارتها تستهدف مكافحة الاحتيال المالي، بحيث تنظر هذه السياسة وتنظم كافة التدابير والإجراءات التي تتبعها الشركة بكافة وحداتها التنظيمية ومستوياتها الإشرافية والتنفيذية للحماية من مخاطر الاحتيال المالي سواء الداخلي أو الخارجي، بالإضافة إلى أن يكون الغرض من هذه السياسة نشر الوعي بين العاملين في الشركة حول أدوار مكافحة الاحتيال المالي، وتحديد من هو المسؤول في الشركة عن مكافحة ومراقبة الاحتيال المالي، وعن تطبيق مختلف جوانب خطة مكافحة الاحتيال المالي وضمان فاعليتها؛ من خلال اخضاعها للمتابعة والمراجعة الدورية بشكل سنوي أو كلما استدعت الحاجة ذلك، وبهذا الخصوص يلزم على الشركة مراعاة ما يلي:

أ. وضع سياسة لمكافحة الاحتيال المالي، على أن تكون معتمدة من مجلس الإدارة، ليصار بعد ذلك إلى تعميم هذه السياسة على جميع العاملين في الشركة بكافة مستوياتهم الوظيفية.

ب. أن يتم صياغة السياسة بالتعاون مع كافة الوحدات التنظيمية في الشركة كونهم الأقدر على تحديد فرص الاحتيال المالي في الأعمال التي يديرونها، وبذات المبدأ الذي يتم فيه اشراكهم في تحديد المخاطر المرتبطة بأعمالهم، حيث يساعد العمل الجماعي ونشر التوعية والثقافة حول مكافحة الاحتيال المالي في الشركة على الاستفادة من الخبرات والأفكار المجمعة.

ج. أن يتم إعداد السياسة على أساس نتائج تحليل تقييم الشركة لمخاطرها من حيث البيئة الداخلية والخارجية.

د. تضمين السياسة بأهداف الشركة حيال مكافحة الاحتيال المالي وجميع السياسات القائمة وإجراءات العمل التي تتصل بمكافحة الاحتيال المالي ومراقبته.

ه. أن تقوم الإدارة التنفيذية العليا بتبني وتنفيذ المبادرات التي تعكس بأنها القدوة بالتصرف بنزاهة والتقيد بروح ونصوص سياسة مكافحة الاحتيال المالي ومراقبته، وأنهم مدركين للمسؤولية والمساءلة عن إيجاد مناخ أخلاقي والمحافظة عليه لإحباط أي محاولة احتيال وتشجيع الإبلاغ عن أي خرق للمعايير المقبولة.

و. أن يتم توفير ما يكفي من العناصر البشرية والموارد المالية والتقنية لضمان نجاح سياسة مكافحة الاحتيال المالي، الأمر الذي سيساهم في ارسال إشارة واضحة وصريحة إلى العاملين في الشركة بأن الإدارة التنفيذية العليا لن تتهاون في موضوع مكافحة الاحتيال المالي.

ز. أن يتم تحديد صورة واضحة لجميع العاملين في الشركة حول أهمية مكافحة الاحتيال المالي ليعوا مسؤولياتهم تجاه التقيد بسياسة مكافحة الاحتيال المالي والمساهمة في الكشف والابلاغ عن أية حالات اشتباه باحتيال مالي والتحقيق بشأنه حسب مسؤوليات كل فرد منهم.

ح. أن تخضع السياسة للمراجعة الدورية وكلما استعدت الحاجة ذلك، لعكس التغييرات في بيئة الشركة التشغيلية وخدماتها، واستعراض قدرتها على تلبية الأغراض المعاد تقييمها، وذلك للحفاظ على قدرة هذه السياسة في مكافحة الاحتيال المالي على نحو كفؤ وفعال.

كما يتطلب من الشركة عند إعداد سياسة مكافحة الاحتيال المالي مراعاة أن تتضمن السياسة إجراءات العمل ذات العلاقة بمكافحة الاحتيال المالي، بحيث يتم فيها تحديد خطوات واضحة للإجراءات الواجب اتخاذها للاستجابة لحالات الاحتيال المبلغ عنها أو المشتبه بها، بالإضافة إلى تدابير منع أو تقليل عمليات الاحتيال المالي؛ بحيث تغطي كافة عمليات الاحتيال التي تعرضت أو يمكن أن تتعرض لها الشركة مستقبلاً، مع مراعاة تحديثها باستمرار بناءً على آخر المستجدات، وبحيث يمكن للموظفين أو الأطراف الثالثة ذات العلاقة الاطلاع عليها وتطبيقها كل حسب موقعه.

وتستخدم العديد من الشركات سياسة مكافحة الاحتيال المالي للإبلاغ عن التزامها بمكافحة الاحتيال المالي والتعامل معه ضمن أي سياسة من سياسات الشركة أو كسياسة منفصلة، وتهدف سياسة مكافحة الاحتيال المالي إلى حماية الشركة من خلال تحسين إدارة مخاطر الاحتيال المالي وتحديد الخطوات الواضحة التي يجب اتخاذها تجاه الاحتيال المبلغ عنه أو المشتبه به، بالإضافة إلى التدابير التي سيتم اتخاذها للحد من أو تقليل مخاطر الاحتيال المالي، وعليه لا بد من تضمين السياسة المحاور التالية كحد أدنى:

أ. أدوار ومسؤوليات مجلس الإدارة والإدارة التنفيذية العليا.

ب. أدوار ومسؤوليات لجنة مكافحة الاحتيال المالي (إن وجدت).

ج. أدوار ومسؤوليات وصلاحيات وحدة مكافحة الاحتيال المالي أو الوحدة التنظيمية المعنية بتنفيذ مهام مكافحة الاحتيال المالي.

د. أدوار ومسؤوليات الوحدات التنظيمية الأخرى داخل الشركة تجاه مكافحة الاحتيال المالي.

ه. الأسس التي تضمن لوحدة مكافحة الاحتيال المالي حق التحقيق في حالات الاحتيال المالي والتعبير والكشف عن نتائج التحقيق للإدارة التنفيذية العليا وإذا لزم الأمر لمجلس الإدارة، والإجراءات التي يتم تطبيقها قبل/ أثناء عملية التحقيق في حالات الاحتيال.

و. الإجراءات والضوابط اللازمة لرصد والكشف عن حالات الاحتيال المالي وطرق الوقاية منها.

ز. آليات وإجراءات وطرق التواصل للإبلاغ عن حالات الاشتباه بعمليات الاحتيال الداخلي، والمسؤول عن التحقيق بعمليات الاحتيال داخل الشركة، تحديد قنوات وآليات تلقي الإبلاغ عن حالات الاحتيال الخارجي وتأمين الحماية المتاحة للمُبلِّغ عن الاحتيال.

ح. أسس تقديم التقارير المتعلقة بمخاطر الاحتيال المالي للإدارة التنفيذية العليا والبنك المركزي.

ط. آلية الاخطارات وتبادل المعلومات والبيانات مع البنك المركزي والجهات المختصة الأخرى ووحدة مكافحة غسل الأموال وتمويل الإرهاب وبما ينسجم مع أحكام التشريعات النافذة.

ي. أسس وآليات حفظ السجلات والمستندات والأدلة المرتبطة بحالات الاحتيال المالي وبما يتفق مع التشريعات النافذة.

ك. أدوار ومسؤوليات وصلاحيات موظفي خدمة العملاء في الخطوط الأمامية للتعامل مع البلاغات التي ترد بشأن عمليات احتيال مالي.

ل. الأسس التي تضمن نشر وتعزيز التوعية والثقافة تجاه أساليب مكافحة الاحتيال المالي وإدارة مخاطره لعملاء الشركة أو العاملين فيها وبما يشمل المساءلة حال الإهمال أو التقصير.

م. أسس دعم وتعزيز قيم الأمانة والنزاهة والاستقامة لإحباط أي محاولة احتيال وتشجيع الإبلاغ عن أي خرق للمعايير المقبولة.

2. تقييم مخاطر الاحتيال المالي

يمثل الاحتيال المالي خطرًا من المخاطر التي تواجه الشركة، ويجب عليها التأكد من تقييمها لهذا الخطر في عملية تقييم المخاطر الكلية التي تقوم بها بشكل دوري، وذلك في سبيل التأكد من أن الإدارة التنفيذية العليا ومجلس الإدارة على دراية تامة بكافة المعلومات اللازمة لمكافحة الاحتيال المالي، بحيث تشمل هذه المراجعة

جميع وظائف وعمليات وأنظمة الشـــركة، وأنها تعالج مخاطر الاحتيال الداخلي والخارجي على حد ســـواء، وتحدد مستوى وطبيعة انكشاف الشركة لهذا الخطر، ومن ثم تحديد التدابير المضادة، ذلك أن عملية المراجعة هي الوسيلة القادرة على تحديد وتقييم المخاطر المتأصلة، وبيان التدابير التي اتخذت وتلك التي يجب اتخاذها للتقليل والتخفيف من حدة مستويات المخاطر، كما يجب الأخذ بعين الاعتبار عند وضع الضوابط الرقابية أن مصادر الاحتيال المالي قد تكون من داخل الشركة أو من خارجها، كما أن التواطؤ من الداخل يقلل من فعالية بعض الضوابط الرقابية كضوابط الفصل بين الواجبات مثلاً.

إن عملية تقييم مخاطر الاحتيال المالي تتم كأي عملية تقييم مخاطر أخرى، حيث تتكون من ثلاث أجزاء رئيسية يمكن أخذها بالاعتبار لدى تنفيذ برنامج تقييم مخاطر الاحتيال المالي وهي على النحو التالي:

أ. **تحديد مخاطر الاحتيال المتأصـــلة؛** في هذه المرحلة يتم تجميع المعلومات المتوافرة حول عمليات الاحتيال والتهديدات الإلكترونية التي يمكن أن تتعرض لها الشركة أو عملائها، وتشمل هذه العملية اعتبار جميع أنواع مخططات الاحتيال واردة الحدوث بغض النظر عن الحوافز أو الضـــغوط أو الفرص المســـببة لعملية الاحتيال، بما في ذلك الثغرات الأمنية التي قد يحدث من خلالها عمليات الاحتيال الإلكتروني.

ب. **تقييم احتمالية حدوث المخاطر وأهميتها؛** تشـــمل هذه المرحلة تقييم الاحتمالية النســـبية لحدوث التهديد/ مخطط الاحتيال والأهمية المحتملة لمخاطر عملية الاحتيال بناء على البيانات المتاحة.

ج. **الاســـتجابة لمخاطر الاحتيال واحتســـاب المخاطر المتبقية؛** في هذه المرحلة يتم احتســـاب المخاطر المتبقية بعد تطبيق الضوابط الرقابية بكافة أنواعها وتحديد نوع الاستجابة الأفضل لمعالجة المخاطر بناء على أسس واضحة كتحليل التكلفة مقابل العائد وتحديد الضوابط الواجب توفيرها بالخصوص.

هذا ولتقييم مخاطر الاحتيال المالي لا بد من التعرف على هذه المخاطر أولاً لتطوير فهم شـــامل لمشـــهد الاحتيال المالي في الشـــركة، وذلك من خلال تحديد مصـــادر البيانات الداخلية والخارجية لتحديد ومراقبة تهديدات الاحتيال الناشـــئة التي قد تتعرض لها الشـــركة أو عملائها، ويمكن للشـــركة الاعتماد على الوســـائل التالية في سبيل التعرف على مخاطر الاحتيال وتحديدها:

أ. جلسات العصف الذهني والاجتماعات المتكررة لوضع سيناريوهات الاحتيال المحتملة.

ب. تقارير التدقيق الداخلي أو الخارجي ومخرجات التحقيق في حالات الاحتيال المالي وتحليل سيناريوهات الاحتيال التي تغطي محاولات الاحتيال وعمليات الاحتيال الفعلية؛ لتحديد أساليب وتقنيات وإجراءات الاحتيال الشائعة.

ج. أنماط الاحتيال الجديدة والناشئة التي تم تحديدها بواسطة أنظمة كشف الاحتيال أو محققي الاحتيال أو وحدة مكافحة الاحتيال المالي في الشركة.

د. قواعد البيانات الخاصة بسيناريوهات الاحتيال المتاحة من قبل وحدة مراقبة الامتثال ووحدة الأمن السيبراني وإدارة الحوادث في الشركة، وفريق الاستجابة لحوادث الأمن السيبراني أو النشرات المعممة من قبل البنك المركزي والجهات المختصة الأخرى وفق ما هو صادر عن المنظمة الدولية للشرطة الدولية (الانتربول).

ه. مصادر خارجية موثوقة وذات صلة بشأن اتجاهات الاحتيال محليًا وعالميًا.

و. سيناريوهات الاحتيال المتاحة والشائعة عبر مواقع الانترنت ذات العلاقة بقطاع الدفع الإلكتروني.

ز. متابعة أبرز التوجهات في سيناريوهات الاحتيال والاختراق الإلكتروني.

الاحتيال المالي والأمن السيبراني:

على الشركة مراعاة المواءمة بين القدرات التشغيلية لوحدة مكافحة الاحتيال المالي ووحدة الأمن السيبراني لديها، وذلك من خلال ما كحد أدنى:

- تحديد الأدوار والمسؤوليات بشكل واضح بين كلا الوحدتين.
- تنفيذ التدريب المتبادل بين الوحدتين.
- تعزيز قنوات الاتصال المؤسسي بين كلا الوحدتين في سبيل تبادل المعرفة بينهما بانتظام.
- تشكيل فرق عمل مشتركة بين كلا الوحدتين لمواءمة ممارسات وقواعد العمل وتعزيز المشاركة الجماعية بينهما.
- إجراء ورش عمل مشتركة بينهما لتقييم التهديدات أو تحليل السيناريوهات المحتملة للاحتيال مع وحدات الأعمال الأخرى في الشركة لتحديد التهديدات بشكل جماعي وتبادل الأفكار بينهما في سبيل ذلك، مع تخزين المعلومات ذات العلاقة بتلك التهديدات ضمن قاعدة بيانات مركزية وتقييد الوصول إليها إلا للأشخاص ذوي العلاقة.
- تحديد الفرص لتوحيد الأنظمة والأدوات المستخدمة لرصد وكشف ومنع الاحتيال (على سبيل المثال، توفير بيانات عن مراقبة المستخدم، أو موقع العميل من خلال عنوان IP).

- تنسيق الإجراءات التصحيحية لحالات الاحتيال (على سبيل المثال، إزالة مواقع الويب الوهمية التي تم اعدادها للحصول على بيانات العملاء).
- إجراء تمارين مشتركة لاستخلاص الدروس المستفادة بأثر رجعي عقب حوادث الاحتيال التي تتعلق بالبيانات والأنظمة والعمليات والضوابط.

والاحتيال بحكم تعريفه ينطوي على سوء سلوك متعمد مصمم بطريقة تحول دون كشفه، ولهذا يجب أن يشارك فريق تقييم مخاطر الاحتيال في التفكير الاستراتيجي لتوقع سيناريوهات الاحتيال التي يمكن أن تتعرض لها الشركة، ويتطلب التفكير الاستراتيجي - والذي يعد مطلباً مهماً في تصميم إجراءات الكشف عن الاحتيال التي قد لا يتوقعها منفذ مخطط الاحتيال- عقلية متشككة والتي يمكن أن تستند إلى طرح الأسئلة التي يمكن أن تقود إلى تصميم إجراءات الكشف، ومن الأمثلة على هذه الأسئلة:

أ. كيف يمكن لمرتكب الاحتيال استغلال نقاط الضعف في بيئة عمل الشركة والضوابط المطبقة؟

ب. كيف يمكن لمنفذ عملية الاحتيال تجاوز الضوابط الرقابية المطبقة لدى الشركة؟

ج. ما الذي يمكن أن يفعله منفذ عملية الاحتيال لإخفاء العملية؟

بعد ذلك تقوم الشركة بتحديد وإدارة مخاطر الاحتيال المالي التي قد تتعرض الشركة أو عملائها لها، من خلال إجراء تقييمات شاملة لمخاطر الاحتيال المالي على مستوى الشركة ككل لتحديد وقياس مخاطر الاحتيال، والأحداث المحتمل أن تتعرض لها وقياسها (الاحتمالية والأثر)، ووضع خطط وتوصيات للتخفيف من المخاطر المتبقية قدر الإمكان، بحيث تشمل جميع الوظائف ووحدات التشغيل والأنظمة التكنولوجية في الشركة، مع مراعاة أن تستند عملية تقييم مخاطر الاحتيال المالي إلى منهجية موثقة تأخذ بالاعتبار ما يلي:

أ. تحديد أنواع الاحتيال المحتملة التي يمكن أن تتعرض لها الشركة أو عملائها من خلال تجميع المعلومات ذات العلاقة بالتهديدات الداخلية والخارجية التي يمكن أن تتم على الخدمات التي تقدمها الشركة وقنواتها الإلكترونية بما في ذلك موظفيها وأنظمتها التكنولوجية.

ب. تقييم احتمالية حدوث مخاطر الاحتيال المحتملة ومستوى تأثيرها على الشركة وعملائها في حالة حدوثها، وبحيث يؤخذ بالاعتبار لدى تقييم مخاطر الاحتيال المحتملة ما يلي:

1. مخاطر الاحتيال المحتملة سواء الداخلية (التي يمكن ارتكابها من قبل أو بمساعدة الأشخاص العاملين في الشركة) أو الخارجية (التي يمكن ارتكابها من قبل أشخاص من خارج الشركة).
2. مخاطر الخدمات والمنتجات التي تقدمها الشركة وكيفية استغلالها لارتكاب عمليات الاحتيال.

3. مخاطر العميل بما في ذلك على سبيل المثال نوع العميل وعدد العملاء ومستوى الوعي لدى العملاء بالاحتيال.
4. مخاطر القنوات الإلكترونية التي يمكن للعميل استخدامها للاتصال بالشركة أو الوصول للخدمات والمنتجات.
5. مخاطر المناطق الجغرافية بما في ذلك مخاطر استخدام الخدمات والمنتجات التي تقدمها الشركة والتي يمكن الوصول إليها في بلد أجنبي أو منطقة ذات خطورة عالية.
6. مخاطر المعاملات كتلك المرتبطة بآلية تنفيذ العمليات التشغيلية أو استلام الأموال أو تحويلها وما إلى ذلك.
7. مخاطر الأطراف الثالثة سواء الوكلاء لتقديم خدمات ومنتجات الشركة أو انشاء علاقة العمل بالنيابة عن الشركة أو لتقديم الأعمال الفنية والتقنية المتصلة بأعمال الشركة.
8. مخاطر الأنظمة التقنية داخل الشركة بما في ذلك قوائم الصلاحيات ومخططات تنفيذ الأعمال من خلالها وغير ذلك.

ج. تنفيذ عملية تقييم مخاطر الاحتيال المالي على أساس سنوي كحد أدنى بما في ذلك تحديثه كلما استدعت الحاجة ذلك وفقًا للمتغيرات التي قد تطرأ على بيئة مخاطر الاحتيال سواء الداخلية أو الخارجية، وتشمل هذه المتغيرات على سبيل المثال لا الحصر (قصور أو ضعف تم تحديده في منظومة البيئة الرقابية، المتطلبات التنظيمية الجديدة الصادرة عن البنك المركزي، المنتجات أو الخدمات أو الأعمال أو التقنيات الجديدة، قنوات جديدة للتسويق للخدمات والمنتجات، التغييرات في البيئة الداخلية للشركة مثل الهيكل التنظيمي أو تغيير الوظائف أو نقل الموظفين، المعلومات الجديدة التي تم الحصول عليها أو التي وردت للشركة ذات صلة بالاحتيال) ، وتحديث ملف مخاطر الاحتيال ومراجعته بشكل دوري.

د. التأكد من فاعلية الضوابط المعمول بها لرصد ومنع المخاطر المحتملة للاحتيال المالي، بما في ذلك فحص مواطن الضعف الداخلية لدى الشركة، والتي قد تزيد من فرص الاحتيال المالي، ومراجعة البيانات التحليلية لعمليات الاحتيال المالي كأداة وقائية وتحقيقية للكشف عن المحتالين.

ه. تحديد مخاطر الاحتيال المتبقية التي تكون الشركة معرضة لها بعد التأكد من فاعلية الضوابط المعمول بها.

و. تطوير خطط عمل لمعالجة مخاطر الاحتيال المتبقية التي تقع خارج نطاق تقبل المخاطر أو يمكن أن تؤدي إلى خرق أنظمة الشركة والقدرة على الاستجابة لها ومراقبتها باستمرار للتأكد من أن المخاطر ضمن المستوى الذي ترغب الشركة في تحمله، بحيث يراعى أن تتضمن تلك الخطط بحد أدنى ما يلي:

1. تصميم أدوات وضوابط رقابية لرصد ومكافحة مخاطر الاحتيال المتبقية والتخفيف منها لدى وقوع أحداث الاحتيال أو عدم اكتشافها في الوقت المناسب، بالإضافة إلى تقييم فعالية وكفاءة هذه الضوابط الرقابية ومراقبتها وتحديثها بشكل مستمر.
2. وضع ومراقبة مؤشرات الإنذار المبكر ومؤشرات مخاطر الاحتيال المالي الرئيسية وتطبيقها على جميع الوحدات في الشركة ومراقبتها بشكل دوري وتحليل النتائج، وإصدار تقارير دورية لاتخاذ القرار المناسب في الوقت المناسب والتخفيف من المخاطر والخسائر قدر الإمكان سواء كانت تلك المؤشرات مرتبطة بالموظفين بشكل خاص أو مرتبطة ببيئة تكنولوجيا المعلومات والاتصالات أو الإجراءات والسياسات المرتبطة بها أو بالأطراف الثالثة أو عملاء الشركة.
3. تحديد آلية الإبلاغ والتعامل مع حالات الاحتيال المالي عند اكتشافها أو الاشتباه بها.

ز. اقتراح الإجراءات والتدابير والخطط والضوابط اللازمة لمكافحة حالات الاحتيال المالي، ضمن خطة زمنية محددة.

ح. تطبيق نهج محدد للتحقيق في عمليات الاحتيال المالي والإجراءات التصحيحية لمعالجة الاحتيال بشكل مناسب وفي الوقت المناسب.

ط. متابعة تنفيذ الإجراءات التصحيحية والوقائية لمكافحة الاحتيال المالي في الشركة ضد المخاطر التي قد تم رصدها في عملية المراجعة.

ي. توثيق عملية المراجعة بالشكل الذي يمكن من الرجوع إليها بسهولة.

ك. تطوير خطة مراقبة الاحتيال المالي باستخدام المؤشرات التنبيهية التي تم رصدها من قبل الشركة.

3. إجراءات الرقابة الداخلية

تعد إجراءات الرقابة الداخلية من أهم العناصر في مكافحة الاحتيال المالي، وقد ألزمت الأطر التنظيمية الصادرة عن البنك المركزي الشركات بوضع أنظمة رقابة داخلية ضمن تلبيتها لمتطلبات الحاكمية المؤسسية، والأمر سيان في مكافحة الاحتيال المالي، حيث لا يزال يؤكد البنك المركزي على أن الاحتيال المالي خطر كباقي المخاطر التي تتعرض لها الشركة، يقابل إدارته وضع ضوابط رقابية داخلية توازي هذا الخطر.

في هذا السياق، ينبغي على الشركة وضع أنظمة رقابية داخلية موثقة، في سياسة مكتوبة، وتحديد إجراءات واضحة وشاملة لتقليص خطر الاحتيال المالي ومكافحته، يجب أن تضمن الشركة تكامل هذه الضوابط مع الإجراءات والضوابط التي تحكم أنشطة الشركة وخدماتها والعاملين فيها وعملائها والأطراف الثالثة، وكما يمكن أتمتة هذه الضوابط إلى حد كبير حسب قدرات الشركة وإمكانياتها، في حين أن هذه الضوابط موجودة لدعم الهدف العام للشركة؛ وهو التقليل من عمليات الاحتيال المالي التي قد تتعرض لها الشركة أو أطراف ثالثة متعاقد معها أو أحد عملائها، ويمكن تصنيفها على النحو التالي:

أ. **الضوابط الوقائية؛** وتشمل الخطوات المتخذة قبل حدوث الاحتيال، وترتبط بعض الضوابط الوقائية بالهيكل التنظيمي، حيث يعد الفصل بين الواجبات -أي عدم السماح لشخص واحد بالسيطرة على جميع جوانب معالجة المعاملة - بمثابة رقابة وقائية، ومن الممكن أن يتم تضمين الضوابط الوقائية الأخرى في أنظمة الشركة مثل الضوابط الأمنية والتقنية المحددة في التعليمات النافذة لا سيما المحددة في تعليمات التكيف مع المخاطر السيبرانية؛ كسياسات كلمات المرور وضوابط الوصول التي تمنع الوصول غير المصرح به إلى الأنظمة أو البيانات، والتي قد تحبط النشاط الاحتيالي قبل حدوثه، وتعد الضوابط الوقائية الطريقة الأكثر فعالية وكفاءة واقتصادية بشكل عام.

ب. **الضوابط الكشفية؛** تستخدم الضوابط الكشفية للعثور على المخالفات في حالة وجودها، وهي مصممة أيضاً لتوفير مستوى معين من التأكيد على أن الضوابط الوقائية تعمل كما هو مخطط لها، ويعد وضع ضوابط رقابية ومؤشرات على أنظمة مراقبة الحركات المالية لدى الشركة أمثلة على الضوابط الكشفية، والاعتماد على تقنيات الكشف مثل أنظمة الكشف عن التهديدات (IDS)، وهي عمومًا أكثر تكلفة وتستغرق وقتًا أطول من الضوابط الوقائية، ومع ذلك لا ينبغي التقليل من أهمية الضوابط الكشفية في التخفيف من مخاطر الاحتيال المالي.

ج. **الضوابط التصحيحية؛** تستخدم لمعالجة حالات الاحتيال المالي أو المخالفات أو الأنشطة المرتبطة بتهديد ما بعد اكتشافها أو بعد وقوع حالة الاحتيال، وقد تساعد الضوابط التصحيحية في تحسين الضوابط الوقائية والكشفية وبالتالي تحسين قدرة الشركة على الاستجابة في المرات اللاحقة.

الضوابط الوقائية:

لتتمكن الشركة من التصدي لحالات الاحتيال المالي بالاعتماد على ضوابطها في بيئة الرقابة الداخلية، فإنه يقع على عاتقها وضع وتفعيل الضوابط والإجراءات المحددة لمكافحة الاحتيال المالي والتي تم توثيقها

في سياسة مكافحة الاحتيال المالي للوقاية من مخاطر الاحتيال المالي، وأبرز الضوابط الوقائية بالخصوص ما يلي:

أ. ضمان تكامل الضوابط المحددة لمكافحة الاحتيال المالي مع الضوابط المفروضة على البيئة التشغيلية للشركة والتي تحكم جميع وظائف الشركة وخدماتها وقنواتها ومرافقها وعملائها.

ب. وضع الضوابط التي تحكم الوصول المقيد والمراقب إلى مواطن الخطر، وحصر وضبط الصلاحيات على كافة المستويات الإدارية والتنفيذية في الشركة بما في ذلك قنواتها الإلكترونية وفقًا لمواطن الخطر المتصلة بالموقع الجغرافي والعميل والقناة الإلكترونية والخدمات والمنتجات المقدمة.

ج. التوثق المحكم من هوية العميل للمصادقة على صحة هوية العميل (عاملين كحد أدنى)، وبحيث لا يقتصر فقط استخدام كلمات المرور لمرة واحدة (OTP) من خلال ارسالها عبر خاصية الرسائل القصيرة، وإنما تنفيذ عوامل إضافية وذلك في الحالات التالية على سبيل المثال لا الحصر وفقًا لدرجة خطورتها:

1. عند إنشاء علاقة العمل.
2. استخدام/ الوصول للقنوات الإلكترونية سواء تطبيق الهاتف النقال أو الموقع الإلكتروني أو غيرها.
3. تنفيذ عملية مالية أو غير مالية أخذًا بالاعتبار نوع العملية ودرجة خطورتها.
4. الموافقة على المعاملات من خلال تطبيق الهاتف النقال (على سبيل المثال إرسال إشعار فوري إلى تطبيق الهاتف النقال على جهاز معروف وموثوق به).
5. تحديد الموقع الجغرافي (على سبيل المثال التحقق من الموقع (GPS) أو عنوان الشبكة (IP) أو التحقق من شبكة الهاتف النقال المستخدمة).
6. النمط السلوكي للعميل (على سبيل المثال الاختلافات في حجم المعاملات المعتادة أو قيمتها أو تكرارها أو العملة المستخدمة).
7. اعتماد الخصائص الحيوية لجسم الانسان (على سبيل المثال بصمة الإصبع أو بصمة الوجه أو بصمة العين).
8. الملف الشخصي السلوكي البيومتري (على سبيل المثال التغييرات في الطريقة التي يستخدم بها العميل أو الموظف متصفحًا أو جهازًا آخر).

9. تغيير في إعدادات القنوات الإلكترونية الحساسة كتغيير الرقم السري أو اسم المستخدم أو غيرها من البيانات الحساسة.
10. إضافة بطاقة دفع على محفظة إلكترونية أو موقع إلكتروني وغيرها.
11. إعادة تعيين بيانات الأمان للدخول إلى القنوات الإلكترونية أو استخدام أدوات الدفع بعد محاولات فاشلة للوصول إليها أو استخدامها.
12. تفعيل تطبيق الهاتف النقال على جهاز جديد.
13. تسجيل الدخول إلى القنوات الإلكترونية من جهاز أو موقع غير معروف سابقًا.
14. تغيير بيانات صاحب الحساب (على سبيل المثال العنوان أو تفاصيل الاتصال).
15. تغيير اللغة المستخدمة في الحساب (على سبيل المثال من العربية إلى الإنجليزية).
16. إعادة تعيين كلمة المرور أو PIN.
17. إصدار وتفعيل بطاقة دفع جديدة.
18. إعادة تنشيط الحسابات الخاملة والتي يقصد بها تلك الحسابات التي لم يتم الدخول إليها من قبل العميل (Log in) خلال فترة زمنية تحددها الشركة بالخصوص وقبل أن تصبح تلك الحسابات حسابات جامدة حسب أحكام التشريعات النافذة.

د. قيام الشركة بطلب عامل مصادقة ثالث (على سبيل المثال إجراء مكالمة هاتفية (صوتية ومرئية) إلى الرقم المعرف ضمن حساب العميل، أو رقم سري لمرة واحدة OTP) وذلك في أي من الحالات التالية:

1. عند اكتشاف محاولة تسجيل دخول المستخدم إلى القنوات الإلكترونية ضمن طريقة غير معتادة (على سبيل المثال، يختلف معرف الجهاز أو الموقع عن معلومات تسجيل الدخول المعروفة سابقًا أو تم وضع علامة على عنوان IP كمخاطرة).
2. يتم توجيه المعاملة من جهاز غير موثوق به إلى مستفيد مضاف حديثًا.
3. تنفيذ سلوك أو مجموعة من الأنشطة التي قد تدل على الاحتيال أو الاستيلاء على الحساب وفقًا لسيناريوهات محددة بالخصوص.
4. تجاوز معدل حركات الدفع أو التحويل بشكل غير طبيعي (على سبيل المثال تنفيذ خمسة عمليات دفع أو تحويل للعميل في الساعة الواحدة) أخذًا بالاعتبار قيام الشركة بتقييد نشاط الحساب لحين المصادقة من هوية العميل والتحقق من موثوقية الجهاز المستخدم من العميل.

ه. ضمان أن الأفراد المسؤولين عن تنفيذ الضوابط الرقابية لمكافحة الاحتيال مستقلين بما فيه الكفاية عن الأفراد الذين يراقبون أداءها، بما في ذلك وضع الضوابط المناسبة لردع وتجنب تضارب المصالح والمعاملات مع الأطراف ذات الصلة كالشركات الخارجية ومديريها وموظفيها، بما في ذلك على سبيل المثال لا الحصر:

1. إنشاء سياسة تحدد بوضوح السلوك المحظور.
2. الحد من تدفق المعلومات بين الإدارات الداخلية والموظفين من خلال حواجز المعلومات.
3. تقديم الإرشادات والتعليمات والأمثلة على تجنب تضارب المصالح.
4. المطالبة بالإفصاح الفوري عن أي تضارب أو تضارب محتمل.

و. تضمين معايير مكافحة الاحتيال المالي الخاصة بالشركة ضوابط رقابية مصممة لمنع الاحتيال الداخلي منها ما يلي:

1. تضمين سياسة التوظيف إجراءات تضمن التأكد من نزاهة الموظف قبل تعيينه، ووضع الإجراءات الكفيلة بمتابعة سلوك الموظف ووضع المؤشرات التي تدل على وجود خلل ما في سلوك ونزاهة الموظف، كالثراء غير المبرر، والتردد في أخذ الاجازات، ورفض الترقية أو استقالته بشكل مفاجئ ودون مبررات.
2. يمكن أن تشمل الضوابط والإجراءات المحددة لمكافحة حالات الاحتيال المالي الداخلي من قبل الموظفين الاجازات الإلزامية، وتبديل برامج الموظف ومهامه على فترات غير متوقعة، وتدقيق حسابات الموظف خلال اجازته، ووضع الضوابط التي تحكم عمل ذوي القرابة أو الصلة معا، وسياسات لقبول الهدايا للكشف عن أي حالات رشوة قد تحدث.
3. حفظ وصيانة وضبط أمن الموجودات القيمة والأنظمة الحساسة والبيانات السرية لدى الشركة.
4. تطبيق مبدأ فصل الوظائف والواجبات بكل صرامة في جميع أعمال الشركة، يشمل ذلك فصل مهام الرقابة عن مهام تنفيذ الضوابط، كذلك فصل الرقابة على الموجودات عن رقابة المستندات المتعلقة بهذه الموجودات.
5. مطالبة الموظفين بالالتزام بقواعد السلوك.
6. الفصل بين الواجبات في عمليات الدفع والوفاء مدعومًا بمصفوفات تفويض موثقة.
7. الضوابط الرقابية الثنائية أو الفحص الثانوي لعملية المراقبة، مع مراجعة إضافية أو عملية الموافقة على المعاملات التي تتجاوز الحدود الموضوعة من قبل الشركة (على سبيل المثال

قيمة المعاملة أو المدفوعات لمورد جديد) أو المعاملات ذات المخاطر العالية (مثل الوصول إلى حالة الحسابات الجامدة).

8. تقييد الوصول إلى تفاصيل العميل السرية لجميع الموظفين (على سبيل المثال بيانات الاعتماد عبر الإنترنت، رسائل OTP).
9. تقييد الوصول إلى بيانات حساب العميل السرية (مثل رصيد الحساب) وذلك للوظائف التي لا تتطلب مثل هذه العمليات (كموظفي تكنولوجيا المعلومات)، أخذًا بالاعتبار عندما يكون الوصول مطلوبًا، يجب تسجيل النشاط وتخزينه بشكل آمن، وتحديد متطلبات التعامل المناسب مع البيانات السرية، وضوابط الوصول إلى ذلك وفق قوائم صلاحيات محددة ومعتمدة بالخصوص.
10. تحديد ضوابط لحماية الأمن المادي للأصول (على سبيل المثال طلب تحديد هوية الموظفين في جميع الأوقات، وتأمين وتتبع المعدات وتقييد الوصول إلى الأصول الحساسة).

ز. تضمين معايير مكافحة الاحتيال المالي الخاصة بالشركة ضوابط رقابية مصممة لمنع الاحتيال الخارجي منها ما يلي:

1. توفير خط ساخن متاح على مدار الساعة للإبلاغ عن حالات الاحتيال المشتبه فيها واتخاذ إجراءات فورية للرد على تلك الحالات (على سبيل المثال، حظر الوصول إلى الحساب أو أداة الدفع).
2. إمكانية توفير الخدمة الذاتية للعملاء لإيقاف أداة الدفع أو تجميد حساباتهم على الفور وحظر المزيد من المعاملات إذا اشتبهوا تعرض حساباتهم أو أدوات الدفع الخاصة بهم لخطر الاحتيال.
3. تحديد ومصادقة هوية العميل وضوابط إدارة الوصول للحسابات الخاصة بهم عبر الإنترنت/ الهاتف النقال والمنتجات الرقمية.
4. استخدام القوائم السوداء لفحص وحظر عناوين الانترنت وعناوين البريد الإلكتروني المشبوهة، والأجهزة التي تم اختراقها أو تلك التي تم استخدامها سابقًا للاحتيال (على سبيل المثال تطبيق الهاتف المحمول المسجل في حساب تم استخدامه لإجراء الاحتيال).
5. مطالبة مستخدمي القنوات الإلكترونية بالموافقة على تنشيط خدمة (GPS) أثناء استخدامها للسماح للشركة بمراقبة الموقع.

6. قدرة تطبيقات الهاتف النقال على اكتشاف الأجهزة التي تخضع لكسر الحماية أو الوصول (Jailbreaking or Rooting)، بالتالي حظر استخدام التطبيق أو تقييد الوصول إلى البيانات أو الميزات الحساسة.
7. فرض قيود على عمليات تسجيل الدخول للقنوات الإلكترونية المتزامنة مع أكثر من هاتف نقال أو قيود على عدد الأجهزة التي يمكن تثبيت القنوات الإلكترونية عليها والوصول إليها.
8. بناء ملفات للتعرف على سلوك العميل والقدرة على تحديد أي سلوك غير عادي، بما في ذلك مراقبة الخدمات أو المنتجات أو الحسابات الخاملة ووضع الضوابط اللازمة عند استخدامها بشكل يعزز من المصادقة على هوية العميل.
9. إرسال إخطار للعميل عند إجراء تغييرات على بيانات حسابه وذلك بالاعتماد على الرسائل النصية القصيرة على رقم هاتفه النقال المعرف ضمن الحساب أو من خلال البريد الإلكتروني أو كلاهما.
10. وضع سقوف للمعاملات الفردية واليومية والشهرية المسموح للعميل بها، ومراجعتها وتحديثها بشكل دوري عند الحاجة (على سبيل المثال مراجعة ملفات تعريف العملاء وسلوكياتهم، وحالات الاحتيال الفعلية)، مع إمكانية السماح للعميل بتحديد تلك السقوف من تلقاء نفسه.
11. تنفيذ عمليات تحقق إضافية للمصادقة على هوية العميل في أي من الحالات التالية، وبحيث تشمل عمليات التحقق كل من (معاودة الاتصال الآلي، أو الاتصال الهاتفي، أو ارسال رسالة نصية إلى رقم الهاتف النقال المسجل، استخدام القياسات الحيوية لجسم الانسان على جهاز الهاتف النقال المعرف لدى الشركة):
    أ. معاملات غير عادية (على سبيل المثال، المعاملات بعد فترة من خمول الحساب، أو عند حدوث تغييرات في سلوكيات العملاء).
    ب. أنماط غير عادية للمعاملات (على سبيل المثال، دفعات متعددة لنفس المستفيد في فترة قصيرة).
    ج. المعاملات التي تتجاوز سقف القيمة المحددة.
    د. طلبات زيادة سقف المعاملة الفردية أو اليومية.
    ه. المعاملات الأولية التي يتم تنفيذها بعد التسجيل في القنوات الإلكترونية أو تسجيل جهاز جديد.

و. المعاملات التي تتم في موقع جغرافي مرتفع المخاطر (على سبيل المثال، استخدام بيانات تحديد الموقع الجغرافي للجهاز المحمول لطلب التحقق إذا حاول المستخدم الوصول إلى المنتجات والخدمات أثناء تواجده في بلد أجنبي لا يتماشى مع ملف تعريف سلوك المستخدم).

12. التفتيش الدوري على القنوات الإلكترونية بحثًا عن أدلة على نشاط مشبوه أو أجهزة يمكن أن تعرض أمن أداة الدفع للخطر.

الضوابط الكشفية:

لتتمكن الشركة من التصدي لحالات الاحتيال المالي بالاعتماد على ضوابطها في بيئة الرقابة الداخلية، فإنه يقع على عاتقها أيضًا اعتماد وتنفيذ معايير للكشف عن حالات الاحتيال المالي التي قد تتعرض لها وبما يتماشى مع مخاطر الاحتيال التي تؤثر على الشركة وعملائها، ولتنفيذ ذلك فإنه يترتب على الشركة مراعاة ما يلي:

أ. تحديد معايير للكشف عن الاحتيال والموافقة عليها وتنفيذها على نحو يجعل الشركة قادرة على التصدي لمخاطر الاحتيال الداخلي والخارجي التي تؤثر على الشركة.

ب. مراجعة وتحديث معايير الكشف عن الاحتيال على أساس دوري والاستجابة لأي تغييرات جوهرية قد تحدث في مشهد الاحتيال أو بناء على نتائج تقييم مخاطر الاحتيال في الشركة.

ج. مراقبة الامتثال لمعايير الكشف عن الاحتيال.

د. قياس فعالية معايير الكشف عن الاحتيال والضوابط ذات الصلة وتقييمها بشكل دوري.

ه. استخدام مخرجات تقييم مخاطر الاحتيال لتحديد مكان تركز نشاط الكشف عن الاحتيال، وأن تكون الضوابط متناسبة مع مستوى المخاطر المقبول في الشركة.

و. عندما يتم تقييم مخاطر الاحتيال المتأصلة على أنها أعلى، يجب أن تتطلب معايير الكشف عن الاحتيال ضوابط كشف إضافية (على سبيل المثال، المراقبة في الوقت الحقيقي، أو مصادر البيانات الإضافية أو نماذج التعلم الآلي) أو معايير أكثر صرامة لحدود الكشف (على سبيل المثال، حدود نقدية أقل قبل التنبيه).

ز. مراعاة أن تتضمن معايير الكشف عن الاحتيال ما يلي كحد أدنى:

1. مصادر البيانات المستخدمة للإبلاغ عن الأنشطة المشبوهة والاحتيال (على سبيل المثال، سجلات العملاء، وأنظمة المعاملات، إدارة الهوية والوصول، وقواعد البيانات الخارجية).

2. الضوابط المطبقة للكشف عن نشاط احتيالي مشتبه به (على سبيل المثال، تصعيد الأحداث والمعاملات عالية الخطورة، والفحص الثانوي، والتسويات، والإبلاغ عن الاستثناءات، والتدريب الداخلي).
3. الضوابط المنفذة للكشف عن نشاط احتيالي مشتبه به يتعلق بطبيعة الحركات المالية المنفذة من قبل عملاء الشركة سواء الصادرة أو الواردة.
4. الأنظمة التقنية المطبقة لاكتشاف الاحتيال المحتمل (على سبيل المثال، برامج الكشف عن الاحتيال، والتنبيهات بشأن الأحداث أو المعاملات عالية القيمة، ومراقبة الوصول).
5. الأدوار والمسؤوليات للكشف عن الاحتيال (على سبيل المثال، صلاحيات النظام، ومراجعة حالات الاحتيال اليدوية، وترتيب وإدارة التنبيهات، ونقطة التصعيد للحوادث الكبيرة المحتملة، والإشراف والرقابة).
6. تحديد الأسباب التي تجعل أنظمة الكشف والضوابط مناسبة للمخاطر التي تواجهها الشركة.

ح. على الشركة مراعاة المتطلبات التالية عند توثيق متطلبات الأفراد والعمليات والتكنولوجيا المستخدمة للكشف عن الاحتيال:

1. بيانات نشاط الموظف (مثل الوصول إلى النظام والفواتير والمدفوعات والموافقات).
2. نشاط حساب العميل (مثل المعاملات والمدفوعات).
3. الوصول إلى حساب العميل وإدارته (على سبيل المثال، تحديد الموقع الجغرافي لتسجيل الدخول واستخدام الجهاز والتغييرات على البيانات الثابتة).
4. بيانات نشاط الطرف الثالث (على سبيل المثال، الوصول إلى واستخدام أنظمة أو بيانات الشركة، الوكالات نيابة عن العملاء، الخدمات المقدمة من الوكلاء).

ط. أن يكون لدى الشركة الموارد الكافية لإدارة المخرجات من كشف الاحتيال اليدوي والآلي (على سبيل المثال، عدد كافٍ من الموظفين لمعالجة تنبيهات العمل، والمهارات المناسبة والتدريب للموظفين لإكمال التحقيقات، ونظام سير العمل لتخصيص التنبيهات وتصنيفها).

ي. توفير أنظمة تنبيهية إلكترونية للكشف عن حالات الاحتيال لتحديد الحالات الشاذة في البيانات المتعلقة بالمعاملات أو سلوك العملاء أو الموظفين، مع مراعاة تضمينها بالمؤشرات والسيناريوهات اللازمة لذلك، وأخذاً بالاعتبار ما يلي:

1. شـمول نطاق عمل أنظمة الكشـف عن الاحتيال مراقبة منتجات العملاء وخدماتهم، والأنظمة الداخلية للمعاملات أو السلوكيات التي قد تدل على الاحتيال.
2. أن تعمل أنظمة الكشف عن الاحتيال على مدار الساعة طوال أيام الأسبوع مع توفير الموارد المناسبة لإدارة المخرجات في الوقت المناسب.
3. تطوير مصادر شاملة للبيانات لاستخدامها في الإبلاغ عن الأنشطة المشبوهة والاحتيال.
4. ضبط واختبار سيناريوهات الكشف عن الاحتيال للتحقق من أنها تعمل وفقًا لما تم تصميمه وتمكين المراقبة وفقًا لمدى تقبل المخاطر في الشركة.
5. دراسة التغذية الراجعة لمراقبة وتحسين أداء الأنظمة وفعالية السيناريوهات والمعايير من خلال مراجعة التنبيهات المزيفة.
6. مراجعة وتعريف قواعد العمل والسيناريوهات في الوقت المناسب وبشكل دوري للتأكد من أنها لا زالت مناسبة في ضوء مخرجات تقييم مخاطر الاحتيال، ولاستهداف الوقاية والكشف عن الأنماط الجديدة أو الناشئة التي تم تحديدها من خلال المراقبة المستمرة او الإخطارات الواردة.
7. اختبار فعالية الأنظمة بشكل دوري، من خلال الضبط المستمر للإعدادات ومكونات النظام مثل تعريف البيانات والتحقق من صحة المدخلات، والتحقق من صحة النموذج، واختبار فعالية السيناريو وإعداد التقارير.
8. تحديث أنماط وقواعد سلوك المستخدم لمراعاة أحدث التهديدات وأنواع الاحتيال.
9. الاحتفاظ بسجل موثق للتغييرات التي تم إجراؤها لقواعد عمل النظام وإعداداته والأساس الذي تم البناء عليه في قرار إحداث التغييرات.
10. مراقبة التغييرات غير المصرح بها على النظام (على سبيل المثال، العبث بالقواعد أو تعطيل ضوابط الرقابة).
11. أن يقتصر الوعي بقواعد عمل النظام بما في ذلك قواعد وسيناريوهات كشف الاحتيال على مجموعة محددة من الموظفين المختصين بمكافحة الاحتيال المالي، وبما لا يشمل الموظفين او الأطراف الثالثة المسؤولة عن تشغيل العمليات والضوابط الخاضعة للرقابة.

ك. تصميم وتنفيذ ضوابط لمراقبة منتجات العملاء وخدماتهم تجاه السلوكيات التي قد تدل على الاحتيال الخارجي، وكحد أدنى، يجب أن تتناول هذه السلوكيات المخاطر التي يمثلها:

1. احتيال الطرف الأول - عندما يقوم عميل الشـــركة بتقديم معلومات خاطئة عن هويته أو يقدم معلومات خاطئة لارتكاب عملية احتيال باستخدام حسابه الخاص أو أداة الدفع أو أي منتج آخر.
2. احتيال الطرف الثاني - حيث يقدم العميل معلوماته الشخصية عن قصد أو يسمح باستخدام هويته لارتكاب عملية احتيال.
3. الاحتيال من طرف ثالث - عندما يحصـــل شـــخص على بيانات العميل دون موافقته أو علمه، عندئذٍ يستخدم تلك البيانات لارتكاب عملية احتيال.

ل. تصـــميم وتنفيذ ضـــوابط لمراقبة الموظفين تجاه الحالات التي تم تحديدها في عملية تقييم مخاطر الاحتيال وتم تصـــنيفها على أنها تمثل خطر لاحتيال داخلي محتمل، بما في ذلك على ســـبيل المثال لا الحصر:

1. تدقيق مسار وصول الموظف إلى الأنظمة الأساسية للشركة.
2. سـجل نشـاط الموظفين تجاه جميع أنظمة وقواعد بيانات العملاء والمحاسـبة المالية (على سـبيل المثال، تســـجيل مســـار مراجعة موظف يقوم بإجراء تغييرات على عنوان العميل، وإضـــافة مستفيد، وإصدار تعليمات بالدفع، وإعطاء إذن بتنفيذ عملية سحب، رفع سقف التعامل).
3. مراقبة السلوكيات أو الأنشطة غير العادية (على سبيل المثال، المعاملات خارج ساعات العمل، أو عمليات الاستثناءات أو التجاوزات التي تمت بدون الموافقات المناسبة/ حسب الأصول).
4. التأكد من عملية المطابقة والتســوية بين الأنظمة المالية وأنظمة العمليات الأخرى في الشــركة، إضافة إلى تنظيم ومراجعة الحسابات المصرفية، وأيضًا التأكد من إعادة ترصيد جميع الحسابات المؤقتة في الشركة (الحسابات الوسيطة).
5. المراقبة والموافقة على استخدام وثائق مستندية أو أدوات يتم بموجبها دفع مطالبات أو تحصيل مستحقات خاصة بالشركة.
6. مراقبة شكاوى الموظفين والتسلسل الإداري المجهول.

الضوابط التصحيحية:

لتتمكن الشركة من التصدي لحالات الاحتيال المالي بالاعتماد على ضوابطها في بيئة الرقابة الداخلية، فإنه يقع على عاتقها أيضًا اعتماد وتنفيذ معايير تصحيحية لمعالجة حالات الاحتيال المالي أو المخالفات أو الأنشطة المرتبطة بتهديد ما بعد اكتشافها أو بعد وقوع حالة الاحتيال، وقد تساعد الضوابط التصحيحية في

تحسين الضوابط الوقائية والكشفية وبالتالي تحسين قدرة الشركة على الاستجابة في المرات اللاحقة، ولتنفيذ ذلك فإنه يترتب على الشركة مراعاة ما يلي:

أ. وضع وتنفيذ خطة معتمدة للاستجابة لحالات الاحتيال ومراجعتها أينما لزم الأمر، مع مراعاة مواءمتها مع عملية إدارة الحوادث التشغيلية في الشركة.

ب. مراقبة الامتثال لخطة الاستجابة لحالات الاحتيال.

ج. قياس فاعلية خطة الاستجابة لحالات الاحتيال والضوابط ذات الصلة بها وتقييمها بشكل دوري.

د. يجب أن تتطلب خطة الاستجابة لحالات الاحتيال تقييمًا سريعًا ومختصًا، والتحقق من، وحل جميع حالات الاحتيال المشتبه بها أو الفعلية.

ه. يجب أن تتضمن خطة الاستجابة لحالات الاحتيال كحد أدنى ما يلي:

1. الطرق التي يتم من خلالها تنبيه الشركة إلى الاحتيال المشتبه به أو الفعلي، بما في ذلك قنوات الإبلاغ المتاحة للعملاء والموظفين والأطراف الثالثة.
2. الأدوار والمسؤوليات العائدة على كل من الأفراد وفرق العمل للرد على حالات الاحتيال المحتملة أو الفعلية.
3. سلطة اتخاذ القرار وإجراءات التصعيد داخل وخارج الشركة بما فيها اتخاذ الإجراءات القانونية واحالتها إلى الجهات المختصة (على سبيل المثال، الإحالة إلى المتخصصين في القضايا المعقدة، والإدارة العليا للاحتيال المادي المحتمل، والمستشار القانوني الداخلي أو الخارجي إذا كانت هناك مخاوف قانونية).
4. إجراءات للاستجابة السريعة لحالات الاحتيال المحتملة التي حددتها الشركة، أو تم ابلاغها من قبل العميل أو من قبل الشركات الأخرى أو البنك المركزي أو الجهات الأخرى المختصة أو أي من الأطراف الثالثة، أخذًا بالاعتبار أن يشمل ذلك تدابير احترازية لحجز الأموال المستلمة حسب الأصول وبما يتفق والتشريعات النافذة.

و. الإجراءات التي ستتخذها الشركة عند الاشتباه في الاحتيال أو وقوعه، بما في ذلك على سبيل المثال لا الحصر:

1. تهيئة وتنسيق الموارد المناسبة لإدارة التنبيهات مع مراعاة حجم حالة الاحتيال.
2. تسجيل وإجراء تقييم أولي لجميع التنبيهات أو تقارير الاحتيال المقدمة رسميًا.

3. عندما يتم تقييم تنبيه أو حالة على أنها لا تتطلب مزيدًا من التحقيق، يجب أن يتم توثيق سبب منطقي يشرح مصوغات هذا القرار.
4. التحقيق في جميع الحالات التي يُشتبه فيها بارتكاب احتيال أو تم وقوعه.
5. آلية استخراج والاحتفاظ بالأدلة وآلية التعامل معها ونسخها وآلية تسليمها لجهات التحقيق أو الجهات القضائية، حيث يجب وضع الآليات لضمان وحفظ تكاملية المعلومات وسريتها (Data Integrity and Confidentiality).
6. الاحتفاظ بسجل شامل لجميع الأدلة والتحقيقات المتعلقة بالاحتيال المحتمل والفعلي ولمدة لا تقل عن المدة الخاصة بالاحتفاظ بالسجلات المنصوص عليها في تشريعات مكافحة غسل الأموال وتمويل الإرهاب النافذة وبما يتناسب مع المدد الواردة في التشريعات النافذة ذات العلاقة.

ز. الاجراءات التي يجب اتباعها في حالة اكتشاف واقعة احتيال محتملة خارج ساعات العمل الرسمية للشركة.

ح. عندما يتعلق الاحتيال المحتمل أو الفعلي بالخدمات والمنتجات المقدمة للعميل أو المدفوعات الخاصة بالشركة، يجب أن تطلب خطة الاستجابة لحالات الاحتيال:

1. تحديد ما إذا كانت المعاملة التي يُحتمل أن تكون احتيالية قد اكتملت أو في طور الانتهاء.
2. إذا لم تكتمل المعاملة؛ ضرورة اتخاذ إجراء فوري لحظر أو تعليق المعاملة والتنسيق بشكل استباقي مع أي جهات أخرى ذات علاقة.
3. الاستجابة بشكل استباقي للطلبات المتعلقة بالمعاملات الاحتيالية المشتبه بها عند تلقي إشعار من العميل أو شركة أخرى أو جهة مختصة أو البنك المركزي.
4. إيقاف الحساب أو أي أداة دفع مرتبطة به مثل بطاقات الدفع لمنع المزيد من المعاملات حتى اكتمال التحقيق، وعند الضرورة تتم إعادة تعيين بيانات الأمنية أو إصدار بطاقة جديدة أو فتح حساب جديد وما إلى ذلك.
5. حظر أي معاملات أخرى من/ إلى حسابات خارج الشركة قد تم استخدامها لارتكاب عملية الاحتيال.
6. التعاون مع الشركات الأخرى عند الحاجة حال تلقي طلب بإيقاف منتج وكان هناك مبررات للاشتباه بعملية احتيال ووفقا لأوامر البنك المركزي الصادرة بالخصوص.

7. الاتصـــال بالعميل أو الطرف الثالث للإبلاغ عن الإجراءات المتخذة والخطوات واجبة التنفيذ للتخفيف من عواقب الاحتيال قدر الامكان.
8. التحقق من هوية العميل قبل إعادة تنشـــيط حســـابه وأدوات الدفع المرتبطة به والتي تم إيقافها بسبب التعرض لعملية احتيالية.

ط. من المفيد قيام الشركة بتوفير نظام لإدارة حالات الاحتيال (Case Management) لإعطائها القدرة على الاســتجابة لحالات الاحتيال بشــكل كفؤ وفعال من خلال إنشــاء قاعدة بيانات لحالات الاحتيال، حيث أن مثل هذه الأنظمة سيسـهل على الشركة توثيق وتسجيل كافة البيانات والمعلومات والتنبيهات المتعلقة بحالات الاحتيال المشــتبه بها أو الفعلية ومراقبتها، وإجراءات التحقيق فيها، وحلّها، إضــافة إلى التقارير الداخلية والخارجية التي بخصـــوص حالات احتيال، مع مراعاة أن يتمتع هذا النظام بالقدرة على ما يلي:

1. تقييد وصول المستخدم إلى الأفراد والأدوار المصرح لهم فيها.
2. إنشـــاء ســـير عمل يتماشـــى مع نموذج العمليات في الشـــركة وفق قوائم صـــلاحيات محددة بالخصوص.
3. أن يكون النظام قابلاً للتعديل للتكيف مع التغييرات التي قد تحدث في نموذج عمل الشـــركة أو خطة الاستجابة لحالات الاحتيال فيها.
4. تصنيف حالات الاحتيال تجاه الوحدات المرتبطة بها.
5. تصنيف الاشتباه في حالات الاحتيال للقدرة على تحديد اتجاهات إبلاغ التقارير.
6. تتبع حالة الاحتيال ضـــمن مســـارها الكلي بدءًا من التنبيه الأولي وصـــولاً إلى معالجة الحالة واتمامها، إلى جانب كافة البيانات المتصلة بعملية الاحتيال (على سبيل المثال، الرقم التسلسلي، تاريخ التنبيه أو الإخطار الأولي، تاريخ ووقت عملية الاحتيال، اسم العميل ورقم الحساب ورقم أداة الدفع، الوســيلة/ القناة المســتخدمة في الاحتيال، الأطراف ذات العلاقة، معلومات المحتال، قيمة الاحتيال، الأساليب والأنماط المستخدمة، وغيرها).
7. تسجيل خطوات التحقيق المتبعة تجاه حالات الاحتيال.
8. العمل كقاعدة بيانات لجميع المعلومات المطلوبة للتحقيق في عملية الاحتيال وحلها (على ســبيل المثال، معلومات الأطراف ذات الصــلة، وملاحظات الحالة، والأدلة المســتندية، والتواصــل مع العملاء، والأساس المنطقي لاتخاذ القرار بشأن حالة الاحتيال).

9. نتائج تسوية عملية الاحتيال، بما في ذلك أي خسائر مترتبة وإجراءات تصحيحية مفروضة.
10. الاحتفاظ بالسجلات للفترات المنصوص عليها وفق سياسة الشركة وبما ينسجم مع التشريعات النافذة.

ي. يجب أن تتضمن الخطة الدروس المستفادة الإجراءات اللاحقة للتعامل مع حالات الاحتيال وبما يشمل وضع الإجراءات الرقابية للحد من تكرار حدوث هذه الحالات، والتحقق من تحديث سجلات المخاطر في حال أن هذه المخاطر لم تكن مشمولة بالأساس بسجل المخاطر.

وعلى الشركة التأكد من وجود عملية متابعة مستقلة ومستمرة وموثوق بها، لضمان حماية الشركة من مخاطر الاحتيال المالي بأقصى قدر ممكن، وتنقسم عملية المتابعة إلى نوعين على النحو التالي:

أ. **المتابعة الداخلية؛** وتعنى بمتابعة الضوابط الداخلية للشركة من خلال تقارير المراجعة الدورية التي ترفع لمجلس الإدارة، سواء من مهمة التدقيق الداخلي، أو أية تقارير قد يتم رفعها من الإدارة التنفيذية مرتبطة بعمليات الاحتيال في الشركة. ومن العمليات الرئيسية التي ترتبط بعمليات الاحتيال غالبًا ويجب أن تخضع لعملية المراجعة هي التأكد من عدم وجود تلاعب في حسابات الشركة، والتأكد من وجود وتفعيل الضوابط الأمنية المختلفة سواء للوصول إلى ملاك الشركة (الوصول الفيزيائي) أو للوصول لأنظمة وبيانات الشركة، ووجود برامج التوعية المناسبة وتفعيلها سواء للموظفين أو العملاء أو الأطراف الثالثة التي تتعامل معهم الشركة حيثما تطلب الأمر ذلك.

الاحتيال المالي والتدقيق الداخلي:

ترتبط وظيفة مكافحة الاحتيال المالي بوظيفة التدقيق الداخلي ارتباطًا وثيقًا، حيث يتوجب على وحدة التدقيق الداخلي في الشركة إجراء عمليات تدقيق للتحقق من أن المهام المرتبطة بوظيفة مكافحة الاحتيال المالي قد تم تنفيذها بشكل مناسب وعلى النحو المنشود، ولتحقيق هذا الترابط بشكل سليم بين الوظيفتين فإنه يتطلب الأخذ بالاعتبار ما يلي:

- ضمان تنفيذ مهام التدقيق على أعمال مكافحة الاحتيال المالي بشكل مستقل ووفقًا لمعايير التدقيق وتعليمات البنك المركزي ذات الصلة.
- تحديد دورية تنفيذ عملية التدقيق على أعمال مكافحة الاحتيال المالي على أساس النهج المستند على المخاطر وفقًا لمخرجات تقييم مخاطر الاحتيال المالي، مع وضع خطة تدقيق معتمدة بالخصوص تتناول مكونات الشركة من أفراد وعمليات وأنظمة تكنولوجية.

- قيام وظيفة التدقيق بالتأكد الدوري من تنفيذ الإجراءات التصحيحية المتعلقة بمكافحة الاحتيال المالي في الشركة وفق توصيات وحدة مكافحة الاحتيال المالي، بما في ذلك الإجراءات المحددة بموجب أوامر البنك المركزي.
- التأكد من أن موظفي وحدة التدقيق المعنيين بالتدقيق على أعمال مكافحة الاحتيال المالي لديهم المستوى المطلوب من الكفاءات والمهارات لتقييم مدى كفاية الإجراءات والعمليات والضوابط المطبقة وفق سياسة مكافحة الاحتيال المالي في الشركة.
- تضمين تقارير وظيفة التدقيق بالنتائج والتوصيات المتعلقة بعمليات التدقيق على أعمال مكافحة الاحتيال المالي، مع مراعاة متابعة الملاحظات التي أفرزتها عملية التدقيق ومراقبة مستويات تنفيذها.

ب. **المراجعة الخارجية**؛ وهنا تعتمد الشركة على جهة خارجية لتقييم مدى فاعلية الضوابط التشغيلية الداخلية، ويتأكد البنك المركزي بتقييم فاعلية أنظمة الضوابط الداخلية لدى الشركة كجزء من عملية الاشراف والرقابة على الشركات. ولضمان فاعلية عمليات المتابعة الخارجية؛ يجب أن لا تقتصر عملية المتابعة على تدقيق ضوابط المحاسبة وصحة المعلومات المالية، بل يجب أن يشمل مراجعة الضوابط التشغيلية الداخلية وصلاح الأنظمة الإدارية والضوابط الأمنية. وبالرغم من أن عملية المراجعة الخارجية لا توفر الفعالية الكافية للكشف عن الاحتيال المالي ومكافحته، إلا أنها توفر مستوى معين من الضبط من خلال تقليل خطر الاحتيال المالي نتيجة التقصير في التقيد في ضوابط الرقابة الداخلية.

4. الإبلاغ عن الاحتيال المالي

على الشركة أن تراعي توفير آليات إبلاغ واضحة ومناسبة تضمن التنسيق الكافي بشأن المسائل المتصلة بمكافحة الاحتيال المالي مع الجهات المعنية سواء داخل أو خارج الشركة بما في ذلك البنك المركزي والجهات المختصة الأخرى ووحدة مكافحة غسل الأموال وتمويل الارهاب، وبحيث تتضمن هذه الآليات ما يلي:

أ. ارتباط عملية الإبلاغ بحدوث حالات الاحتيال بمدير وحدة مكافحة الاحتيال المالي أو من ينوب عنه أو من يوازيه بالوظيفة التي تتولى القيام بمهام مكافحة الاحتيال المالي كمدير الامتثال.

ب. إبلاغ الوحدات المعنية/ الأشخاص المعنيين بالحدث بشكل فوري سواء من داخل أو خارج الشركة من خلال توفير قنوات خاصة للإبلاغ على سبيل المثال البريد الالكتروني، كتب رسمية، الأنظمة الإلكترونية وغيرها.

ج. عند ثبوت عملية الاحتيال يجب على الشركة تفعيل إجراءات التصعيد المناسبة في التحقيق في عملية الاحتيال، ويشمل ذلك، ابلاغ الشركات المالية الأخرى التي ثبت أو يشتبه بتأثرها بعملية الاحتيال للعمل بشكل مشترك على حل قضية الاحتيال ووفقا لتوجيهات البنك المركزي بالخصوص، وإبلاغ الجهة المختصة (سلطات إنفاذ القانون) حال تطلب الأمر ذلك بالاعتماد على حيثيات عملية الاحتيال، وإبلاغ البنك المركزي، وإبلاغ وحدة مكافحة غسل الأموال وتمويل الإرهاب، أخذًا بالاعتبار أن إبلاغ الشركة عن عملية الاحتيال لا يقلل من مسؤولية الشركة عن إحالة عملية الاحتيال إلى الجهات الأمنية الأخرى ذات الاختصاص، ولا يقلل من مسؤوليتها في معالجة عملية الاحتيال وتحمل تبعاتها.

د. إبلاغ مجلس الإدارة والادارة التنفيذية العليا ودائرة التدقيق الداخلي لدى حدوث الاحتيال، وبشكل مباشر بحالات الاحتيال ذات الأثر الجوهري التي تؤثر/ قد تؤثر بشكل سلبي ومباشر على أعمال الشركة حاليا أو مستقبلاً بعد اكتشاف الحدث متضمنة كافة التفاصيل ذات العلاقة بالإضافة الى التقارير الدورية التي يتم تزويدهم بها.

ه. وضع البرامج الكفيلة بتدريب الموظفين بوضوح على هيكلية نظام الإبلاغ وإجراءات التعامل مع الإبلاغ عن النشاط الاحتيالي، والإجراءات الوقائية لحماية المبلغين عن عمليات الاشتباه في الاحتيال، كما على الشركة ضمان إدراك الموظف لأهمية الإبلاغ عن عمليات الاحتيال بما في ذلك الفاشلة منها، فالمحاولة الفاشلة بخطورة المحاولة الناجحة فهي في حال لم يتم الإبلاغ عنها توفر للمحتال فرصة الاستفادة من التجربة الأولى للمحاولة مرة أخرى.

و. توعية العملاء حول أساليب الاحتيال، وآليات الإبلاغ التي يمكن لهم من خلالها الإبلاغ عن اشتباههم بعملية احتيال عليهم أو في حال تم الاحتيال عليهم، وتوقيت الإبلاغ وأهمية الإبلاغ في السرعة الممكنة وعدم تأجيل ذلك، ومدى المسؤولية التي سيتحملها العميل في حال تأخر عن الإبلاغ أو عدمه والخسائر المادية التي قد يتعرض لها.

ز. كجزء من نظام الإبلاغ عن الاحتيال، على الشركة تطوير آليات وسياسات مناسبة لمساندة المشتكين وحمايتهم من عمليات الانتقام نتيجة الإبلاغ عن نشاطات الاحتيال كسياسة دق ناقوس الخطر، وأن لا

يشـمل البلاغات الكيدية وتلك التي رفعت عن سـوء نية، واتخاذ الإجراءات اللازمة لإزالة المخاوف لدى الموظفين من الإبلاغ عن عمليات الاحتيال المشتبه بها.

5. التحقيق في عمليات الاحتيال

بعد تلقي الشركة بلاغاً عن عملية احتيال، أو اكتشاف ذلك، يتطلب من الشركة هنا بدء التحقيق في عملية الاحتيال، وهنا يحتاج فريق الشـركة المسـؤول عن التحقيق في الحادثة إلى العمل بتكاتف مع جميع الأطراف المعنية وضـمن ضـوابط الأمن والسـرية بحيث لا يؤثر حدث الاختراق أو الاحتيال على سـمعة الشـركة واستمرارية أعمالها ولضمان استمرار اعتقاد المحتال بأنه لم يتم اكتشافه بعد. وفي سبيل ذلك يقع على عاتق الشركة القيام بما يلي:

أ. التأكد من وجود إجراءات واضحة ورسمية للتحقيق في أي عملية احتيال، وتدريب الموظفين عليها، وفي هذا الخصوص يجب على الشركة بحد أدنى ضمان ما يلي:

1. الاحتفاظ بسـجلات لجميع حالات الاحتيال المكشـوف عنها والتحقيقات التي تمت ووضـع أنظمة لمتابعة التحقيق والابلاغ عن وضعه ونتائجه وتحديثه بشكل مناسب.
2. توضـيح مسـؤوليات الشـخص الذي يتلقى بلاغًا عن عملية احتيال مشـتبه به أو مكشـوف ضـمن إرشادات وسياسة الشركة في مكافحة الاحتيال، وتشمل تلك المسؤوليات، تسجيل جميع تفاصيل البلاغ أو الاشتباه بأسرع وقت في ملف سري يشـار إليه كتقرير قضـية، وتشمل هذه التفاصيل بحد أدنى:
   - تاريخ ووقت البلاغ أو الحادث أو الاشتباه.
   - اسم المبلغ/ المشتكي.
   - تفاصيل الاتصالات وقناة الإبلاغ المستخدمة.
   - طبيعة البلاغ.
   - وقت أو فترة الاحتيال المزعوم.
   - ظروف جريمة الاحتيال المبلغ عنها.
   - مرتكب عملية الاحتيال في حال تم كشفه.
   - مبلغ الاحتيال والاداة أو القناة التي تم عليها الاحتيال.
   - أي بلاغ كتابي أو وثائق معززة تم تقديمها في عملية الإبلاغ (يجب ختمها وتوثيقها).

ب. عادة ما يكون هناك عدد من الأدلة يمكن للشركة الاستناد إليها في اتخاذ القرارات أثناء التحقيق في حادثة الاحتيال ومن هذه الأدلة:

1. بيانات تحديد الموقع الجغرافي: تحديد الموقع الجغرافي لموقع إتمام العملية والتأكد من ملاءمتها مع موقع السكن الخاص بالعميل أو موقع عمله.
2. مواعيد إتمام الحركة: هل كان وقتًا معقولاً من اليوم بالنسبة إلى العميل، أو متناسب مع الأدلة الأخرى مثل الموقع الجغرافي.
3. عنوان الانترنت الخاص بالعميل (IP address): هل تطابق عنوان الانترنت للمشتري مع عنوان العميل إذا لم يكن الأمر كذلك فقد يشير هذا إلى أن العملية كانت احتيالية.
4. خدمات الحماية المقدمة من الشركات العالمية (3D Secure) مثل (Verified by Visa) أو (MasterCard Secure Code) والتأكد هل تم استخدام مثل هذه التقنيات أثناء المعاملة.
5. المؤشرات السلوكية: هل تبدو الحركة غير معتادة نظراً لنمط سلوك العميل المعتاد.
6. نشاط الحساب: هل كانت هذه حادثة لمرة واحدة أم كانت هناك مجموعة من المعاملات غير المصرح بها مرتبطة بحساب العميل.

ج. بعد إجراء التقييم الأولي لحالة الاحتيال بناء على جميع البيانات الاستدلالية التي تم جمعها، تتخذ الشركة قرارها بشأن عملية الاحتيال، والذي يشمل التوصل إلى واحدة من الاستنتاجات التالية:

1. لا أساس للشكوى ولا لزوم لأي إجراء لاحق.
2. القضية يجب أن تحال إلى مدير أعلى أو إلى الوحدة المسؤولة عن التحقيق في عمليات الاحتيال لدى الشركة.
3. القضية بحاجة إلى أخذ مشورة من البنك المركزي أو وحدة الجرائم الإلكترونية أو غيرها من الجهات المختصة الأخرى.

د. يتم تسجيل القرار في تقرير القضية إلى جانب ما يلي:

1. سبب القرار ومبرراته.
2. الأساس الذي تم الاستناد عليه في اتخاذ القرار.
3. الإجراءات الواجب اتخاذها (إذا وجدت).
4. الشخص أو الجهة الخارجية المسؤولة عن اتخاذ إجراء لاحق.
5. اسم ومنصب الشخص الذي اتخذ القرار.

6. تاريخ القرار.
7. الخيارات المتاحة لمعالجة قضـــية الاحتيال، بما في ذلك الخيارات المطروحة حول تولي جهة أخرى مستقلة يتم الاستعانة بها في التحقيق والموارد والخبرات المطلوبة.

ه. في حال تم أخذ قرار بالســير بعملية التحقيق في حالة احتيال مشــبوهة، يجب على مســؤول عملية التحقيق (اللجنة المشكلة بالخصوص) وضع خطة للتحقيق تأخذ بعين الاعتبار ما يلي:

1. نطاق وشروط التحقيق.
2. القضايا والأمور المحددة الواجب استقصاؤها.
3. تحديد المجالات التشغيلية والموظفين الرئيسيين الذين سيشتركون في عملية التحقيق.
4. تحديد الخبرة المختصة أو المساندة المطلوبة.

و. على مسؤول عملية التحقيق أن يعيد باستمرار تقييم عملية التحقيق ومدى الحاجة إلى إبلاغ الجهات التنظيمية الأخرى بما في ذلك ســلطات إنفاذ القانون، وإبقاء الإدارة التنفيذية العليا على اطلاع بآخر المستجدات بعملية التحقيق.

ز. الاحتفاظ بكافة الأدلة المرتبطة بعملية الاحتيال، وحمايتها من التلف والضياع والتلاعب وحفظها في أماكن آمنة، كذلك الاحتفاظ بنســخ عن وثائق عملية التحقيق، مع الاحتفاظ بســجلات تحدد كل من تعامل بهذه الأدلة.

ح. الاحتفاظ بتقارير عملية الاحتيال لمدة خمس ســنوات في مكاتبها، وفي حال تم تخزينها بشــكل إلكتروني، يجب أن تلبي هذه الســجلات شــروط الســجل الإلكتروني المنصــوص عليها بموجب التشريعات النافذة.

ط. بعد الانتهاء من عملية التحقيق السير بإجراءات تقييم الضـوابط الداخلية لمنع تكرار عملية الاحتيال مستقبلا، واتخاذ الإجراءات اللازمة لاسترداد عائدات جريمة الاحتيال في حال وجدت.

6. معالجة حالات الاحتيال المالي

على الشـركة مراعاة وضـع واعتماد وتنفيذ ومراجعة إجراءات لتحديد السـبب الرئيسـي لحدوث عملية الاحتيال المالي، واستخلاص الدروس المستفادة منها واتخاذ الإجراءات التصحيحية لمنع تكرارها مستقبلاً، وبهذا الخصوص يقع على عاتق الشركة ما يلي:

أ. عند السعي نحو تحديد السبب الرئيسي في حدوث حالة الاحتيال المالي، فإنه يتوجب على الشركة الأخذ بالاعتبار ما يلي:

1. فهم نقطة القصور/ الخلل/ الانتهاك (على سبيل المثال، القناة التي تم استخدامها لارتكاب عملية الاحتيال أو السيطرة على حساب/ أداة الدفع).
2. تحديد ما إذا كان من الممكن أن تكون أطراف أخرى متورطة في عملية الاحتيال (على سبيل المثال، موظفي الشركة من خلال التواطؤ أو أشخاص معروفين للعميل).
3. مراجعة ما إذا كانت إجراءات الرقابة الوقائية قد فشلت أو تجاوزها الموظف.
4. تقييم ما إذا كان قد تم تحديد عملية الاحتيال بشكل استباقي عن طريق الرصد والبحث أو من خلال الاعتماد على إخطار العميل التفاعلي أو إخطار من الأطراق الثالثة، او إخطار من الجهات المختصة بما في ذلك البنك المركزي.

ب. بعد تحديد السبب الرئيسي لحدوث عملية الاحتيال، يجب على الشركة وضع الآليات المناسبة لتحديد الدروس المستفادة والإبلاغ بالإجراءات التصحيحية لمنع تكرار مثل هذا الحالات الاحتيالية مستقبلاً، على أن تراعي هذه الآليات كحد أدنى ما يلي:

1. تجميع البيانات التي قد تدعم تحليل الأنماط المتبعة في تنفيذ حالات الاحتيال.
2. تقييم ما إذا كانت هناك فجوة أو قصور في إطار البيئة الرقابية الداخلية القائم حالياً.
3. تحديد ما إذا كانت الإدارات الأخرى في الشركة لديها نفس نقاط الضعف.
4. تقييم ما إذا كانت المشكلة يمكن أن تؤثر على الشركات الأخرى ومشاركتها بالمعلومات ذات الصلة التي قد تمنع تكرارها (على سبيل المثال، مواقع الويب المزيفة التي تنتحل هوية الجهات الحكومية أو حسابات وسائل التواصل الاجتماعي).
5. توثيق الإجراءات التصحيحية لمعالجة السبب الرئيسي لحدوث عملية الاحتيال ومنع تكرارها.

ج. على الشركة اتخاذ إجراءات تصحيحية لمعالجة السبب الرئيسي لحدوث عملية الاحتيال وكذلك الآثار التي نتجت عنها، والتي قد تشمل على سبيل المثال لا الحصر:

1. تنفيذ قواعد عمل أو ضوابط رقابية جديدة أو تعزيز القواعد والضوابط الموجودة.
2. تعزيز مجالات التدريب أو توصيل مواد توعوية جديدة لتحسين وعي الموظف أو العميل أو الطرف الثالث.

3. إعادة وضع العميل محل ضحية الاحتيال إلى الوضع الذي كان عليه قبل وقوع حدث الاحتيال وفق نتائج التحقيق فيها (على سبيل المثال، استرداد الأموال المسروقة).
4. تقديم الدعم للعميل محل ضحية الاحتيال (على سبيل المثال، الإبلاغ عن الخطوات التالية، وتقديم بطاقة جديدة، وتوفير التوعية المناسبة).
5. محاولة استرداد أموال أو أصول محل الاحتيال لصالح الشركة.
6. الخروج من علاقة العمل مع العميل أو الطرف ثالث إذا تبين ارتباطهما بمرتكب عملية الاحتيال.
7. اتخاذ إجراء تأديبي بحق الموظف إذا ارتبط بعملية احتيال داخلي، وكذلك اتخاذ اجراء اداري بحق أي طرف ثالث مرتبط بعملية احتيال.

د. قيام إدارة مكافحة الاحتيال المالي بتتبع مدى قبول الإجراءات التصحيحية الجديدة وتنفيذها مع التصعيد إلى لجنة مكافحة الاحتيال حال رفض الإجراءات من قبل الإدارات التنفيذية في الشركة أو تأخير تنفيذ الإجراءات التصحيحية.

7. نشر التوعية والتثقيف

على الشركة أن تدرك بأن مساهمة الموظفين والعملاء في مكافحة الاحتيال هو أمر أساسي وأن أغلب حالات الاحتيال لن يتم كشفها أو مراقبتها بدون تعاون الموظفين أو العملاء، ولذلك تدعو الحاجة إلى زيادة وعي هاتين الفئتين وتعزيز التزامهما بمكافحة الاحتيال، وذلك من خلال سلسلة من المبادرات المستمرة وعلى النحو التالي:

أ. وضع وتنفيذ برامج تدريبية متكاملة للموظفين لتعريفهم بالاحتيال وأشكاله وأساليبه وآليات الإبلاغ عنه ومخاطره، ودور ومسؤولية كل شخص في الشركة تجاه مكافحة الاحتيال ومراقبته، مع ضرورة استخدام أمثلة واقعية (قدر الإمكان) ذات صلة بعمليات الشركة مستخلصة من حالات فعلية واجهت الشركة أو شركات أخرى.

ب. إعداد حلقات توعوية وجلسات نقاشية دورية لموظفي الشركة حول أنظمة المراقبة والأمن في الشركة، وسياسة الشركة في مكافحة الاحتيال، والمسؤوليات والأخلاق المرتبطة بمكافحة الاحتيال، وقواعد السلوك والابلاغ عن الاحتيال، والتأكيد على الموظفين أن تعاونهم يسهم بشكل مباشر بتفعيل سياسة مكافحة الاحتيال المالي.

ج. وضع برامج دورية لتوعية وتثقيف العملاء وموظفي الشركة حول أساليب الاحتيال المالي والقائمة والمتجددة منها، مع مراعاة تحديد الأدوات والأسلوب الأمثل للتوعية وفقًا لكل فئة أو صنف من العملاء أو الموظفين، ليصار بعد ذلك إلى قياس مدى فاعلية وكفاءة أدوات التوعية وبناء المؤشرات القياسية ووضع التوجهات اللازمة لرفع مستوى الوعي بالاحتيال المالي.

د. استخدام كافة الطرق المتاحة والمناسبة لإيصال الرسائل التوعوية للفئات المستهدفة حول أساليب الاحتيال وطرق الحماية منها، ومن هذه الطرق على سبيل المثال الكتيبات الارشادية والرسائل النصية ووسائل الإعلان المرئية والمسموعة ومواقع التواصل الاجتماعي.

ه. مراقبة ومتابعة مصادر المعلومات حول أساليب الاحتيال المستحدثة والسلوك الأفضل للتغلب عليها، وتوزيع المعلومات ذات الصلة للموظفين والعملاء.

و. تعزيز وعي العملاء حول مخاطر التعرض للاحتيال المالي، ومسؤوليتهم تجاه الشركة في حال اكتشاف تعرضهم لعملية الاحتيال المالي، وسبل الحماية من عمليات الاحتيال المالي.

ملحق (1): أمثلة على أبرز حالات الاحتيال المالي في نظام المدفوعات الوطني

ملحق (2): إرشادات عامة للعملاء للحماية من مخاطر الاحتيال

.....

ملحق (1)

أمثلة على أبرز حالات الاحتيال المالي في نظام المدفوعات الوطني

في هذا الملحق، نسلط الضوء على أبرز مؤشرات وأنماط حالات الاحتيال المالي التي تعرضت لها مكونات نظام المدفوعات الوطني والتي تم رصدها وتحليلها من قبل الشركات التي تقدم خدمات الدفع الإلكتروني أو إدارة وتشغيل أنظمة الدفع الإلكترونية وتم إبلاغ البنك المركزي بها، بالإضافة إلى الحالات التي يمكن أن تحدث نظرًا للطبيعة الإلكترونية لأنظمة وأدوات وقنوات الدفع، والممارسات في مجال الاحتيال الإلكتروني.

الاحتيال عبر سرقة الهوية

- استخدام بيانات مزورة لفتح حسابات بنكية وذلك من خلال استغلال ضعف منظومة فتح الحسابات عن بعد لدى البنك.
- فتح حسابات نقود إلكترونية باستخدام معلومات وهمية ووثائق مزورة من خلال استغلال ضعف منظومة فتح الحسابات عن بعد لدى الشركة.

الاحتيال عبر منتج المحافظ الإلكترونية

في هذا النوع من القنوات عادة ما تشمل عمليات الاحتيال على استخدام الهندسة الاجتماعية للوصول إلى بيانات صاحب المحفظة الإلكترونية وسحب رصيدها أو استخدامها في عمليات غير مشروعة، ومن الأمثلة على عمليات الاحتيال في هذه القناة:

- الاحتيال على العملاء من خلال اقناعهم بتحويل مبلغ مالي من خلال محافظ الإلكترونية إلى محفظة المحتال لغايات الحصول على دعم أو مساعدات مالية.
- استغلال نقاط ضعف أو خلل تقني لدى الشركة وتحويل مبالغ بين المحافظ الإلكترونية دون خصمها من المرسل.
- احتيال الوكلاء على مقدمي خدمات الدفع من خلال تنفيذ حركات إيداع متكررة لغايات الحصول على عمولات إضافية.

التصيد الاحتيالي (Phishing)

- يقوم المحتالون بإنشـــاء موقع إلكتروني للتصـــيّد الاحتيالي لجهة خارجية يبدو مثل موقع إلكتروني رسمي، مثل موقع إلكتروني لأحد البنوك أو موقع للتجارة الإلكترونية أو محرك بحث، وما إلى ذلك.
- يتم تعميم الروابط إلى هذه المواقع من قبل المحتالين من خلال خدمة الرســائل القصــيرة (SMS)/ وسائل التواصل الاجتماعي/ البريد الإلكتروني/ المراسلة الفورية، إلخ.
- يقوم العديد من العملاء بالنقر فوق الرابط دون التحقق من معلومات الموقع (URL) وإدخال بياناتهم الحســاســة مثل رقم التعريف الشــخصــي (PIN) وكلمة المرور لمرة واحدة (OTP) وكلمة المرور وما إلى ذلك، والتي يتم التقاطها واستخدامها من قبل المحتالين.

مكالمات التصيد (Vishing)

- يتصــل المحتالون بالعملاء أو يتواصــلون معهم من خلال مكالمة هاتفية أو عبر وســائل التواصــل الاجتماعي متنكرين كمصــرفيين أو مديرين تنفيذيين في شــركة دفع أو وكلاء تأمين أو مســؤولين حكوميين، إلخ. وذلك لاكتساب الثقة، حيث يشارك المحتالون بعض تفاصيل العملاء مثل اسم العميل أو تاريخ ميلاده.
- في بعض الحالات، يضغط المحتالون / يخدعون العملاء لمشاركة تفاصيل سرية مثل كلمات المرور أو رقم التعريف الشخصي (PIN) أو كلمة السر المستخدمة لمرة واحدة (OTP) أو رقم التحقق من البطاقة (CVV) وما إلى ذلك، من خلال الاســتشــهاد بحالة طوارئ مثل الحاجة إلى حظر معاملة غير مصرح بها، أو الدفع لوقف بعض العقوبات أو الغرامات، أو تقديم خصم جذاب، وما إلى ذلك، ثم يتم استخدام بيانات الاعتماد هذه للاحتيال على العملاء.

الاحتيال بسبب استخدام تطبيقات غير معروفة/ لم يتم التحقق منها

- ينشر المحتالون عبر الرسائل القصيرة / البريد الإلكتروني / وسائل التواصل الاجتماعي / المراسلة الفورية، وما إلى ذلك، روابط تطبيقات معينة مقنعة لتبدو مشــابهة للتطبيقات الحالية للكيانات المعتمدة.
- يخدع المحتالون العميل للنقر على هذه الروابط مما يؤدي إلى تنزيل تطبيقات غير معروفة / لم يتم التحقق منها على الهاتف النقال أو جهاز الكمبيوتر الخاص بالعميل وما إلى ذلك.

- بمجرد تنزيل التطبيق الضار، يحصل المحتال على وصول كامل إلى جهاز العميل. يتضمن ذلك التفاصيل السرية المخزنة على الجهاز والرسائل / كلمات المرور لمرة واحدة المستلمة قبل وبعد تثبيت هذه التطبيقات.

الاحتيال عبر سرقة بيانات بطاقات الدفع من خلال أجهزة الصراف الآلي

- يقوم المحتالون بتثبيت أجهزة القشط (النسخ) في أجهزة الصراف الآلي وسرقة البيانات من بطاقة العميل.
- قد يقوم المحتالون أيضًا بتثبيت لوحة مفاتيح وهمية أو كاميرا صغيرة، مخفية جيدًا عن الأنظار لالتقاط رقم التعريف الشخصي (PIN).
- في بعض الأحيان، قد يتظاهر المحتالون بكونهم عملاء آخرين يقفون بالقرب من العميل للوصول إلى رقم التعريف الشخصي عندما يقوم العميل بإدخاله في جهاز الصراف الآلي.
- تُستخدم هذه البيانات بعد ذلك لإنشاء بطاقة مكررة وسحب الأموال من حساب العميل.

احتيال من خلال مسح رمز الاستجابة السريعة (QR)

- غالبًا ما يتصل المحتالون بالعملاء تحت ذرائع مختلفة ويخدعونهم لمسح رموز الاستجابة السريعة (QR) باستخدام التطبيقات الموجودة على هواتف العملاء.
- من خلال مسح رموز الاستجابة هذه، قد يأذن العملاء للمحتالين عن غير قصد بسحب الأموال من حساباتهم.

الاحتيال عن طريق اليانصيب

- يرسل المحتالون رسائل بريد إلكتروني أو يجرون مكالمات هاتفية تفيد بأن العميل قد ربح يانصيباً ضخماً. ومع ذلك، من أجل الحصول على الأموال، يطلب المحتالون من العملاء تأكيد هويتهم عن طريق إدخال تفاصيل حسابهم المصرفي أو بطاقة الائتمان الخاصة بهم على موقع ويب يتم من خلاله التقاط المحتالين للبيانات.
- يطلب المحتالون أيضًا من العملاء دفع ضرائب أو رسوم تداول مقدماً أو دفع رسوم الشحن، ورسوم المعالجة أو المناولة، وما إلى ذلك، لتلقي اليانصيب أو المنتج.

- قد يتظاهر المحتالون في بعض الحالات أيضًا بأنهم ممثلون للبنك المركزي أو بنك أجنبي أو شركة أو مؤسسة مالية دولية ويطلبون من العميل تحويل مبلغ صغير نسبياً من أجل الحصول على مبلغ أكبر بالعملة الأجنبية من تلك المؤسسة.
- نظراً لأن الأموال المطلوبة تمثل عموماً نسبة صغيرة جداً من اليانصيب أو الجائزة الموعودة، يقع العميل في فخ المحتال ويقوم بالدفع.

الاحتيال عبر الرسائل القصيرة / البريد الإلكتروني / الرسائل الفورية / الرسائل الخادعة

- يقوم المحتالون بتوزيع الرسائل المزيفة في تطبيقات المراسلة الفورية أو الرسائل القصيرة أو منصات التواصل الاجتماعي على قروض جذابة واستخدام شعار أي شركة أو بنك معروف كصورة للملف الشخصي في رقم الهاتف المحمول الذي يتم مشاركته من قبلهم لتحقيق المصداقية.
- قد يقوم المحتالون بمشاركة بطاقة أو هوية رسمية مزيفة.
- بعد إرسال مثل هذه الرسائل الجماعية أو الرسائل القصيرة أو رسائل البريد الإلكتروني، يتصل المحتالون بأشخاص عشوائيين ويشاركون رسائل عقوبات مزيفة ونسخ من الشيكات المزيفة وما إلى ذلك مع العميل، ويطالبون برسوم مختلفة، بمجرد أن يدفع العميل هذه الرسوم، يهرب المحتالون بالمال.

عمليات الاحتيال القائمة على الرسائل النصية المستخدمة لمرة واحدة (OTP)

- يقوم المحتالون الذين ينتحلون صفة الشركة المالية أو البنك بإرسال رسائل نصية قصيرة تقدم قروضًا أو تعزز حد الائتمان على حسابات قروض عملاء الشركة أو البنوك، والطلب من العملاء الاتصال بهم على رقم هاتف محمول.
- عندما يتصل العملاء بهذه الأرقام، يطلب المحتالون منهم ملء استمارات لجمع بيانات الاعتماد المالية الخاصة بهم، ويقوم المحتالون بعد ذلك بإقناع العملاء بمشاركة تفاصيل كلمة المرور لمرة واحدة أو رقم التعريف الشخصي وإجراء عمليات تحويل غير مصرح بها من حسابات العملاء.

مخططات بونزي (Ponzi) والتسويق الهرمي أو الشبكي

- يستخدم المحتالون مخططات بونزي والتسويق الهرمي للوعد بأموال سهلة أو سريعة عند تسجيل أو إضافة الأعضاء وذلك من خلال استخدام منصات الكترونية بالخصوص.

- لا تضمن المخططات عوائد عالية فحسب، بل تدفع أيضًا الأقساط القليلة الأولى لكسب ثقة الأشخاص وجذب المزيد من المستثمرين من خلال الدعاية الشفهية.
- تشجع المخططات إضافة المزيد من الأشخاص إلى السلسلة أو المجموعة، بحيث يتم دفع العمولة للمسجل عن عدد الأشخاص الذين ينضمون إلى النظام، وليس مقابل بيع المنتجات.
- يصبح هذا النموذج غير مستدام بعد مرور بعض الوقت عندما يبدأ عدد الأشخاص المنضمين إلى النظام في الانخفاض. بعد ذلك، يغلق المحتالون المخطط ويختفون بالمال الذي استثمره الناس حتى ذلك الحين.

.....

ملحق (2)

إرشادات عامة للعملاء للحماية من مخاطر الاحتيال المالي

يتحمل العميل جزء كبير من مسؤولية حماية نفسه من الاحتيال المالي، وبهذا الصدد ندرج بعض الارشادات التي يجب على العملاء الانتباه لها لحماية أنفسهم من الوقوع ضحية لأي عملية احتيال مالي، حيث يجب على العميل التذكر دائمًا أن الاحتيال المالي عملية تبدأ خطواتها باستجابة منه، وأن تجنب عمليات الاحتيال المالي تبدأ بعدم الاستجابة إلى أي طرف مجهول يطلب منه الإفصاح عن بياناته المالية والشخصية مهما بدى موثوقًا له؛ فالثقة سلاح المحتال لطمأنت العميل وإقناعه بمصداقيته. هذا ويمكن للشركات الاستفادة منها لدى تنفيذ برامجها التوعوية لعملائها حول الاحتيال المالي.

روابط التصيّد

- لا تنقر على روابط غير معروفة أو لم يتم التحقق منها وقم على الفور بحذف الرسائل القصيرة أو البريد الإلكتروني المرسل من قبل شخص غير معروف لتجنب الوصول إليها عن طريق الخطأ في المستقبل.
- قم بإلغاء الاشتراك في رسائل البريد التي توفر روابط إلى موقع إلكتروني لبنك أو موقع تجارة إلكترونية أو محرك بحث وحظر معرف البريد الإلكتروني الخاص بالمرسل، قبل حذف رسائل البريد الإلكتروني هذه.
- اذهب دائمًا إلى الموقع الرسمي للبنك أو مقدم الخدمة الذي تتعامل معه، وتحقق بعناية من تفاصيل موقع البنك أو الشركة الإلكتروني، خاصةً عندما يتطلب ذلك إدخال بيانات الأمن السرية، وتحقق من وجود العلامة الآمنة (https مع رمز القفل) على الموقع الإلكتروني قبل إدخال البيانات الأمنية السرية.
- تحقق من عناوين المواقع الإلكترونية (URL) وأسماء المجالات (Domain) الواردة في رسائل البريد الإلكتروني بحثًا عن الأخطاء الإملائية، وفي حالة الاشتباه، أبلغ عن ذلك.

التصيد عبر المكالمات الصوتية

- لا يطلب مسؤولو البنك والمؤسسات المالية أو البنك المركزي أو أي كيان رسمي من العملاء أبدًا مشاركة المعلومات السرية مثل اسم المستخدم / كلمة المرور / تفاصيل البطاقة / OTP / CVV.
- لا تشارك هذه التفاصيل السرية أبدًا مع أي شخص، حتى مع أفراد عائلتك وأصدقائك.

.....

التصيد عبر تطبيقات غير معروفة / لم يتم التحقق منها

- لا تقم مطلقًا بتنزيل تطبيق من أي مصـــادر لم يتم التحقق منها أو غير معروفة أو عند إرشـــادك من قبل شخص مجهول.
- كممارســـة حكيمة قبل التنزيل، تحقق من ناشـــري أو مالكي التطبيق الذي يتم تنزيله بالإضـــافة إلى تقييمات المستخدمين الخاصة به وما إلى ذلك.
- أثناء تنزيل أحد التطبيقات، تحقق من الأذونات وأذونات الوصـــول إلى البيانات التي يطلبها، مثل جهات الاتصـــال والصـــور وما إلى ذلك، امنح فقط تلك الأذونات المطلوبة تمامًا لاســـتخدام التطبيق المطلوب.

التصيد عبر رموز الاستجابة السريعة (QR Code)

- كن حذراً أثناء مسـح رمز الاسـتجابة السـريعة (QR) ضـوئيًا باسـتخدام أي تطبيق دفع، قد تحتوي رموز (QR) على تفاصيل حساب مضمنة فيها لتحويل الأموال إلى حساب معين.
- لا تقم أبدًا بمســـح أي رمز (QR) لتلقي الأموال، لا تتطلب المعاملات التي تنطوي على اســـتلام الأموال مسـح الرموز الشـريطية، أو رموز الاسـتجابة السـريعة أو إدخال رقم التعريف الشـخصـي للخدمات المصرفية عبر الهاتف المحمول (PIN) وكلمات المرور وما إلى ذلك.

سرقة بيانات البطاقات من خلال أجهزة الصراف الآلي

- تأكد دائمًا من عدم وجود جهاز إضـافي متصـل، أو بالقرب من فتحة إدخال البطاقة أو لوحة المفاتيح بجهاز الصراف الآلي، قبل إجراء أي معاملة.
- قم بتغطية لوحة المفاتيح بيدك الأخرى أثناء إدخال رقم التعريف الشخصي.
- لا تقم بكتابة رقم التعريف الشخصي على بطاقة الدفع الخاصة بك.
- لا تقم بإدخال رقم التعريف الشخصي في وجود أي شخص آخر/ غير معروف بالقرب منك.
- لا تقم بإعطاء بطاقة الصراف الآلي الخاصة بك لأي شخص لسحب النقود.
- لا تقم باتباع التعليمات التي يقدمها أي شـخص مجهول أو أخذ المسـاعدة أو الإرشـاد من الغرباء أو الأشخاص المجهولين عند أجهزة الصراف الآلي.
- في حالة عدم صـرف النقود في جهاز الصـراف الآلي، قم بالضـغط على زر "إلغاء" وانتظار ظهور الشاشة الرئيسية قبل مغادرة الصراف الآلي.

- **الاحتيال عبر اليانصيب**

- احذر من عمليات اليانصيب أو العروض التي لا تصدق، لا أحد يعطي أموالًا مجانية، خاصة المبالغ الضخمة من المال.
- لا تقم بتنفيذ مدفوعات أو مشـــاركة بيانات آمنة رداً على أي مكالمات أو رســـائل بريد إلكتروني في اليانصيب.
- البنك المركزي لا يفتح أبدًا حســـابات أفراد للجمهور أو يأخذ ودائع منهم، ولا يطلب منهم مطلقاً بيانات الأمنية السرية الخاصة بهم، وأن هذه الرسائل احتيالية.
- عدم الرد أبدًا على الرســـائل التي تعرض أو تعد بجوائز مالية، ومســـاعدات حكومية مقابل تحديث بيانات اعرف عميلك (KYC) لتلقي أموال الجوائز من البنوك والمؤسسات وما إلى ذلك.

- **الاحتيال عبر الرسائل المستخدمة لمرة واحدة (OTP)**

- لا تقم بمشـاركة رقم التعريف الشـخصـي (PIN) وكلمة المرور لمرة واحدة (OTP) أو التفاصـيل الشخصية، وما إلى ذلك، بأي شكل من الأشكال مع أي شخص، بما في ذلك الأصدقاء وأفراد العائلة.
- تحقق بانتظام من الرسـائل القصـيرة ورسـائل البريد الإلكتروني للتأكد من عدم إنشـاء (OTP) دون علمك المسبق.
- قم بالوصـول إلى الموقع الرسـمي للبنك أو الشـركة أو مقدم خدمة المحفظة الإلكترونية أو الاتصـال بالفرع للاستفادة من خدماتهم والبحث عن المعلومات والتوضيحات المتعلقة بالمنتجات والخدمات.

- **الاحتيال عبر مخططات بونزي والتسويق الهرمي**

- العوائد تتناسب مع المخاطر. كلما زاد العائد، زادت المخاطر.
- أي مخطط يقدم عوائد عالية بشكل غير عادي (40-50٪) باستمرار يمكن أن يكون أول علامة على احتيال محتمل ويجب توخي الحذر.
- لاحظ أن أي دفعة أو عمولة أو مكافأة أو نســبة مئوية من الربح بدون البيع الفعلي للســلع أو الخدمة أمر مشبوه وقد يؤدي إلى الاحتيال.
- لا تنجذب إلى وعود العوائد المرتفعة التي تقدمها الكيانات التي تدير التسويق الهرمي.

- **أمن جهاز الهاتف النقال أو الكمبيوتر**

- قم بتغيير كلمات المرور على فترات منتظمة.

- قم بتثبيت برنامج مكافحة الفيروسات على أجهزتك وتثبيت التحديثات متى توفرت.
- قم دائمًا بفحص وحدات التخزين كوحدات (USB) غير المعروفة قبل الاستخدام.
- لا تترك جهازك مفتوحًا.
- فعل القفل التلقائي للجهاز بعد وقت محدد.
- لا تقم بتثبيت أي تطبيقات أو برامج غير معروفة على هاتفك أو جهاز الكمبيوتر.
- لا تخزن كلمات المرور أو المعلومات السرية على الأجهزة.

تصفح الإنترنت بأمان

- تجنب زيارة المواقع الإلكترونية غير الآمنة وغير المعروفة.
- تجنب استخدام متصفحات غير معروفة.
- تجنب حفظ كلمات المرور على الأجهزة العامة.
- تجنب إدخال بيانات أمنية على المواقع الإلكترونية أو الأجهزة العامة غير المعروفة.
- لا تشارك المعلومات الخاصة مع أي شخص، ولا سيما الأشخاص غير المعروفين على وسائل التواصل الاجتماعي.
- تحقق دائمًا من أمان أي صفحة إلكترونية بالتأكد من وجود علامتي (https ورمز قفل لوحة)، أكثر من ذلك عند إعادة توجيه رابط بريد إلكتروني أو رسالة نصية قصيرة إلى هذه الصفحات.

للحصول على خدمات مصرفية آمنة عبر الإنترنت

- استخدم دائمًا لوحة المفاتيح الافتراضية على الأجهزة العامة، حيث يمكن أيضًا التقاط ضغطات المفاتيح من خلال الأجهزة المخترقة ولوحة المفاتيح وما إلى ذلك.
- قم بتسجيل الخروج من جلسة الخدمات المصرفية عبر الإنترنت مباشرة بعد الاستخدام.
- تحديث كلمات المرور بشكل دوري.
- لا تستخدم كلمات المرور نفسها للبريد الإلكتروني والخدمات المصرفية عبر الإنترنت.
- تجنب استخدام المحطات الطرفية العامة (مثل مقهى الإنترنت، وما إلى ذلك) للمعاملات المالية.

العوامل التي تشير إلى أنه يتم التجسس على الهاتف

- يتم تنزيل تطبيقات غير مألوفة على الهاتف.
- استنزاف أسرع من المعتاد لبطارية الهاتف.

- قد يكون ارتفاع درجة حرارة الهاتف علامة على قيام شخص ما بالتجسس عن طريق تشغيل برنامج تجسس في الخلفية.
- قد تكون الزيادة غير المعتادة في مقدار استهلاك البيانات أحياناً علامة على تشغيل برنامج تجسس في الخلفية.
- قد تتداخل تطبيقات برامج التجسس أحيانًا مع عملية إيقاف تشغيل الهاتف بحيث يفشل الجهاز في إيقاف التشغيل بشكل صحيح أو يستغرق وقتًا طويلاً بشكل غير عادي للقيام بذلك.
- لاحظ أنه يمكن لبرامج التجسس والبرامج الضارة استخدام الرسائل النصية لإرسال البيانات واستلامها.

الإجراءات الواجب اتخاذها بعد وقوع الاحتيال

- قم بإعلام بنك أو شركتك مباشر دون تأجيل.
- أحظر ليس فقط بطاقة الخصم وبطاقة الائتمان ولكن أيضًا قم بإيقاف الخصم من الحساب المصرفي المرتبط بالبطاقة عن طريق زيارة فرعك أو الاتصال برقم خدمة العملاء الرسمي المتاح على موقع البنك الإلكتروني.
- تحقق وتأكد من سلامة القنوات المصرفية الأخرى مثل (Internet Banking) و (Mobile Banking) وما إلى ذلك، لمنع استمرار الاحتيال بمجرد حظر بطاقات الخصم والائتمان وما إلى ذلك بعد عملية احتيال.

الاحتياطات المتعلقة ببطاقات الدفع

- يجب عليك إلغاء تنشيط الميزات المختلفة لبطاقة الائتمان / الخصم، أي المعاملات عبر الإنترنت لكل من المعاملات المحلية والدولية، في حالة عدم رغبتك في استخدام البطاقة لفترة من الوقت وتفعيلها فقط عندما يكون استخدام البطاقة مطلوبًا.
- وبالمثل، يجب إلغاء تنشيط ميزة الاتصال بالحقل القريب (NFC)، في حالة عدم استخدام البطاقة.
- قبل إدخال رقم التعريف الشخصي في أي موقع من مواقع نقاط البيع (POS) أو أثناء استخدام البطاقة في قارئ NFC، يجب عليك التحقق بعناية من المبلغ المعروض على شاشة جهاز نقطة البيع وقارئ NFC.
- لا تدع التاجر يأخذ البطاقة بعيدًا عن عينيك لتمريرها أثناء إجراء المعاملة.

.....

لأمن كلمة المرور

- استخدم مزيجًا من الأحرف الأبجدية الرقمية والرموز الخاصة في كلمة مرورك.
- احتفظ بمصادقة ثنائية لجميع حساباتك، إذا كانت هذه التسهيلات متاحة.
- قم بتغيير كلمات المرور الخاصة بك بشكل دوري.
- تجنب كتابة تاريخ ميلادك واسم زوجتك ورقم السيارة وما إلى ذلك ككلمات مرور.

كيف تعرف ما إذا كان البنك أو الشركة مرخص أم لا؟

- تحقق مما إذا كان اسم البنك أو الشركة يظهر في قائمة البنوك والشركات المرخصة المتاحة على موقع البنك المركزي ضمن تبويب أنظمة الدفع.
- يجب أن تعرض الشركة بشكل بارز ترخيصها الصادرة عن البنك المركزي على موقعها الإلكتروني.

إرشادات عامة

- احتفظ برقم التعريف الشخصي (PIN) وكلمة المرور ورقم بطاقة الائتمان أو الخصم ورقم (CVV) وما إلى ذلك، بشكل خاص ولا تشارك المعلومات الأمنية السرية مع البنوك أو المؤسسات المالية أو الأصدقاء أو حتى أفراد العائلة.
- تجنب حفظ تفاصيل البطاقة على مواقع إلكترونية أو الأجهزة أو أجهزة الكمبيوتر العامة.
- قم بتشغيل التوثق المحكم من خلال عاملين حيثما تتوفر هذه الميزة.
- لا تقم مطلقًا بفتح أو الرد على رسائل البريد الإلكتروني الواردة من مصادر غير معروفة لأنها قد تحتوي على مرفقات مشبوهة أو روابط تصيد احتيالي.
- لا تشارك نسخًا من دفتر الشيكات ووثائق اعرف عميلك مع الغرباء.

"انتهى"