وحدة المعلومات المالية
Financial Intelligence Unit

جرائم الاحتيال – الأنماط والاتجاهات

تقرير تحليل استراتيجي

وحدة المعلومات المالية لدولة الإمارات العربية المتحدة - صندوق بريد 854 - البرج الدولي - شارع الكرامة، أبوظبي.

رقم الهاتف: +97126919955

البريد الإلكتروني: uaefiu@uaefiu.gov.ae

جدول المحتويات

الهدف

يُعدُّ هذا المشروع جزءاً من منهجية وخطة التحليل الاستراتيجي التي اعتمدتها وحدة المعلومات المالية لدولة الإمارات العربية المتحدة ("وحدة المعلومات المالية")، ويأخذ أيضاً في الاعتبار متطلبات ***"التقييم الوطني لمخاطر غسل الأموال وتمويل الإرهاب المتأصلة بدولة الإمارات العربية المتحدة"*** و ***"خطة عمل دولة الإمارات العربية المتحدة الوطنية لتطبيق الاستراتيجية الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب"***.

يعرض هذا التقرير نتائج التحليل الاستراتيجي المتعلق بأنماط واتجاهات وأساليب الجرائم الاحتيالية، بجانب المخاطر المصاحبة التي تم التعرّف عليها أثناء التحليل.

والغرض من هذا التقرير هو:

- تعزيز المعرفة ورفع الوعي بأنواع وسمات عمليات الاحتيال.
- فهم طبيعة وكيفية حدوث عمليات الاحتيال.
- التعرّف على أنماط، واتجاهات وأساليب العمليات الاحتيالية وأنواعها المتكررة.
- رفع مستويات الوعي والمعرفة بهذه الظاهرة في القطاعين العام والخاص.

المنهجية

تم إجراء التحليل الاستراتيجي بناء على "منهجية التحليل الاستراتيجي" المعتمدة لدى "وحدة المعلومات المالية"، بما يضمن منهاجاً منظّماً وشاملاً قائماً على المخاطر، يهدف إلى تطوير البيانات والمعلومات الأولية وتحويلها إلى مخرجات وفرضيات ومعلومات يمكن استخدامها في تحديد وتحديث السياسات واتخاذ القرارات، وأيضا تطوير الأنشطة التشغيلية.

وتستند التحليلات والنتائج المبيّنة في هذا التقرير إلى البيانات والمعلومات التي تحتفظ بها وحدة المعلومات المالية، بالإضافة إلى بيانات ومعلومات أخرى يتم الحصول عليها من جهات او مصادر أخرى سواء كانت على الصعيد المحلي او الدولي، خلال الفترة 2019-2021.[1]

مقدمـة

يشير مصطلح "**الجرائم المالية**"، بوجه عام، إلى الجرائم التي يرتكبها شخص أو مجموعة من الأشخاص والتي تتضمن الاستيلاء على أموال أو ممتلكات أخرى تعود لشخص آخر، بغرض تحقيق مكاسب شخصية (مالية أو مهنية) بغير وجه حق. كما يُعرف عن الجرائم المالية أنها تتسق نسبياً مع جرائم أخرى، منها على سبيل المثال لا الحصر، الاحتيال، والجرائم الإلكترونية، وغسل الأموال، وتمويل الإرهاب.

تشكّل جرائم الاحتيال تهديدا على المستوى العالمي، وبينما تتسارع معدلات انتشارها على نحو مثير للقلق، تتصاعد أيضاً الخسائر التقديرية الناجمة عنها. ومن ثم، يتعيّن على السلطات والجهات الرقابية والإشرافية ومؤسسات القطاع المالي والقطاعات الأخرى ذات الصلة، أن تعي وتفهم طبيعة المخاطر المحيطة بهذه النوعية من الجرائم، وتشرع في اتخاذ الإجراءات والتدابير اللازمة لحماية نفسها وحماية عملائها.

[1] تشمل البيانات والمعلومات التي يتم تحليلها، على سبيل المثال لا الحصر، تقارير المعاملات المشبوهة، وقواعد معلومات الأنشطة المشبوهة، ومعلومات تم استلامها من سلطات محلية اخرى، ومعلومات تم استلامها من وحدات معلومات مالية نظيرة، ومن الجهات المبلغة.

ولأسباب تتعلق بطبيعة الجرائم المالية، يصعب تتبع أو تحديد حجم غسل الأموال المرتبط بها. فعلى سبيل المثال، أشار "مكتب الأمم المتحدة المعني بالمخدرات والجريمة" إلى أن " الطبيعة السريّة لعمليات غسل الأموال تجعل من الصعب التوصل إلى تقدير دقيق للمبلغ الإجمالي الذي يتم غسله كل عام على المستوى العالمي. والتقدير الأكثر شيوعاً للأموال التي يتم غسلها على مستوى العالم في السنة الواحدة هو ما يتراوح بين 2 إلى 5% من الناتج المحلي الإجمالي العالمي، أي 800 مليار إلى 2 تريليون دولار أمريكي.[2]

ووفقاً لمعلومات متاحة للعامة، أوردت بعض التقارير أن إجمالي خسائر الجرائم المالية قد تجاوز الثلاثة (3) تريليون دولار أمريكي[3]. وحسب التقديرات[4]، فإن خسائر التجارة الإلكترونية ذات الصلة بـ "عمليات الاحتيال في معاملات الدفع الإلكتروني" على مستوى العالم قُدرت بحوالي 20 مليار دولار أمريكي في سنة 2021. بينما قُدّر في المملكة المتحدة، أن 92 مليون جنيه إسترليني قد فقدت من خلال عمليات احتيال في تطبيقات المواعدة في سنة 2021 وحدها.

وفي دولة الإمارات العربية المتحدة بات الاحتيال محل تركيز واهتمام باعتباره واحداً من الجرائم الأكثر شيوعاً التي تواجه النظام المالي. وتُرتكب الجرائم الاحتيالية كل يوم تقريباً وتبدو كخطر يواجه كافة الحكومات في جميع أنحاء العالم وتحاول جميعها مكافحته. وبينما تجهد سلطات إنفاذ القانون والكيانات الأخرى ذات الصلة في تعقّب ومقاضاة مرتكبي الجرائم المالية، يعكف المحتالون على تطوير أساليب أكثر تعقيداً لارتكاب هذه الجرائم.

وقد بلغت الخسائر التقديرية المتعلقة بـ "تحويل الأموال الاحتيالي" العالمية (وفقاً لمعلومات تم جمعها من الكيانات التي ترفع التقارير، بجانب تقارير الأنشطة المشبوهة التي تسلمتها وحدة المعلومات المالية) حوالي **152 مليون درهم في سنة 2020**، و**132 مليون في سنة 2021**. بينما بلغت الخسائر ذات الصلة بـ "تحويل الأموال الاحتيالي" المحلية حوالي **154 مليون درهم في سنة 2020**، و**162 مليون درهم في سنة 2021**.[5]

ووفقاً لمعلومات تم استلامها من مصرف الإمارات العربية المتحدة المركزي، بلغ عدد الشكاوى المستلمة ذات الصلة بـ "الاحتيال" 668 شكوى في سنة 2019، و812 شكوى في سنة 2020، و973 شكوى في سنة 2021.وقد تضمن معظم هذه الشكاوى عمليات احتيال ذات صلة بـ "البطاقات"، تليها عمليات احتيال تتعلق بـ "حسابات البنوك" بينما تعلقت بقية الشكاوى بعمليات احتيال وقعت من خلال خدمات أخرى توفرها المؤسسات المالية.

[2] https://www.unodc.org/
[3] https://www.clari5.com/
[4] https://www.statista.com/
[5] تستند التقديرات إلى المعلومات التي تم جمعها من الجهات التي ترفع التقارير وكذلك التحليل المنفّذ بشأن التقارير المشبوهة المستلمة من قبل وحدة المعلومات المالية لدولة الإمارات العربية المتحدة.

خلفية

الاحتيال جريمة جنائية تشير إلى الخداع المتعمّد الذي يستهدف الحصول على أو كسب ربح غير عادل أو غير مشروع، أو التجريد أو الحرمان من حقوق ملكية الأموال. ويتضمن الاحتيال تحريف الحقائق أما بالكلمات او بالأفعال، أو حجب المعلومات المهمة، أو حتى بتصريحات كاذبة يدلي بها طرف (الجاني) لطرف ما، متسبباً في خسائر مالية أو غير مالية أو محتملة لطرف آخر (الضحية).

وفي السياق القانوني يعتبر الاحتيال فعل جنائي، ولدى الدول أطر قانونية تفرض عادة عقوبات جنائية ومدنية على مرتكبيه. وهنالك عناصر يتعين أن تتوفر لتعريف الأفعال الاحتيالية. ولأجل أن تسمى حادثة ما "احتيالاً" يجب أن تكون بعض العناصر الأساسية حاضرة، على سبيل المثال لا الحصر:

- خداع متعمد (أي تصريح كاذب، أو تحريف للحقائق)
- النيّة (نية الجاني تجريد الضحية من شيء، عادة ما يكون مالاً/أصولاً قابلة للاستبدال)
- الضرر (تكبد الضحية خسائر محتملة أو فعلية بسبب النشاط الاحتيالي)

وبجانب العناصر الواردة أعلاه، قد تؤدي بعض الظروف الأخرى إلى وقوع عمليات الاحتيال. فهنالك فرضية قديمة استحدثها عالم جريمة معروف تسمى "مثلث الاحتيال"، وتسلّط هذه الفرضية الضوء على ثلاثة عوامل تهدف إلى فهم أسباب ارتكاب جريمة الاحتيال. وتتضمن هذه العوامل الثلاث: أولاً "الفرصة" وثانياً "الدافع" أو "الضغط" وأخيراً "التبرير". وفي سياق المؤسسات المالية، عادة ما يعمد المحتالون إلى استغلال نقاط الضعف والفجوات في ثلاثة عوامل: أولاً كونهم موظفون في المؤسسة، ثانياً السياسات والإجراءات الداخلية، وثالثاً البنية التحتية للنظم.

وكما سبقت الإشارة، فإن بإمكان فرد أو مجموعة من الأفراد ارتكاب جريمة الاحتيال، بل حتى مجموعات أكبر حجماً تعرف بـ "جرائم الاحتيال المنظّمة" أو "مجموعات الاحتيال الإجرامية" وبما أن هنالك أنواع لا تحصى من عمليات الاحتيال تنشأ كل يوم، فإن هذا التقرير سيكتفي بعرض أنماط وأساليب الاحتيال الرئيسية التي تم التعرّف عليها من قبل وحدة المعلومات المالية لدولة الإمارات، وسيورد أمثلة لحالات منقحة توضّح المخططات الاحتيالية التي تم التعرّف عليها.

ويرتكز التحليل المقدم في هذا التقرير إلى نطاق واسع من البيانات والمعلومات، بما في ذلك، على سبيل المثال لا الحصر، قواعد البيانات المملوكة لوحدة المعلومات المالية لدولة الإمارات أو متاح لها إمكانية الوصول إليها مباشرة، خاصة قواعد بيانات تقارير المعلومات المشبوهة، وتقارير الأنشطة المشبوهة، بالإضافة إلى طلبات البيانات والمعلومات الواردة إلى وحدة المعلومات المالية من السلطات المحلية او الدولية، مثل النيابة العامة الاتحادية، وإدارات الشرطة المحلية، ووحدات المعلومات المالية النظيرة، خاصة خلال الفترة **2019-2020**.

نود التنويه أيضا بأنه تم طلب معلومات إضافية من مجموعة مختارة من الجهات المبلّغة (الكيانات الي ترفع تقارير المعاملات المشبوهة)، والتي زوّدت وحدة المعلومات المالية بمدخلات مفيدة تسهم في التحليلات المستمرة وفي التعرف على الأنماط ذات الصلة، بجانب بعض من عوامل المخاطر ذات الصلة.

نظرة عامة على البيانات والمعلومات ذات الصلة التي يقوم عليها التحليل الاستراتيجي

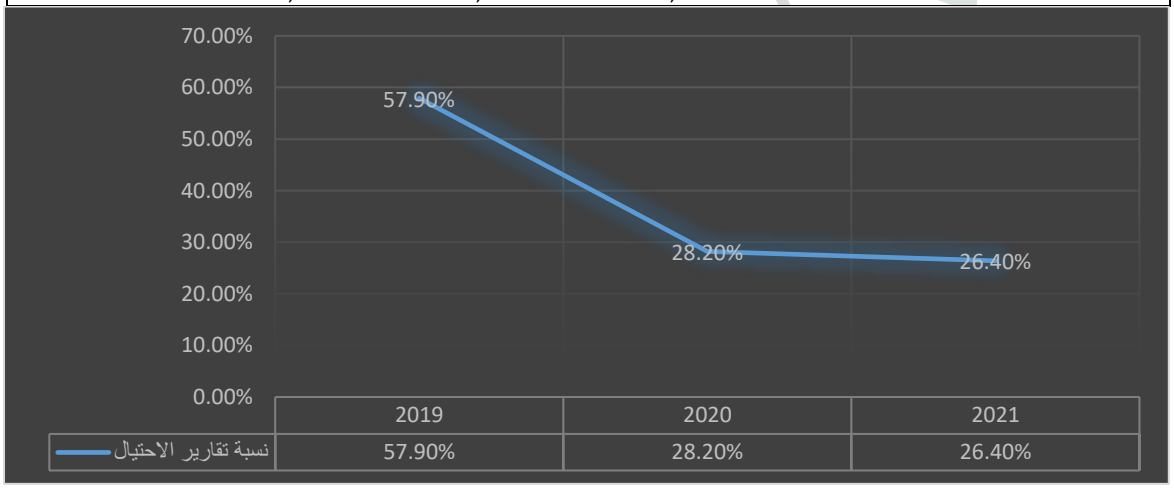
1. مراجعة وتحليل التقارير المشبوهة التي تسلمتها وحدة المعلومات المالية

خلال الفترة من سنة 2019 حتى 2021، تسلمت وحدة المعلومات المالية لدولة الإمارات تقارير مشبوهة بلغت في إجمالها **49,469** تقريراً، وتضمنت **تقارير معاملات مشبوهة، وتقارير أنشطة مشبوهة**. وقد لوحظ أن هنالك زيادة لا تخفى في أرقام تقارير المعاملات المشبوهة وتقارير الأنشطة المشبوهة خلال الفترة المذكورة، كما لوحظ انخفاض في عدد التقارير ذات الصلة بـ "الاحتيال". ويمكن أن يعزى ذلك إلى:

- جهود السلطات الرقابية، وجهود سلطات إنفاذ القانون ووحدة المعلومات المالية لدولة الإمارات في زيادة الوعي بعمليات "الاحتيال" في القطاع المالي بدولة الإمارات العربية المتحدة؛
- الإجراءات التي تم اتخاذها من قبل سلطات إنفاذ القانون بحق الأطراف المتورطة في عمليات الاحتيال؛
- جهود وحدة المعلومات المالية لدولة الإمارات في وقف دفع الأموال المتحصلة من عمليات الاحتيال.

ويظهر الجدول أدناه النسب المئوية للتقارير ذات الصلة بالاحتيال التي تسلمتها وحدة المعلومات المالية لدولة الإمارات، مقارنة بمجمل التقارير المشبوهة.

السنة	نظام الإبلاغ عن المعاملات المشبوهة القديم	goAML	إجمالي تقارير المعاملات المشبوهة/الأنشطة المشبوهة ذات الصلة بالاحتيال	إجمالي تقارير المعاملات المشبوهة/الأنشطة المشبوهة المستلمة	نسبة تقارير الاحتيال
2019	6,167	1,300	7,467	12,880	**57.9%**
2020	-	4,659	4,659	16,522	**28.2%**
2021	-	5,294	5,294	20,067	**26.4%**



ملحوظة: لا يتضمن الجدول أعلاه أنواع التقارير الأخرى المشمولة في نظام goAML (مثل تقرير معاملات الدول عالية المخاطر، وتقرير أنشطة الدول عالية المخاطر، وتقرير مطابقة الاسم الجزئية، وتقرير تجميد الأموال) ولكنه يأخذ فقط في الاعتبار تقارير المعاملات والأنشطة المشبوهة.

وعند النظر إلى "سبب الإبلاغ" الذي يتم اختياره من قبل الكيانات المرسلة للتقارير المتعلقة بتقارير المعاملات المشبوهة/الأنشطة المشبوهة ذات الصلة، لوحظ أن غالبية التقارير المستلمة (39%) في سنة 2021 كانت تتعلق

بـ "عمليات الاحتيال"، تليها بنسبة (26%) بشأن "طلبات استرداد الأموال المحلية" وتقديرات متقاربة جداً بنسبة 14% و13%، تتعلق بـ "عمليات احتيال بنكية الكترونية/الاستحواذ على الحساب" و "طلبات استرداد الأموال الدولية"، على التوالي.

أسباب الإبلاغ	النسبة المئوية من مجمل تقارير الاحتيال (بناء على أسباب الإبلاغ)		
	2019	2020	2021
يقوم العميل بتحويل الأموال نيابة عن أطراف ثالثة غير ذات صلة مقابل عمولة- عملية احتيال محتملة في تحويل الأموال.	2%	2%	2%
عملية احتيال – احتيال برسوم مقدمة/احتيال من خلال تصيّد أو بريد إلكتروني/احتيال ميراث/احتيال جوائز زائفة/احتيال في العلاقات العاطفية.	48%	51%	39%
احتيال- إعادة تقديم طلب قرض سبق أن تم رفضه، مع تغييرات رئيسية في تفاصيل المقترض، من مقترض فرد إلى شركة، وقد يحدد هذا النشاط الشخص نفسه وهو يحاول الحصول على قرض على نحو احتيالي من خلال شخص ليس له وجود.	0%	0%	0%
احتيال- عمليات الاحتيال من خلال أجهزة الصرف الآلي/سرقة بيانات البطاقات	1%	0%	0%
احتيال- أنشطة احتيالية في مجال الأعمال الخيرية/التبرعات	1%	3%	0%
احتيال- شيكات مودعة من حساب غسل أموال محتمل تبدو موقّعة مسبقاً، وتحمل خطأ مختلفاً في حقل التوقيع وفي حقل المستفيد- شيكات مزيّفة.	2%	0%	0%
احتيال – احتيال مؤسسي	0%	1%	1%
احتيال – عميل يقدم سجل زائف عن شغله وظيفة سابقة أو حالية في نموذج طلب قرض.	2%	1%	2%
احتيال – عميل يحاول إخفاء/تزييف مستندات إثبات هوية أو يرفض تقديم نسخ أصلية للتثبت.	3%	2%	2%
احتيال- موظف يقوم تكراراً بتجاوز الضوابط الداخلية أو صلاحيات الموافقة المعتمدة، أو يلتف على السياسات (احتيال الموظفين).	1%	0%	0%
احتيال- مطالبات تأمين زائفة/احتيالية	0%	0%	0%
احتيال- تزييف الشيكات المصدّقة، والشيكات المصرفية أو الشيكات غير النقدية المسحوبة على حساب مقترض/بائعين بدلاً عن حساب مؤسسة مالية.	1%	0%	0%
احتيال – طلب استرداد أموال- محلي	8%	26%	26%
احتيال – طلب استرداد أموال- دولي	6%	13%	13%
احتيال- تقييم بقيم منخفضة، وعدم جود علاقة متحفظة بين المشترين في البيع على المكشوف والبائعين، أو محاولات بيع احتيالي سابقة في معاملات البيع على المكشوف	0%	0%	0%

2. مراجعة الافصاحات التلقائية وطلبات الاستعلام الواردة من وحدات المعلومات المالية الأجنبية

خلال فترة المراجعة نفسها، تسلمت وحدة المعلومات المالية لدولة الإمارات **314 طلب استعلام** من وحدات معلومات مالية أجنبية، تتعلق بـ "أنشطة احتيالية محتملة". وفي المقابل، أرسلت وحدة المعلومات المالية لدولة الإمارات **122 طلب استعلام** إلى وحدات معلومات مالية نظيرة، تتعلق بالمخاوف نفسها. وقد تم تصنيف التقارير إلى الفئات المبينة أدناه:

الاشتباه الرئيس	عدد الطلبات الواردة من وحدات معلومات مالية نظيرة			
	2019	2020	2021	الإجمالي
عملية احتيال محتملة	70	62	47	179
احتيال محتمل من خلال البريد الإلكتروني لمؤسسة الأعمال	1	8	19	28
عملية تزييف/تزوير محتملة	4	12	9	25
تحويلات سلكية احتيالية محتملة	1	5	18	24
عملية احتيال من خلال الاستثمار	1	12	11	24
مستندات احتيالية محتملة	0	5	4	9
احتيال- خيانة أمانة محتملة	0	1	6	7
مخططات "بونزي" محتملة	0	2	3	5
مخططات هرمية محتملة	0	0	3	3
احتيال محتمل في ضريبة القيمة المضافة/رسوم الإنتاج	0	1	2	3
تزييف وقرصنة منتجات محتملة	1	0	1	2
تزييف عملة محتمل	0	0	2	2
احتيال محتمل في جهاز الصرّاف الآلي- جريمة احتجاز النقود	0	1	0	1
احتيال محتمل في الهوية- أو سرقة الهوية	0	0	1	1
احتيال محتمل في الإنترنت- القرصنة الإلكترونية	0	0	1	1
الإجمالي	**78**	**109**	**127**	**314**

لأغراض هذه الدراسة، قامت وحدة المعلومات المالية لدولة الإمارات بإجراء تحليل مجموعة تكمن في حوالي 20% من كافة تقارير المعلومات الدولية الواردة. وقد تطابقت نتائج مراجعة طلبات التعاون الدولي مع نتائج مراجعة تقارير المعاملات المشبوهة/تقارير الأنشطة المشبوهة.

وقد لوحظ أن هنالك تماثل في التوجهات والأساليب في الطلبات الدولية التي تم استلامها وتقارير المعاملات المشبوهة/الأنشطة المشبوهة اتي أرسلتها الكيانات التي ترفع التقارير المحلية، وسوف تتم مناقشتها بمزيد من التفصيل في جزء لاحق من هذا التقرير.

وإضافة لذلك، لوحظ أن أغلبية المعلومات المالية السابق ذكرها قد وردت من وحدات معلومات مالية نظيرة معينة في بلدان ذات صلة استراتيجية.

3. طلبات استرداد الأموال التي تلقتها المؤسسات المالية في دولة الإمارات العربية المتحدة

تم إرسال طلب بشأن معلومات تخص طلبات استرداد الأموال الدولية التي تم استلامها، والتي تتعلق بالاحتيال، إلى 235 كياناً من الكيانات التي ترفع التقارير، شملت بنوكاً محلية، وبنوكاً أجنبية/مكاتب تمثيل ومحلات صرافة. ومن إجمالي هذه الكيانات استجاب 178 كيانا (76%) لطلب وحدة المعلومات المالية لدولة الإمارات، أكّد منها 22 كياناً فقط (9%) أنها قد تلقت مثل هذه الطلبات من مؤسسات دولية نظيرة.

وإجمالاً، تسلمت الكيانات الـ 22 المستجيبة المشار إليها، 698 طلباً لاسترداد أموال، بمبلغ إجمالي قدره حوالي 179 مليون درهم في سنة 2020، و726 طلباً لاسترداد أموال بمبلغ إجمالي يبلغ حوالي 169 مليون درهم في سنة 2021.

في سنة 2020، تمت بنجاح إعادة حوالي 27 مليون درهم (15%) من إجمالي طلبات استرداد الأموال الدولية. وفي المقابل، ارتفع عدد طلبات استرداد الأموال الناجحة إلى حوالي 37 مليون درهم (22%) في سنة 2021.

تم إرسال طلب مماثل لمعلومات تتعلق بطلبات استرداد أموال محلية ذات صلة بمعاملات احتيالية إلى الكيانات المبلّغة بشأن تقارير المعاملات المشبوهة/الأنشطة المشبوهة ذات الصلة بالاحتيال، أكّدت منها 20 كياناً استلامها طلبات استرداد أموال ذات صلة بتحويلات احتيالية محلية.

والأرقام الواردة أدناه هي عدد طلبات استرداد الأموال المحلية التي تم استلامها، والمبالغ الإجمالية التي تضمنتها خلال السنوات 2020 و2021، إضافة إلى عمليات الاسترداد الناجحة ذات الصلة بالاحتيال.

طلبات استرداد الأموال المحلية (2020-2021)					
2020			2021		
عدد طلبات استرداد الأموال المستلمة	المبلغ الإجمالي المتضمن (بالدرهم)	المبلغ الإجمالي المسترد بنجاح (بالدرهم)	عدد طلبات استرداد الأموال المستلمة	المبلغ الإجمالي المتضمن (بالدرهم)	المبلغ الإجمالي المسترد بنجاح (بالدرهم)
2,458	170,255,327	16,022,834	2,164	168,733,844	5,958,496

في سنة 2020، بلغت طلبات استرداد الأموال الناجحة 16 مليون درهم (9.41%) من إجمالي طلبات استرداد الأموال التي تسلمتها البنوك ومحلات الصرافة في دولة الإمارات من مؤسسات مالية أخرى، بينما تراجع هذا المبلغ في سنة 2021 إلى حوالي 6 مليون درهم (3.53%). ومن الممكن أن يكون لسبب هذا الانخفاض شقان، أحدهما تأخر التدخلات من جانب البنك المحوِّل (حساب الضحية) والثاني يمكن أن يكون الاستخدام والتبديد السريع للأموال من قبل الجاني (الجناة)، وترك الحساب خالياً من الرصيد أو حد أدنى من الرصيد لا يكفي لإنجاح الاسترداد. وقد يكون الاستيلاء على الأموال وانفاقها قد تم من خلال عمليات السحب النقدي (بصورة رئيسية) أو تحويل الأموال لاحقاً إلى حساب (حسابات) في بنك آخر داخل أو خارج الدولة.

4. طلبات التعاون المحلي

كان تبادل المعلومات مع السلطات المحلية في دولة الإمارات العربية المتحدة عنصراً آخراً حرصنا على أخذه في الاعتبار خلال المراجعة التي شملتها هذه الدراسة. فخلال الفترة الممتدة من **شهر يوليو 2019** وحتى **شهر يونيو 2022**، تسلمت وحدة المعلومات المالية لدول الإمارات **10,707 طلباً** من أصحاب مصالح محليين مثل **وزارة الداخلية، والنيابة العامة الاتحادية، وإدارات الشرطة** المختلفة. وتمحور حوالي **3.24%** من تلك الطلبات حول الاحتيال والاستفسارات و/أو التحقيقات بشأن جرائم الإنترنت.

الأنماط والاتجاهات

لقد خضعت جميع البيانات والمعلومات التي تم جمعها وعرضها في هذا التقرير لتحليل تفصيلي من قبل وحدة المعلومات المالية لدولة الإمارات، للتعرّف على أنماط واتجاهات جرائم الاحتيال واساليبها. فقد قامت وحدة المعلومات المالية بمراجعة حوالي **1,000 تقرير معاملة مشبوهة/تقرير أنشطة مشبوهة**، وحوالي **62 تقارير مشاركة تلقائية/طلبات معلومات واردة**، وفي نهاية المراجعة، لاحظت وحدة المعلومات المالية لدولة الإمارات بعض التوجّهات وأنواع أنشطة الاحتيال المتكررة كما هو مبيّن أدناه:

- **تحويلات الأموال الاحتيالية**

يعد هذا النوع أكثر أنواع الاحتيال الشائعة التي تمت ملاحظتها في التقارير المشتبه بها المستلمة، وربما يعتبر أيضاً واحداً من أكثر أنواع الاحتيال ضرراً من الناحية المالية، لأنه يشتمل على قدرٍ كبيرٍ من الأموال. إن الاحتيال في تحويلات الأموال هو أموال محوّلة برقياً/إلكترونياً ذات طبيعة احتيالية. تأتي هذه الأحداث (في معظم السيناريوهات) متبوعةً "بطلب استرداد الأموال" أو ما يسمى بـ "طلب إعادة الأموال للموطن الأصلي"، يقوم بإرساله البنك المُرسِل (حساب الضحية) إلى البنك المستفيد (حساب الجاني أو حساب المتورط في الاحتيال).

وعادة ما تختفي الأموال الاحتيالية المستلمة في حساب الجاني بسرعة، إما بسحبها نقداً/شيكات أو تحويلها لاحقاً لحساب (حسابات) أخرى كما في حالات أكثر تعقيداً. ومن خلال مراجعة البيانات، فإن الأموال المستلمة يشتبه في أن تكون إما عائدات جريمة احتيال وقعت خارج دولة الإمارات (الاحتيال في تحويلات الأموال دولياً)، أو أنها عائدات جريمة احتيال وقعت داخل دولة الإمارات (الاحتيال في تحويلات الأموال محلياً).

وبطبيعة الحال، من الصعب تحديد مستوى الاستغلال واختراق المعلومات الذي يفتح الأبواب أمام المجرمين للمعاملات الاحتيالية من جانب واحد. وينطوي ذلك غالباً على "هجمات سيبرانية" عبر عمليات قرصنة مخططة (برامج ضارة أو فيروسات) تُمكّن المُحتال من الحصول على المعلومات الشخصية الخاصة بالضحية وعلى معلومات جوهرية لإجراء حوالات احتيالية، أو بالأحرى ربطها بعمليات احتيال داخلية أو خارجية، تم شرح بعضها أدناه.

- **اختراق البريد الإلكتروني التجاري (ما يخص الكيانات الاعتبارية)**

خلال تحليل البيانات الواردة في هذا التقرير، تمت ملاحظة أن استغلال واختراق البريد الإلكتروني للمؤسسات والأعمال هو أحد المسائل المثيرة للقلق التي ورد من معظم وحدات المعلومات المالية النظيرة طلب للمعلومات بشأنها. يشير هذا النمط إلى نوع من الهجمات السيبرانية (عادة عن طريق القرصنة أو التصيّد)، ويشمل ذلك انتحال شخصية مسؤول في شركة ما لإجراء معاملات غير مصرح بها. تبدأ هذه الخطة عادةً إما باستغلال معلومات متاحة

لجمهور العامة، أو بقرصنة البريد الإلكتروني لفرد أو مؤسسة ما. وبعد الحصول على معلومات كافية يمكن استخدامها لارتكاب الاحتيال بواسطة الشركات، يستخدم الجُناة عادةً أساليب شائعة أخرى لخداع الضحايا.

فعلى سبيل المثال، يتظاهرُ المحتال بأنه مورد أو مقدم خدمة ويخدع مشتري/مستخدم الخدمة من خلال تغيير تفاصيل المستفيد من الحساب المصرفي. يُسمى هذا أيضاً بـ "احتيال إعادة التوجيه".

ومثال آخر هو عندما يقوم الجاني الذي يتصرف كمورد حقيقي بإرسال بريد إلكتروني إلى الطرف المستهدف، طالباً الدفع مقابل السلع/الخدمات المزعومة أو الحقيقية التي يجب تقديمها إلى الطرف المستهدف. ويكون عنوان البريد الإلكتروني للمرسل عادةً تقليدٌ لعنوان بريد إلكتروني للمورد المعروف – حيث لا يتم تغيير إلا حروف البريد الإلكتروني، أو يتم استخدام اسم مختصر أو نطاق إنترنت آخر يبدو مشابهاً لنطاق الإنترنت الفعلي للمورد وما إلى ذلك. وعادةً ما يكون البريد الإلكتروني الاحتيالي مصحوباً بوثائق داعمة مزورة، مثل اتفاقية عقد، وفاتورة، وبوليصة شحن، وما إلى ذلك. تشتمل الفاتورة على التفاصيل المصرفية "للمورد"، حيث يتعمد الجاني تعديل رقم الحساب المصرفي فقط (الذي يملكه في الواقع الجاني أو المتورط في الاحتيال) بحيث يستلم المحتال أو المتورط في الاحتيال التحويلات مباشرةً.

- **<u>الاحتيال عن طريق الخداع</u>**

الخداع هو خطة مضللة أخرى تمت ملاحظتها خلال قيامنا بالتحليل. وعلى مر السنين، يقوم المخادعون باستمرار بتطوير أساليب معقدة لتضليل الأشخاص المستهدفين (ضحاياهم) للكشف عن معلوماتهم السرية و/أو معلوماتهم الشخصية للحصول على منافع نقدية أو شخصية.

ومن خلال الاطلاع على تقارير المعاملات المشبوهة/تقارير الأنشطة المشبوهة، فإن أساليب/طرق العمل الشائعة التي يستخدمها المحتالون لخداع ضحاياها هي:

- **الاحتيال في المنتجات المقلّدة/المواقع الإلكترونية المزيفة:** عادةً ما يتصرف الجناة بأنهم: (1) بائعو منتجات في مواقع التواصل الاجتماعي، ويعلنون عن منتجاتهم بأسعار أقل من قيمتها الفعلية في السوق. وعادةً ما يُفضل المستهلكون الاستفادة من التوفير الذي قد يحصلون عليه من شراء هذه المنتجات بتكلفة أقل. وقد تكون المنتجات موجودة بالفعل، إلا أن العلامة التجارية وخصائصها هي في حقيقة الأمر دون المستوى المطلوب. من ناحية أخرى، قد يكون الموردون قد استلموا الدفعة عن طريق الإنترنت، ولكنه لن يتم تسليم المنتجات إلى العملاء مطلقاً، حيث لا توجد منتجات في الواقع؛ (2) يقوم شخص ينتحل شخصية موظف الجمارك بإبلاغ العملاء بأن هناك شحنة قادمة إليهم. ويميلُ الجناة إلى المطالبة بمجموعة متنوعة من الرسوم الجمركية حتى يتمكنوا من تسليم الشحنة بنجاح. وفي حالات كثيرة، يتواطأ أكثر من فرد واحد لخداع الضحية المتوقعة.

- **الاحتيال في التأشيرات/التذاكر المزيفة:** ينتحل الجناة شخصية وكيل سفر يوفّر خدمة التأشيرات أو التذاكر ويطالبون باستكمال الدفع عن طريق الإنترنت قبل القيام بإصدار التأشيرة أو التذكرة. إلا أنه بعد القيام بتحويل المبلغ، يتوقف وكيل السفر (المحتال) عن الاتصال بضحيته.

- **الخداع/الاحتيال في الاستثمار:** ظلّ هذا النوع من الاحتيال معروفاً على نطاق واسع منذ وقت ظهوره، بغض النظر عن الوضع الاقتصادي والوقت الحالي. وتمت ملاحظة أن الاحتيال في الاستثمار قد تسبب في

خسائر مالية كبيرة، ليس فقط للأفراد بل أيضاً للعديد من الشركات. إن السمة الرئيسية لهذا الاحتيال هي أن الجاني يميل إلى عرض استثمار (وهمي في كثير من الأحيان) على الشخص المستهدف ويقدّم وعداً بعائد مرتفع مع مخاطر قليلة أو عدم وجود مخاطر على الإطلاق. إن الاستثمارات المحتملة في هذا النوع من الخداع تكون عادةً على ثلاثة أشكال: أسهم شركات، عقارات، وأوراق مالية.

فضلاً عن ذلك، ونظراً للتطور الحالي في الخدمات المصرفية المالية وتزايد الطلب على العملات الافتراضية، فقد وجد المجرمون أيضاً طرقاً لاستغلال خصائص تلك العملات الافتراضية في الأنشطة الاحتيالية، بما في ذلك عمليات الخداع في الاستثمار. بالإضافة لذلك، ومن خلال الاطلاع على تقارير المعلومات الواردة من وحدات معلومات مالية نظيرة، تم تسليط الضوء على أن النظام المالي لدولة الإمارات ربما كان مستهدفاً أو مستخدماً في تمويه المتحصلات من عائدات الأنشطة الاحتيالية التي حصلت خارج الدولة.

- **التصيّد / سرقة البيانات الشخصية**

يحصل المحتالون على معلومات حساسة أو معلومات شخصية للضحية إما عبر الإنترنت أو عن طريق المكالمات الهاتفية. وفى هجمات التصيّد، ينبغي على الضحية عادةً الضغط على رابط ضار، حيث يتم الطلب من الضحايا إدخال معلوماتهم. قد يؤدي هذا الضغط إلى تحميل برنامج ضار أو فيروسات على الجهاز الذي تستخدمه الضحية، لتمكين المهاجم من الحصول على كافة المعلومات المدخلة. وفي معظم السيناريوهات الشائعة، يُنشئ المهاجم موقعاً إلكترونياً مزيفاً أو ما يشبه موقعاً إلكترونياً لمؤسسة مالية، ويعطي الضحية بعض الخطوات لاتباعها. أما في حالة سرقة البيانات الشخصية، يستخدمُ المحتالون طرقاً مختلفة وأساليب الهندسة الاجتماعية لإقناع الضحايا بالكشف عن معلوماتهم الشخصية أو الحساسة برضاهم عبر مكالمة هاتفية.

- **التزوير / التقليد**

التزوير هو تعديل أداةٍ أو وثيقة (أصلية) بشكل غير قانوني بنية خداع طرف آخر. مثلاً "تزوير التوقيع"، والذي ينطوي على تقليد توقيع شخص آخر بشكل غير قانوني. ومثال آخر هو "تزوير شيك"، وينطوي على إجراء تعديلات غير قانونية على تفاصيل مثل المبلغ، أو قد يقترن بتزوير التوقيع. ومن ناحية أخرى، فإن التقليد هو تقليد أداة أو وثيقة (هي غير أصلية ولكن يتم تقليد الأصل) بشكل غير قانوني. مثلاً، إنشاء وثائق هوية مزورة تماماً، تحرير شيكات مزورة، أو عملات مزورة، وإصدار فواتير كاذبة.

مؤشرات المخاطر

نظراً للتنوع الكبير لأنواع ومصادر وفئات الاحتيال، ولأن كل نوع يحافظُ على خصائصه وعلى مؤشرات الخطر الخاصة به، وضعت وحدة المعلومات المالية لدولة الإمارات بعض المؤشرات العامة للمخاطر التي قد تكون ذات صلة مباشرة أو غير مباشرة بالاحتيال. إن وجود مؤشر مثل ذلك في حالة ما يُمكن أن يثير الشكوك والمباشرة في التحقيقات التي تؤدي إلى مزيدٍ من وضع مؤشرات أخرى. وعلى الرغم من ذلك، لا يُمكن التوصل إلى أي نشاط إجرامي استناداً إلى مؤشر واحد، ولكن من خلال حدوثه في آنٍ واحد مع تحليل المعلومات المتاحة الأخرى، فقد يوحي بارتكاب جريمة احتيال.

وفيما يلي بعض المؤشرات المطوّرة التي تدل على المخاطر ويمكن أن تنبّه إلى خطر الاحتيال:

- عميل يُقدّم وثائق يشتبه في أنها تحتوي على أي بيانات أو مدخلات كاذبة أو وهمية أو احتيالية مادياً.
- قيام عميل وبعلمه بتزييف أو إخفاء أو تغطية حقيقة جوهرية عن طريق أي خدعة أو خطة أو قيامه بتصريح أو تمثيل كاذب مادياً.
- التناقضات التي تمت ملاحظتها بين الحقائق التي تم رفع تقارير بها، والبيانات التي تمت ملاحظتها، و/أو الوثائق الداعمة.
- الوثائق الداعمة غير الكافية أو التي تم تعديلها بشكل واضح (مثل التعديلات على أي معلومات مهمة، والتسريبات، والأخطاء الإملائية، وما إلى ذلك).
- المستندات الداعمة التي تحتوي على إيصالات الموردين و/أو المستندات الداعمة الأخرى التي يبدو أنه تم تعديلها (أماكن تم استخدام سائل أبيض بوضوح لإخفاء الأخطاء، حالات قص، حذف).
- تكرار "طلبات استرداد الأموال" المستلمة من مصارف مختلفة قامت بالتحويل لنفس المستفيد.
- المبالغ المالية المستلمة عن طريق الحوالات البرقية (الدولية أو المحلية) من أطراف غير ذات صلة ثم عمليات السحب الفورية أو الحوالات الخارجية.
- حوالات الأموال الواردة متبوعةً بـ "طلب استرداد الأموال" من المصرف الذي قام بالتحويل.
- حوالات الأموال الواردة المتكررة من أطراف غير ذات صلة إلى حساب (حسابات) مفتوحة مؤخراً.
- المبررات غير الكافية التي تم الحصول عليها من صاحب الحساب بشأن الأموال المستلمة، أو من عميل لا يعلم بوضوح الغرض من الأموال المستلمة في الحساب ومصدرها.

- الحسابات المفتوحة لغرض "الراتب"، وخصوصاً الأفراد باعتبارهم عمالاً من ذوي الدخل المنخفض ولا يوجد دخل فعلي للراتب في الحساب، وبدلاً من ذلك، يدخل للحساب حوالات أو إيداعات متعددة من أطراف غير ذات صلة.

مؤشرات قياس المخاطر الأخرى (المالية / السلوكية):

- المعاملات غير المعتادة أو الحوالات فيما بين الحسابات (بما في ذلك المبالغ الصغيرة ذات الصلة).
- ارتفاع التكاليف بلا تفسير أو التي لا تتناسب مع زيادة الإيرادات.
- الموظفون الذين يبدو أنهم يرتكبون عدداً أكبر من الأخطاء مما هو معتاد، خاصة عندما تؤدي هذه الأخطاء إلى خسائر مالية من خلال المعاملات النقدية أو الحسابات.
- الموظفون الذين يتم تقديم شكاوى ضدهم و/أو يسعون لخرق القواعد، والذين يطلبون أيضاً تفاصيل حول نطاقات التدقيق الداخلي المقترحة أو عمليات التفتيش.

أمثلة على حالات واقعية

مثال على حالة (1): الاحتيال في دفعة مسبقة

استلمت وحدة المعلومات المالية لدولة الإمارات تقريرين (2) من تقارير المعاملات المشبوهة بشأن فردين (الشخص "أ" والشخص "ب") قاما بالاحتيال على الضحية ("س ع") من خلال "الاحتيال في دفعة مسبقة" و"الاحتيال في وسائل التواصل الاجتماعي". اتصل الشخص "أ" في البداية بالشخص "س ع" من خلال تطبيق على وسائل التواصل الاجتماعي يخبره بأن طرداً يحتوي على عطور تحمل علامة تجارية فخمة، وأجهزة هاتف آيفون وساعات فاخرة له سيتم تسليمها بعد دفع رسوم الشحن.

وفي اليوم التالي، قام الشخص "ب"، والذي ينتحل شخصية موظف جمركي، بالاتصال بالشخص "س ع" بشأن الطرد نفسه، وطالب بدفعة إضافية لرسوم التخليص الجمركي. لاحقاً لذلك، اتصل الشخص "ب" بالشخص "س ع" مرةً أخرى وطلب دفع التأمين ورسوم متفرقة أخرى.

التزم الشخص "س ع" بجميع طلبات الدفع الثلاثة وأرسل الأموال من خلال شركة صرافة. وبعد استلام جميع الحوالات، توقف كل من الشخص "أ" والشخص "ب" عن الاتصال بالشخص "س ع" للرد على استفساراته ولم يحصل على أي طرد أو استرداد للمبالغ المالية.

أجرت وحدة المعلومات المالية لدولة الإمارات تحليلها المكثّف بشأن الشخص "أ" والشخص "ب". ويبدو جلياً تورط الشخصين المعنيين في أنشطة احتيالية اخرى، لا سيما الاحتيال في دفعة مقدمة، والاحتيال على ضحايا أفراد من بعض الجنسيات المتكررة. قامت وحدة المعلومات المالية بإحالة القضية الى سلطات إنفاذ القانون لإجراء مزيدٍ من التحقيقات. ووفقاً لردود سلطات إنفاذ القانون، يبدو أن الأشخاص المعنيين متورطون في أنشطة احتيالية، وبالتالي تم فتح قضية تتعلق بغسل الأموال.

تم تحديد المؤشرات التي تدل على المخاطر:

- استلام مبالغ مالية من أفراد مختلفين لا صلة لهم
- انتماء المستفيد من المبالغ المالية إلى فئة العمال من ذوي الدخل المنخفض
- عدم توافق معدل دوران الحساب مع المعلومات المذكورة في ملف "اعرف عميلك"
- الاستخدام الواسع لوسائل التواصل الاجتماعي للتواصل مع العملاء

مثال على حالة (2): سرقة البيانات الشخصية

تلقت وحدة المعلومات المالية لدولة الإمارات العديد من تقارير الأنشطة المشبوهة من جهة مبلّغة تقارير بشأن نمط مشترك يستخدمه المحتالون للاحتيال على عملائهم. يتواصل الضحايا، ومعظمهم من المواطنين والمقيمين، إلى الجهة المبلّغة، لتقديم شكوى حول مستفيدٍ جديدٍ تمت إضافته إلى حساباتهم المصرفية على الهاتف المتحرك/الإنترنت ولكنهم ينكرون إضافته بأنفسهم.

في البداية، يتلقى الضحية مكالمة هاتفية من المحتال، ومن خلال تقنيات الهندسة الاجتماعية، يستطيع المحتال أن يقنع الضحية بالإفصاح عن معلوماته/معلوماتها الشخصية، بما في ذلك الاسم ورقم الهوية والتفاصيل المصرفية.

تواصلت وحدة المعلومات المالية لدولة الإمارات مع الجهة المبلّغة، وأوضحت الجهة أن عملائها المذكورين في تقارير الأنشطة المشبوهة هم ضحايا لعملية خداع لسرقة البيانات الشخصية، حيث تمت مشاركة المعلومات المصرفية، بما فيها الرقم السري لمرة واحدة، مع المحتال الذي يقوم بعد ذلك بإنشاء ملف للبيانات المصرفية على الإنترنت باستخدام تفاصيل الضحايا، ومن ثم إضافة مستفيد جديد لأغراض احتيالية. كما أضافت الجهة التي ترفع التقارير بأنها أجرت عملية مراجعة وأكدت أن عملية المستفيد على قنواتها الإلكترونية تكون مدعومة بالتحقق من كلمة مرور لمرة واحدة، مما يعني أنه لا يمكن إضافة المستفيد إلى قائمة المستفيدين الخاصة بالعميل دون إرسال كلمة المرور لمرة واحدة من قبل الجهة التي ترفع التقارير إلى رقم الهاتف المتحرك المسجل الخاص بالعميل. أما المستفيد الجديد، فتتم إضافته إما من قبل المحتال أو من قبل العميل نفسه بعد استلام كلمة المرور لمرة واحدة. وعلى الرغم من وجود عدد من التقارير المتعلقة بنفس طريقة العمل، فقد أكدت الجهة التي ترفع التقارير عدم وجود خسائر مالية مقيدة.

مثال على حالة (3): الاحتيال/التزوير في الطلبات

تلقت وحدة المعلومات المالية لدولة الإمارات العديد من تقارير المعاملات المشبوهة من عدة جهات مبلّغة، بما في ذلك بنوك محلية وشركات تمويل، فيما يتعلق بأنشطة احتيالية تتم من خلال تزوير الوثائق. وعادةً، يتواصل المحتال مع الجهة التي ترفع التقارير بغرض تقديم طلب للحصول على تسهيل ائتماني (قرض شخصي/قرض سيارة، بطاقات ائتمانية). تطلُب الجهة التي ترفع التقارير تقديم وثائق داعمة لتقييم أهلية مقدّم الطلب. تشمل الوثائق، على سبيل المثال لا الحصر، جواز السفر، وبطاقة الهوية، وتأشيرة الإقامة (للمقيمين)، وإثبات الدخل، وعقد العمل، وما إلى ذلك.

وتتضمن الوثائق المقدمة بصفة رئيسية شهادة راتب مزورة (مبالغ فيها)، وعقد عمل، وتأشيرة، وكشف حسابات (مزوّر) للجهة التي تقوم برفع التقارير أثناء طلب الحصول على تسهيل ائتماني. خلال إجراء وحدة المعلومات المالية لدولة الإمارات تحقيقاً في تقارير المعاملات المشبوهة المتعلقة بنفس أسلوب الاحتيال، تم التوصّل إلى بعض النتائج المشتركة التالية:

- تحمل الوثائق الداعمة التي تأتي من الشركة (مثل شهادة الراتب، عقد العمل) الختم الفعلي للشركة والتوقيع المطلوب من الموظفين المخولين (ينطبق على الأفراد فقط).
- بعد منحهم التسهيل الائتماني، يعتزم الجناة مغادرة الدولة بعد دفع أقساط قليلة أو عدم الدفع نهائياً.
- يستخدم الذين يحصلون على الائتمان شهادات راتب لوظيفة سابقة وتفاصيل شركة أخرى لتقديم طلب للحصول على تسهيل ائتماني جديد.

- يقوم الجاني، والذي يتظاهر بأنه موظف قانوني في شركة معينة، بتقديم وثائق داعمة تكون مزورة بالكامل. على سبيل المثال، تفاصيل شركة وهمية، تفاصيل تأشيرة مزورة وعقد عمل، وراتب مُبالغٌ فيه من أجل اجتياز معايير الأهلية التي يحددها البنك.

قامت وحدة المعلومات المالية لدولة الإمارات بإحالة قضايا احتيال مماثلة الى سلطات إنفاذ القانون في دولة الإمارات، والتي بدورها قامت بإضافة القضايا إلى قواعد بياناتها.

الخاتمة

وفي الختام، يمتد تأثير الاحتيال إلى ما هو أكثر من مجرد خسائر مالية، ويؤثر الاحتيال على الأفراد، والمؤسسات في قطاعات واقتصادات مختلفة. وبالنسبة للمؤسسات المالية فإن الخسائر في السمعة ستكون أكثر ضرراً من الخسائر المالية الناجمة عن الاحتيال. ولذلك، يجب على المؤسسات المالية فهم كيفية ارتكاب جرائم الاحتيال، ووضع تدابير فعالة للكشف عن هذه الأحداث ومنعها بهدف حماية مصالح عملائها والمصالح الخاصة بهم.
ستساعد عمليات تقييم مخاطر الاحتيال، بما في ذلك تحليل الأسباب الجذرية، المؤسسات في تحديد وتنفيذ خطط وتدابير إدارية ملائمة. وبالإضافة لذلك، سيركّز تقييم مخاطر الاحتيال أيضاً على تحديد ومعالجة نقاط الضعف وبيئة المخاطر المحيطة بكلٍ من الاحتيال الداخلي (أي اختلاس الأصول) والاحتيال الخارجي (أي قرصنة وسرقة الأصول أو المعلومات)، وبالتالي وضع ضوابط وقائية وضوابط رقابية للكشف عن الاحتيال (يدوياً وآلياً).

ومن المؤسف أن جرائم الاحتيال ليست بالأمر الذي سيتلاشى ببساطة، ويجب بذلُ جهود عالمية ووطنية للتصدي له على نحو استراتيجي، وزيادة روح المبادرة للعمل بدلاً من ردة الفعل. إن الوعي والوقاية وضوابط الكشف وكذلك التحقيقات الداخلية تعدّ كلها عناصر ضرورية ينبغي تجميعها في استراتيجية فعالة لمكافحة الاحتيال، وسيحقق نجاحها فائدة كبيرة.