

خدمات التجار من بنك أبوظبي التجاري - حلول الأعمال



المحتويات

٢	١	وفر الحماية لأعمالك
٣	٢	التصريح
٤	٣	المطالبة بإسترداد المبالغ المدفوعة
٥	٤	التحقق من هوية المشتري
٥	٥	معاملات مع وجود البطاقة
٧	٥	معاملات مع عدم وجود البطاقة
٩	٥	أنواع البضائع التي يستهدفها المحتالون
٩	٦	حماية أعمالك من الإحتيال
٩	٧	حماية أعمالك من الإحتيال مع وجود البطاقة
١٠	٨	حماية أعمالك من العمليات الإحتيالية عبر الإنترنت وأوامر الشراء عبر البريد والهاتف
١١	٩	حماية أعمالك من عمليات الإحتيالية لتحويل الأموال
١٢	١٠	مخاطر أخرى يواجهها التاجر
١٤	١١	التقليل من المخاطر التي يواجهها التاجر عبر الإنترنت
١٤	١٢	متطلبات الموقع الإلكتروني

وفر الحماية لأعمالك

يواجه التجار العديد من المخاطر المتنوعة عند قبولهم للمعاملات المدفوعة باستخدام بطاقات الائتمان. وقد تم تطوير هذا الكتيب لمساعدتك على فهم أنواع المخاطر التي تواجهها والإجراءات التي يتعين عليك إتخاذها للتقليل من مخاطر التعرض للخسائر.

تمثل المعاملات الإحتيالية واحدة من أكبر المخاطر التي يواجهها التجار. فإذا لم تكن منتبهاً وحريصاً بشكل كافي، يمكن أن تكلف المعاملات الإحتيالية أعمالك أموالاً طائلة. وهناك بعض التجار الذين يتعرضون أكثر من غيرهم للمعاملات الإحتيالية بسبب نوع البضائع التي يبيعونها. ويتعين على التاجر فهم مدى إحتيالية إستهدافه من قبل المحتالين ومن الضروري أن يتمتع التاجر بفهم صحيح وواضح لعمليات الإحتيال بإستخدام بطاقات الائتمان وكيفية إكتشافها وطريقة منع حدوثها. وسوف نقوم بمناقشة هذه النواحي والمفاهيم فيما يلي.

هناك ثلاثة أنواع رئيسية لمعاملات بطاقات الائتمان هي:

◀ معاملات بوجود البطاقة (تجار البيع المباشر)

◀ والمعاملات عبر الإنترنت

◀ و أوامر الشراء عبر البريد/الهاتف.

وعادة ما يتم الإشارة إلى التجار الذين يتعاملون من خلال الإنترنت وبأوامر الشراء عبر البريد/الهاتف على أنهم التجار «في عدم وجود البطاقة» حيث لا يكون أي من البطاقة أو المشتري متواجدين فعلياً في محل التاجر في وقت الشراء.

وتتضمن الأمثلة على ذلك عمليات الشراء التي يقدم فيها العميل بيانات بطاقة الائتمان الخاصة به عبر الإنترنت أو الفاكس أو الهاتف أو من خلال إشعار بريدي.

ملاحظة: يجب عليك الإمتناع تماماً عن طلب موافاتك ببيانات بطاقة الائتمان الخاصة بالعميل عبر البريد الإلكتروني لدفع قيمة أي بضائع و/أو خدمات، لأن هناك الكثير من المحتالين الذين يفضلون تنفيذ معاملات الشراء في عدم وجود البطاقة بسبب عدم الكشف عن هوية المشتري عند إستخدام هذه الطريقة لدفع قيمة المشتريات.

كما تمكن الطول القائمة على أساس عدم وجود البطاقة المحتالين من إصدار أوامر شراء عبر الإنترنت أو من خلال أوامر الشراء عبر البريد/الهاتف في جميع أنحاء العالم. وإذا كان هؤلاء المحتالون يقيمون في الخارج فإن فرص إتخاذ الإجراءات القانونية والجنائية ضدهم تكون منخفضة جداً وهو ما يمثل حافزاً إضافياً لإتباع هذا الأسلوب الإحتيالي. عدد كبير من العمليات الإحتيالية المنفذة بإستخدام بطاقات الائتمان يتم إرتكابه في حالات عدم وجود البطاقة. كما أن عدد هذا النوع من العمليات الإحتيالية أخذ في الإزدياد بمعدل سريع.

فكرة: إلتزم دائماً بأحكام وشروط إتفاقية التاجر التي قمت بتوقيعها وبقواعد خطة البطاقة.

التصريح

يكون من الضروري أن تفهم تعبير أو مصطلح « التصريح » - ماذا يعني وماذا لا يعني.

ما يعنيه مصطلح التصريح

- ◀ هو أن رقم الحساب صحيح
- ◀ وأنه لم يتم الإبلاغ عن فقدان أو سرقة البطاقة،
- ◀ بالرغم من أن البطاقة قد تكون قد فقدت أو سرقت أو تم التلاعب فيها (الحصول على أو نسخ بيانات البطاقة بشكل غير صحيح) وأن حامل البطاقة على علم بوجود أموال كافية لتغطية قيمة المعاملة.

أما ما لا يعنيه مصطلح التصريح

- ◀ فهو أنه لا يؤكد أن الشخص المقدم لرقم البطاقة هو مالك البطاقة القانوني والشرعي. وتظل هناك
- ◀ مخاطرة أن يكون الشخص المقدم لرقم بطاقة الائتمان قد قام بسرقة البطاقة أو حصل عليها بطريقة غير مشروعة.
- ◀ وهناك أيضاً مخاطرة أن يكون المشتري قد حصل على رقم البطاقة بطريقة غير مشروعة دون أن تكون البطاقة في حيازته فعلياً.

وبالرغم من أنه من المهم جداً الحصول على تصريح بتنفيذ كل معاملة، فإن ذلك لا يحميك من مخاطر الإحتيال أو المطالبة بإسترداد المبالغ المدفوعة إذ أن مخاطر الإحتيال تظل قائمة بالرغم من الحصول على التصريح.

فكرة: التصريح لا يضمن الدفع إذا كانت المعاملة منغدة بواسطة شخص آخر غير حامل البطاقة الشرعي.

المطالبات بإسترداد المبالغ المدفوعة

بصفتك تاجر فإنك تواجه احتمال إستلام مطالبات بإسترداد المبالغ المدفوعة. ويتم رد المبالغ عندما يقوم حامل البطاقة (أو البنك الذي يتعامل معه) بالمنازعة فيما يتعلق بأي معاملة منفذة من خلال شركتك. وإذا تم حسم النزاع لصالح حامل البطاقة، يتم رد قيمة المعاملة (خصم قيمتها) من حسابك. أي بمعنى آخر، فإنك تخسر عوائد البيع بالكامل.

وتتمثل الأسباب الشائعة للمطالبات بإسترداد المبالغ المدفوعة فيما يلي:

- ◀ حامل البطاقة لم يقيم بتنفيذ المعاملة (غالباً ما تكون هذه إشارة إلى حدوث إحتيال)
- ◀ أو معاملات ملغاة متكررة
- ◀ أو عدم مطابقة البضائع للوصف المذكور
- ◀ أو وجود عيوب في البضائع أو الإخفاق في الإستجابة لمطالبات القسائم.

ويمكن أيضاً أن تنشأ المطالبات بإسترداد المبالغ المدفوعة لعدد من الأسباب الأخرى ومنها على سبيل المثال لا الحصر:

- ◀ عدم إستلام البضائع/ الخدمات
- ◀ أو تخطي الحد المقرر من قبل التاجر دون الحصول على تصريح بذلك.

وبصفة عامة، يمكن تقديم المطالبات بإسترداد المبالغ المدفوعة بواسطة حامل البطاقة أو البنك الذي يتعامل معه خلال مدة أقصاها ١٢ شهراً من تاريخ تنفيذ المعاملة أو من التاريخ الذي كان يتعين تسليم البضائع أو الخدمات فيه حيثما يكون من المتوقع تسليم البضائع بعد الدفع.

ويواجه التجار الذين يتعاملون على أساس عدم وجود البطاقة مخاطر إضافية لا تنطبق على التجار الذين يتعاملون على أساس وجود البطاقة تتعلق بالمطالبات بإسترداد المبالغ المدفوعة، ويعود ذلك تحديداً إلى عدم توقيع المشتري على قسيمة المبيعات أو إدخال رقم تعريفه الشخصي في منفذ البيع. وإذا أنكر حامل البطاقة في مرحلة لاحقة تنفيذه للمعاملة، فإنك عادة ما تكون عرضة لرد المبالغ المدفوعة لعدم قدرتك على إثبات أن حامل البطاقة هو من قام بتنفيذ معاملة الشراء.

ولهذا السبب، يكون من الضروري للتجار الذين يتعاملون على أساس عدم وجود البطاقة إتخاذ إجراءات وخطوات للتعرف على هوية المشتري والتأكد من أن المعاملة قانونية ومشروعة، وسيتم مناقشة الطرق التي يمكنك إتباعها للقيام بذلك في الصفحة (٤).

فكرة: قلل مخاطر المطالبات بإسترداد المبالغ المدفوعة إلى أدنى حد ممكن عن طريق التعرف على كيفية وسبب تقديم تلك المطالبات.

التحقق من هوية المشتري

في جميع الأوقات، يقع عبء إثبات أو التحقق من هوية المشتري على كاهل التاجر. وهذا ينطبق على جميع التجار بصرف النظر عن الطريقة التي يقبلونها للدفع بواسطة بطاقات الائتمان. ويكون من المهم بصفة خاصة، فيما يتعلق بالتجار الذين يتعاملون عبر الإنترنت أو أوامر الشراء عبر البريد/الهاتف، التعرف على هوية المشتري. بيد أن بنك أبوظبي التجاري يوصي التجاري بقبول الدفع بواسطة بطاقات الائتمان في ظل بيئة يقوم التعامل فيها على أساس وجود البطاقة بالإضافة إلى إتخاذ إجراءات للتحقق من هوية المشتري خاصة عندما يتعلق الأمر بمشتريات كبيرة. إذا قمت ببيع البضائع إلى مشتري ليس هو حامل البطاقة الحقيقي، فإنك قد تتعرض إلى إمكانية إستلام مطالبة بإسترداد المبالغ المدفوعة. ونود التأكيد هنا مرة أخرى أن التصريح لا يشكل تحققاً من هوية المشتري وأن المعاملة قد تكون منطوية على إحتيال بالرغم من الحصول على تصريح بتنفيذها.

المعاملات مع وجود البطاقة

عندما تكون البطاقة موجودة في منفذ البيع، إلقي نظرة جيدة وتفحص البطاقة بإمعان للتأكد من أنها بطاقة صحيحة وحقيقية. تأكد من إحتفاظك بحيازة البطاقة حتى إتمام المعاملة.

تفحص بطاقة الدفع

- ◀ هل تبدو حقيقية؟ هل الخط البارز واضح ومتساوي
- ◀ وهل تبدو الطباعة البارزة منفذة بشكل إحتراقي يجب أن تكون أرقام البطاقة بارزة وواضحة ومستقيمة
- ◀ في بطاقات فيزا وبطاقات ماستركارد تكون الأرقام الأربعة الأولى من رقم البطاقة مطبوعة تحت سطر الطباعة البارزة.
- ◀ ملاحظة: غالباً ما تكون الأرقام غير مطابقة أو تم تغييرها على البطاقات المزورة
- ◀ إفحص وجه وظهر البطاقة للتأكد من أن البطاقة تحتوي على:
 - ◀ شعار مصدر البطاقة
 - ◀ وإسم حامل البطاقة
 - ◀ ورقم البطاقة
 - ◀ وتاريخ إنتهاؤها
 - ◀ والتوقيع
 - ◀ CVV2/CVC2 رقم مكون من ثلاثة أعداد ظاهر على أو بالقرب من شريط التوقيع على بطاقة الائتمان
 - ◀ ويجب أن تكون العلامة المائية ظاهرة بشكل ثلاثي الأبعاد ويتغير لونها عند إمالتها لمشاهدة طائر فيزا أو خريطة العالم الخاصة بـ ماستركارد.
- ◀ وقم بمراجعة توقيع حامل البطاقة على الإيصال ومقارنته بالتوقيع الظاهر على شريط التوقيع الموجود على بطاقة الائتمان
- ◀ وتأكد من أن كلمات «فيزا» أو ماستركارد» مطبوعة بشكل متكرر بزواوية ميل ٤٥ درجة علماً بأن شريط التوقيع مصمم لكشف عمليات العبث أو التلاعب به.
- ◀ قم بمراجعة تواريخ الإنتهاء الظاهرة على جميع بطاقات الائتمان. لا تقبل أي بطاقة ائتمان منتهية الصلاحية وتأكد من أن الرقم المطبوع على الجهة الأمامية من البطاقة مطابق للرقم الظاهر على الإيصال.
- ◀ هل الإسم مطابق لإسم العميل؟ هل جنس مقدم الطلب مطابق للإسم المطبوع على البطاقة؟ وإذا ساورك أي شك أطلب بطاقة هوية تحمل صورة شخصية للتأكد من صحة البيانات الصفحة (0) والصفحة (٦).

قم بتمرير أو إدخال بطاقة الدفع

ولا تقم أبداً بإدخال رقم البطاقة يدوياً. إنتبه وكن أكثر حذراً إذا طلب منك العميل إدخال بيانات أي معاملة يدوياً.

الجهاز الطرفي في الموقع وشريحة التعريف الشخصي

البطاقات ذات الشرائح الذكية هي بطاقات ماستركارد وفيزا (بطاقات الائتمان وبطاقات الخصم المباشر) التي تحتوي على شريحة أمنية توفر المزيد من الحماية للمساعدة على التقليل إلى أدنى حد ممكن من مخاطر حدوث معاملات إحتيالية وبالتالي من المطالبات بإسترداد المبالغ المدفوعة. تفحص البطاقة، وإذا كانت هناك شريحة، قم دائماً بإدخال البطاقة في جهاز قراءة الشريحة أولاً بأول ومثل أي معاملة أخرى، يجب الإلتباه بنفس الدرجة وممارسة الحيطة والحذر اللازمين عند تنفيذ المعاملات بإستخدام البطاقات ذات الشريحة. إذا أظهر الجهاز عبارة «أدخل الشريحة» عند تمرير البطاقة عبر الجهاز ولم يكن هناك شريحة في البطاقة المعنية فإن المعاملة لن تتم ويقوم الجهاز بعرض عبارة «أدخل الشريحة» وعند إدخال الشريحة لا يمكن للجهاز قراءتها فلا تستمر في تنفيذ المعاملة.

إبحث عن

يجب عليك أن تكون حريصاً ومنتبهاً لبطاقات الائتمان غير المعتادة وإلا أصبح وقوعك فريسة للمعاملات الاحتيالية محتملاً بشكل كبير.

- ◀ إبحث عن العملاء الذين يبدو أنهم غير مهتمين بالبضائع التي يشترونها، ويتعين على التجار أن يسألوا أنفسهم ما إذا كان ويطلبون بضائع من الأنواع المذكورة بالتفصيل في قسم «أنواع البضائع التي يستهدفها المحتالون»
- ◀ مثل العملاء الذين يقومون بشراء أعداد كبيرة من نفس القطعة بصرف النظر عن المقاس أو اللون أو الطراز أو السعر
- ◀ والذين يبدو أنهم غير مهتمين بالبضائع التي يشترونها، ويتعين على التجار أن يسألوا أنفسهم ما إذا كان من المحتمل أن يقوم أي شخص بشراء أعداد كبيرة من شئ معين دون الإلتباه للتفاصيل،
- ◀ مثل هؤلاء الذين لا يقومون بالإطلاع على المقاس أو السعر أو الذين يقومون بتجميع عدد كبير من البضائع بسرعة
- ◀ أو الذين لا يهتمون بالضمانة
- ◀ أو العملاء الذين يطلبون التسليم الفوري أي هؤلاء الذين يرغبون في إستلام بضائع كبيرة وباهظة التكاليف فوراً
- ◀ أو العملاء الذين يقومون بشراء أشياء كبيرة ولكن يرفضون توصيل مشترياتهم إلى المنازل بالرغم من أن السعر يغطي تكلفة التوصيل. وفي هذه الحالة قد يكون العميل غير راغب بإعلام التاجر بعنوانه نظراً لإنطواء عملية الشراء على نشاط إحتيالي.
- ◀ ومثل العملاء الذين يطلبون منك إدخال رقم البطاقة يدوياً
- ◀ والعملاء الذين يقومون بعمليات شراء متكررة خلال فترة زمنية قصيرة والعملاء الذين تبدو عليهم علامات القلق أو التوتر أو نفاذ الصبر والعملاء الذين يحاولون تشتيت إنتباهك في وقت تنفيذ المعاملة خاصة عندما تكون المعاملة كبيرة
- ◀ كما يتعين الإلتباه بشكل خاص عندما يتم تنفيذ معاملة شراء كبيرة بإستخدام بطاقة سارية المفعول حديثة الإصدار، لأنه يتم في بعض الأحيان سرقة بطاقات الائتمان حديثة الإصدار عند إرسالها من البنك إلى حامل البطاقة الشرعي.
- ◀ تقديم العديد من البطاقات. إنتبه بشكل خاص إلى العملاء الذين يقدمون لك أرقام أكثر من بطاقتين
- ◀ أو الذين يحاولون تقسيم المشتريات.

لا تقم بتمرير البطاقة في الجهاز مرتين

إذ أن تمرير البطاقة في الجهاز مرتين يشير إلى أن التاجر يقوم بتنفيذ معاملة جديدة عند تمرير البطاقة للمرة الثانية في الجهاز وأن المعاملة الثانية جاري تنفيذها. لقد تم تعريف تمرير البطاقة لمرتين على أنه السبب الرئيسي في عدد كبير من حالات التلاعب ببيانات البطاقات حول العالم. وعند تنفيذ مثل هذه المعاملات، يكون التجار عرضة للغرامات ورسوم الإسترداد الأخرى المفروضة من قبل بنك أبوظبي التجاري.

تعليمات أخرى

- ◀ لا تقبل المعاملات المرفوضة. لا تقم بتقسيم أي معاملة مرفوضة إلى مبلغ أصغر.
- ◀ وإنتبه دائماً للبطاقات المزورة. قم بمراجعة الشريحة الموجودة على البطاقة للتأكد من أنها متضمنة في نسيج البطاقة وليست بارزة على السطح. ويمكنك التأكد من ذلك ببساطة عن طريق تمرير أصبعك على سطح الشريحة.
- ◀ إنتبه أيضاً إلى العملاء الذين يقدمون بطاقات ليست باسمائهم مدعين، عند السؤال، أن البطاقة تعود إلى أحد الشركاء أو الأصدقاء.

وفي حالة عدم تعاون العميل أو عدم مطابقة البيانات والمعلومات، لا تقم بتنفيذ المعاملة وأطلب من العميل الدفع بطريقة أخرى. وإذا بدى العميل مثيراً للريبة أو إذا بدت المعاملة مشكوك فيها، يتعين على الموظف المعني، قبل إتخاذ قرار بتنفيذ أوعدم تنفيذ المعاملة، الإتصال بمركز البطاقات في بنك أبوظبي التجاري.

فكرة: إذا تصرف العميل بطريقة مثيرة للشك، تذكر أن خسارة عملية البيع أفضل بكثير من خسارة كل من البضائع المباعة وقيمتها.

المعاملات المنفذة في عدم وجود البطاقة

المعاملات المنفذة في عدم وجود البطاقة هي تلك المعاملات التي لا يكون أي من البطاقة أو العميل متواجدين فعلياً في منفذ البيع في وقت تنفيذ المعاملة مثل تلك المعاملات التي تتم عبر الإنترنت أو بواسطة أوامر الشراء عبر البريد/الهاتف. و يكون التجار الذين يتعاملون بهذه الطريقة عرضة أكثر من غيرهم لمواجهة مخاطر أعلى للوقوع كضحايا لعمليات الإحتيال نظراً لأن تنفيذ المعاملات مع عدم وجود البطاقة وعدم التعرف على هوية العميل يجعلهم مستهدفين بشكل أكبر من قبل المحتالين. وقد تساعد الأفكار التالية على التقليل من إحتمال حدوث الإحتيال عند اللجوء إلى تنفيذ المعاملات مع عدم وجود البطاقة.

- ◀ أحصل على أكبر قدر ممكن من المعلومات: رقم بطاقة الائتمان وإسم البنك والإسم الكامل والعنوان وتاريخ الإنتهاء وأرقام الهويات (بما فيها الخط الأرضي). وفي حالة تنفيذ المعاملة من خلال جهاز طرفي مستقل، تأكد من إدخال بيانات البطاقة بشكل صحيح طبقاً لإرشادات التشغيل الخاصة بمعاملات الشراء بأوامر عبر البريد/الهاتف.
- ◀ وإستخدم شكلاً من أشكال التحقق من صحة المعاملة مثل الصفحات البيضاء الإلكترونية للتأكد من صحة البيانات المقدمة.
- ◀ قم بالإتصال بالعميل على رقم الهاتف المقدم إليك للتأكد من تفاصيل الطلب خاصة فيما يتعلق بأوامر الشراء الكبيرة و/أو المشكوك فيها.
- ◀ أطلب المزيد من إثباتات الهوية مثل صورة ضوئية من الجهة الأمامية والخلفية للبطاقة، أذ أن ذلك يثبت أن مقدم الطلب يحتفظ بالبطاقة في حوزته.
- ◀ تأكد من أن الصورة الضوئية حقيقية وسليمة وليست صورة منقذة بواسطة برنامج الفوتوشوب.
- ◀ وفي حالة قبولك لدفعات عبر موقع إلكتروني، قم بالإتصال بمزود خدمات البوابة الإلكترونية الذي تتعامل معه للتأكد مما إذا كان لديه برمجيات لمنع الإحتيال يمكنك إستخدامها.
- ◀ وإحتفظ بكافة المراسلات بما فيها الفواتير ورسائل البريد الإلكتروني وعروض الأسعار والرسائل الموجهة عبر الفاكس و إثباتات تسليم البضائع إلخ.

وأحصل دائماً على تصريح بكافة المعاملات التي يتم تنفيذها مع عدم وجود البطاقة وبكامل مبلغ المعاملة بصرف النظر عن القيمة. تذكر، أن التصريح يؤكد فقط توافر الأموال في وقت إجراء الإتصال وأنه لم يتم الإبلاغ عن فقدان أو سرقة البطاقة ولا يضمن أن الشخص الذي يقوم بذكر رقم البطاقة هو مالك البطاقة أو شخص مصرح له بإستخدامها (الصفحة V).

ما الذي يتعين البحث عنه

- ◀ البضائع التي يتم طلبها بكميات غير معتادة أو طلبات الشراء المتعددة لنفس نوع البضاعة.
- ◀ وطلبات الشراء الأكبر من تلك التي يتم طلبها عادة في سياق أعمال شركتك.
- ◀ وطلبات الشراء المطلوبة على أساس عاجل أو لتسليم خلال ليلة واحدة. كما يجب عليك الإنتباه إلى أنه عند إلغاء طلبات الشراء، يطلب العميل تحويل الأموال إلى بطاقة أخرى أو بطريقة دفع أخرى تختلف عن بطاقة الائتمان الأصلية (مثال: أوامر الدفع أو الحوالات المالية) وهذا غير مسموح به.
- ◀ وأنتبه أيضاً لتلك الحالات التي يتم فيها تقديم عدد من البطاقات المختلفة (تتضمن على أسماء حملة بطاقات مختلفين) ولكن مكان التسليم المحدد هو نفس المكان وأبحث أيضاً عن أوامر الشراء المقدمة باستخدام العديد من البطاقات بخصوص أنواع البضائع المذكورة بالتفصيل في قسم أنواع البضائع التي يستهدفها المحتالون.
- ◀ وهناك العملاء الذين يصدر عن عدد من أوامر الشراء خلال فترة زمنية قصيرة. بالإضافة إلى أوامر الشراء التي يتم إصدارها فوراً بعد رفض قبول البطاقة المقدمة والتي يتم بعدها مباشرة تقديم بطاقة ثانية.
- ◀ كما يتعين الإنتباه إلى أوامر شراء بضائع يتم شحنها إلى دولة يمكن شراء هذه البضائع فيها محلياً بسهولة.
- ◀ والسؤال الذي يجب توجيهه في هذه الحالة هو لماذا يكون المشتري مستعداً لدفع مصاريف الشحن والإنتظار لفترة أطول حتى وصول البضائع؟
- ◀ وكذلك أوامر الشراء الذي يكون رقم الهاتف الوحيد المذكور فيها هو رقم هاتف متحرك ويجب أيضاً الإنتباه إلى أوامر الشراء التي إصدارها خلال فترة زمنية قصيرة باستخدام أرقام بطاقات ائتمان متشابهة جداً بحيث لا تختلف سوى الأعداد الأربعة الأخيرة من أرقامها بالإضافة إلى طلبات شراء بضائع لا تتعامل بها عادة شركتك.

تعليمات أخرى

- ◀ قم بمراقبة عناوين التسليم المختلفة التي يستخدمها العملاء المتكررين.
- ◀ وقم بالتعرف على المناطق المنتشرة فيها الجرائم في بلدك وراقب تسليم البضائع إلى تلك المناطق.
- ◀ إنتبه جيداً عند إستلامك طلبات شراء من دول أجنبية مثل طلبات الشراء المستلمة من منطقة آسيا والشرق الأوسط وأفريقيا وهي طلبات الشراء التي يمكن أن تنطوي على مستوى أعلى من المخاطر.
- ◀ تذكر دائماً أن المسؤولية عن كافة المعاملات المنفذة في عدم وجود البطاقات تقع دائماً على عاتق التاجر. وبناء عليه، كلما زادت المعلومات التي تقوم بالحصول عليها وتدوينها كلما أقتنعت نفسك بأن المعاملة سليمة وكلما زادت فرصك لإكتشاف حالات الإحتيال وتقليل إتمالات تقديم طلبات إسترداد الأموال (الصفحة ٨).

فكرة: ننصح التجار الذين يساورهم الشك بخصوص المعاملات أو بخصوص المشتري بعدم شحن البضائع حتى ولو كان قد تم التصريح بتلك المعاملات.

أنواع البضائع التي يستهدفها المحتالون

بسبب قيمتها العالية والقدرة على إعادة بيعها، عادة ما يستهدف المحتالون أنواع البضائع التالية:

- ◀ الأدوات الكهربائية
 - ◀ والأدوات المنزلية
 - ◀ والمجوهرات
 - ◀ وأجهزة الحاسب الآلي
 - ◀ والأثاث
 - ◀ والبضائع التي يسهل التصرف فيها مقابل مبالغ نقدية.
- إذا كنت تقوم ببيع أي من أنواع البضائع هذه، فإننا نهيئ بك ممارسة أقصى درجات الحيطة والحذر قبل تسليم/ شحن البضائع. وبصفة خاصة، يتعين عليك إتخاذ كافة الإجراءات والخطوات الممكنة للتأكد من أن المشتري هو حامل البطاقة الصحيح والحقيقي. وهذا ينطبق على جميع التجار سواء كانوا يمارسون أعمالهم ويحصلون على دفعاتهم باستخدام البطاقات سواء في وجود أو عدم وجود البطاقات.

فكرة: عادة ما يستهدف المحتالون البضائع ذات القيمة العالية التي يسهل إعادة بيعها.

وفر الحماية لأعمالك وأحمي معاملاتك من مخاطر الإحتيال عند الدفع المباشر بإستخدام بطاقة موجودة

بالإضافة إلى ممارسة الحيطة والحذر لإكتشاف المعاملات المشكوك فيها، تتمثل وسيلة الدفاع الرئيسية المتاحة للتجار لمكافحة الإحتيال في تلك المواقف التي تكون البطاقة موجودة فيها في فحص البطاقة بعناية والتأكد من أنها بطاقة صحيحة وحقيقية وإدخال البطاقة في الجهاز عندما يطلب جهاز الدفع الطرفي في نقطة البيع ذلك والتأكد من صحة المعاملة بإستخدام رقم التعريف الشخصي أو الحصول على توقيع حسبا يطلب الجهاز وحيثما ينطبق، مضاهاة توقيع العميل على قسيمة المشتريات بذلك التوقيع الظاهر على الجهة الخلفية من البطاقة. وسوف تطلب أجهزة الدفع الطرفية التحقق من الهوية إما بواسطة رقم التعريف الشخصي أو من خلال التوقيع أو ربما لا يكون هذا التحقق من الهوية مطلوباً حسب طبيعة المعاملة.

ويتعين على التجار إتباع التعليمات الصادرة عن جهاز الدفع الطرفي في جميع الأوقات والإمتناع عن إدخال بيانات المعاملات يدوياً لأي سبب مهما كان في وجود كل من البطاقة والمشتري وبصفة خاصة عندما يقترح المشتري ذلك. يكون من شأن إدخال بيانات المعاملات يدوياً نقل المسؤولية إلى التاجر فيما يتعلق برموز طلبات إسترداد المبالغ المدفوعة بسبب الإحتيال لأن هذا الإجراء يؤدي إلى التنازل على الإجراءات الأمنية وإجراءات التحقق من الهوية ومن صحة البطاقة والمعاملة والجهاز الطرفي. ويتعين أيضاً القيام بإختبارات أمن المعلومات التالية:

- ◀ قم بفحص البطاقة بعناية وقم بمراجعة تواريخ بدء وإنتهاء صلاحية البطاقة وتأكد من أن البطاقة تحتوي على الإجراءات المناسبة للتأكد من حماية أمن المعلومات.
- ◀ وتأكد من أن الأعداد الأربعة الأولى من رقم البطاقة المطبوع بشكل بارز على وجه البطاقة تتطابق الأعداد الأربعة المطبوعة أسفل أو أعلى الرقم البارز مباشرة.
- ◀ وعند إمساك البطاقة بطريقة مائلة، يتعين أن تتحرك العلامة المائية الظاهرة على بطاقات ائتمان فيزا وماستركارد و أو أن يتغير لونها.

- ◀ وفيما أمكن، قم بتقديم البطاقة دائماً حسب التعليمات الظاهرة على شاشة جهاز الدفع الطرفي سواء كانت تقضي بإدخال البطاقة أو تمرير البطاقة أو النقر بالبطاقة.
- ◀ وعند تنفيذ أي معاملة يدوياً تأكد من حصولك على نسخة من البطاقة والحصول على توقيع المشتري على قسيمة المشتريات وتأكد من أن التوقيع الظاهر على قسيمة المشتريات مطابق للتوقيع الظاهر على شريط التوقيع للجهة الخلفية للبطاقة وتأكد من أن كلمات «فيزا» و «ماستركارد» تظهر بشكل متكرر بميل بزاوية ٤٥ درجة.
- ◀ وتأكد كذلك من أن الرقم المختصر لبطاقة الائتمان الظاهر على قسيمة المشتريات يطابق رقم البطاقة. وإذا لم تكن الأعداد مطابقة، فإن ذلك يشكل إشارة واضحة إلى أن البطاقة مزورة.
- ◀ تفحص عن كُتب كلاً من الجهة الأمامية والجهة الخلفية من البطاقة للتأكد مما إذا كان قد تم تغيير أو العبث بأي جزء من البطاقة.

فكرة: لا تقم أبداً بتنفيذ أي معاملة تتعلق برد مبلغ مدفوع إلى بطاقة مختلفة سواء نقداً أو بواسطة شيك أو بواسطة حوالة مالية إلكترونية.

وفر الحماية اللازمة لأعمالك ضد عمليات الإحتيال عبر الإنترنت وأوامر الشراء المستلمة عبر البريد/الهاتف

يمكن للتجار الذين يتبعون هذه الطريقة التقليل إلى أدنى حد ممكن من إمكانية التعرض لعمليات الشراء الإحتيالية وطلبات إسترداد المبالغ المدفوعة من خلال الإنترنت وطلبات الشراء عبر البريد/الهاتف عن طريق إتباع الإجراءات التالية.

- ◀ مطالبة المشتري بتقديم رقم CVV2 (فيزا) أو رقم CVC2 (ماستركارد) المكون من ثلاثة أرقام والظاهر على شريط التوقيع الموجود على الجهة الخلفية من بطاقة الائتمان.
- ◀ إذا لم تكن البطاقة في حيازة المشتري، فإنه من غير المرجح أن يكون المشتري على علم بهذا الرقم.
- ◀ طلب إسم البنك المصدر للبطاقة. عادة ما لا يكون المحتالون الذين حصلوا على بيانات الحساب من خلال إجراءات إحتيالية على علم بهذه المعلومة.
- ◀ وإذا أظهر المشتري أي تردد في ذكر أسم البنك الذي يتعامل معه، يتعين على التاجر الإلتباه وممارسة الحيطة والحذر.
- ◀ مطالبة المشتري بتقديم نسخة عبر الفاكس من رخصة القيادة الخاصة به.
- ◀ تأكد من أن العنوان الظاهر في الفواتير وعنوان تسليم البضائع متطابقين.
- ◀ وقم بمراجعة دليل الهواتف للتحقق من صحة العنوان وأرقام الهواتف المذكورة من قبل المشتري.
- ◀ لا تقم أبداً بإرسال البضائع إلى صندوق بريد وأحصل على إيصال موقع من حامل البطاقة عند تسليم البضائع.
- ◀ وفي حالة طلبات الشراء المنطوية على أعداد كبيرة من بضائع مختلفة، قم بالإتصال بحامل البطاقة بعد إستلام طلب الشراء لتأكيد الطلب. وأطلب أيضاً من المشتري إعادة تلاوة جميع بيانات طلب الشراء.
- ◀ في كثير من الأحيان، عندما يكون طلب الشراء ينطوي على حالة إحتيال، لا يكون المشتري قادراً على تأكيد كافة هذه التفاصيل إذ أنه كان يطلب بضائع بشكل عشوائي دون وجود سجل لما تم طلبه.
- ◀ يتعين عليك الشعور بالقلق عند إستخدام العديد من البطاقات لتنفيذ عملية شراء واحدة.
- ◀ ولا تستمر في محاولة الحصول على تصريح بعد إستلام رفض لهذا التصريح.
- ◀ وإنتبه بشكل خاص إلى أوامر الشراء المستلمة من خارج الدولة التي تمارس أعمالك فيها.
- ◀ ويتعين دائماً تأجيل شحن طلبات الشراء الكبيرة حتى يتم الإلتهاء من إجراء كافة الإستفسارات الآتفة الذكر للتأكد من مصداقية المشتري.
- ◀ يتعين على التجار الإمتناع عن شحن البضائع حتى يتم التأكد من مشروعية ومصداقية المشتري.

فكرة: لا تقم أبداً بتنفيذ معاملة رد مبالغ مدفوعة إلى بطاقة مختلفة أو نقداً أو بواسطة شيك أو بواسطة حوالة مالية إلكترونية (الصفحة ١٠)

حماية نفسك من المعاملات الإحتيالية

لتحويل الأموال في بعض الأحيان يطلق على المعاملات الإحتيالية لتحويل الأموال عبر الإنترنت «الإحتيال النيجيري» وهي المعاملات التي تشكل باستمرار مشكلة للتجار. وتنطوي هذه المعاملات على إستخدام معلومات بطاقات ائتمان مسروقة للحصول على أموال عبر حوالات مالية.

ما هي طريقة تنفيذ هذه المعاملات؟

يتمثل الهدف النهائي من هذه العملية الإحتيالية في خداعك لتقديم الأموال إلى المحتالين أو إلى طرف ثالث غير معلوم (غالباً ما يكون يعمل لصالح المحتالين) من خلال طريقة دفع أخرى مثل بطاقة ائتمان مختلفة أو نقداً أو بواسطة شيك أو بأي طريقة تحويل أموال إلكترونية أخرى. ويمكن أن يتخذ هذا الشكل البديل للدفع هيئة رد أموال أو طلب لتنظيم عملية شحن لدى شركة تسليم بريد معينة لا وجود لها فعلياً.

مثال:

في هذا السياق، تستخدم البطاقات المزورة لشراء بضائع / خدمات ويقوم بعد ذلك حامل البطاقة المزعوم بدفع قيمة المعاملة إلى طرف ثالث مرتبط به. على سبيل المثال، يتم شراء ملابس وإكسسوارات بمبلغ ٤,٠٠٠ درهم من خلال طلب شراء عبر الهاتف ويطلب حامل البطاقة من التاجر تغطية تكلفة خدمات شركة تسليم البريد البالغة ١,٠٠٠ درهم وبذا تصل قيمة المعاملة إلى ٥,٠٠٠ درهم إمارات. يدفع التاجر إلى شركة تسليم البريد مبلغ ١,٠٠٠ درهم بحوالة مالية/ مصرفية وهو المبلغ الذي يصبح خسارة مباشرة. ويدعي حامل البطاقة بعد ذلك بعدم صحة المعاملة (أو يقوم بمنازعة في مبلغ المعاملة) وبالتالي يتم عكس قيد المعاملة ورد مبلغ ٥,٠٠٠ درهم بالخصم من حساب التاجر. ويتحمل التاجر خسارة إضافية في حالة إستبدال البضائع.

ملاحظة: هذا مجرد مثال واحد على المعاملات الإحتيالية. يتميز المحتالون بقدراتهم الإبداعية وإمكانية التوصل إلى سيناريوهات مختلفة للإحتيال على التجار، بيد أن تحويل الأموال إلى حامل البطاقة أو إلى طرف ثالث بواسطة وسائل أخرى عادة ما تكون حوالات مالية إلكترونية أحد أهم العناصر الشائعة للإستخدام.

ما الذي يتعين علي فعله؟

- ❖ إستخدم حدسك وحواسك إذا بدت عملية البيع جيدة بشكل مبالغ فيه وبطريقة مثيرة للشك فعادة ما تكون منطوية على إحتيال.
- ❖ لا تقم برد أي مبالغ إلا إلى بطاقة الائتمان المستخدمة لتنفيذ معاملة أصلية وإمتنع عن إرسال الأموال من خلال الحوالات المالية الإللكترونية في هذا السياق.
- ❖ وقم بمراجعة المعاملات التي تنطوي على مستويات أعلى من مخاطر الإحتيال بما فيها أوامر الشراء المستلمة من الخارج من مناطق مثل غرب أفريقيا وشرق أوروبا.
- ❖ حاول الإبتعاد عن سيناريوهات سوق الحظ إذ أن هذه المعاملات عادة ما تستغل حسن نيتك.

مخاطر أخرى يتعرض لها التجار

تبييض المبيعات : (التنفيذ بواسطة طرف ثالث)

يشير تعبير « التبييض » في سياق أعمال أي تاجر إلى أي موقف مثل قبول محل تجاري تنفيذ معاملات بالنيابة عن شركة أخرى في بعض الأحيان يسعى الأفراد من ذوي السمعة السيئة إلى التجار الشرعيين وذوي السمعة الجيدة لطلب تنفيذ معاملات باستخدام بطاقات الائتمان الخاصة بهم وعادة ما يتم دفع نسبة من مبلغ المعاملة إلى التاجر. وبالإضافة إلى أن هذا التصرف يشكل مخالفة صارخة لأحكام وشروط بنك أبوظبي التجاري، فإنه يعتبر أيضاً ممارسة شديدة الخطورة تعرض أعمال التاجر إلى مخاطر كبيرة. في كثير من الحالات يكون الشخص الذي يطلب من التاجر تنفيذ معاملاته غير قادر على الحصول على تسهيلات التجار بإسمه، ربما بسبب ممارسات سابقة غير لائقة. وبالتالي، تكون فرص حدوث معاملات إحتيالية كبيرة جداً ومرتبعة للغاية. يجب على التاجر الإمتناع عن تنفيذ أي معاملة بالنيابة عن أي شخص آخر أو فيما يتعلق بأي معاملة لا يقوم فيها ببيع البضائع أو الخدمات مباشرة إلى عملائه.

فكرة: التبييض، في سياق أعمال التجار، يشكل ممارسة خطيرة جداً يمكن أن تؤدي إلى تكبد خسائر كبيرة.

المعاملات الإحتيالية لإسترداد الأموال

يتمثل أحد الأنواع الشائعة للإحتيال في إضافة الموظفين لأموال (مبالغ مستردة) إلى حساباتهم الخاصة، ولتفادي إكتشاف هذه الحالات، يمكن لهؤلاء الموظفين أن يقوموا بخصم مبالغ كبيرة باستخدام بطاقة مزورة و تسوية هذا الخصم بإضافة المبلغ إلى حساباتهم الخاصة. وفي هذا النوع من المواقف، عادة ما يستغرق الأمر بضع أسابيع أو حتى أشهر قبل إكتشاف حالة الإحتيال. وللتصعب من هذا النوع من الإحتيال، فإننا نوصي التجار بمتابعة كافة المبالغ المضافة في الحسابات عن كُتب و مراجعة كافة الإيداعات والخصومات المتعلقة بنفس رقم البطاقة. ويتعين الإنتباه بصفة خاصة إلى المبالغ الكبيرة المضافة في الحسابات، وهناك طريقة أخرى يمكن للتجار من خلالها توفير الحماية لأنفسهم ضد هذا النوع من الإحتيال تتمثل في تغيير كلمة المرور الخاصة بجهاز الدفع الطرفي أو الخاصة بهم كمستخدمين لهذا الجهاز بصفة منتظمة وبصفة خاصة بعد ترك أحد الموظفين للخدمة لديهم.

فكرة: تأكد من تغيير كلمة المرور الخاصة بك بانتظام لمنع الإستخدام غير المصرح به أو غير المشروع للتصريح الإلكتروني بالمشتريين.

المخاطرة الرئيسية التي تواجه التجار الذين يقبلون تنفيذ المعاملات عبر الإنترنت

هي الصعوبة التي يواجهونها في التأكد من أن المشتري هو حامل البطاقة الحقيقي والصحيح. وعند تقديم حامل البطاقة لمنازعة في عملية شراء تمت إلكترونياً عبر الإنترنت، بصرف النظر عن صحة هذا الإدعاء من عدمه، عادة ما يكون التاجر ملزماً برد مبلغ عملية الشراء. وقد حاولت كل من شركة فيزا وشركة ماستركارد بصفة مشتركة التغلب على هذه العبء الملقى على عاتق التجار الذين يستخدمون الإنترنت عن طريق تطوير خدمة التحقق من هوية حامل البطاقة تعرف بأسم «تم التحقق بواسطة رمز المصدر من فيزا و ماستركارد» (الصفحة ١٢) حيث يشير تعبير 3D Secure إلى المنصة التقنية التي يتم تقديم هذه الخدمة من خلالها.

وتتمثل آلية عمل «تم التحقق بواسطة رمز المصدر من فيزا وماستركارد» فيما يلي:

- ◀ يقوم حامل البطاقة بالتسجيل لدى البنك الذي يتعامل معه ويقوم حامل البطاقة بإختيار كلمة مرور (مماثلة لرقم التعريف الشخصي المستخدم في أجهزة الصراف الآلي)
- ◀ ويقوم حامل البطاقة بزيارة الموقع الإلكتروني الخاص بالتاجر وإختيار البضائع/ الخدمات التي يرغب بشرائها.
- ◀ وعند محاولة حامل البطاقة تنفيذ عملية الشراء، يطلب منه إدخال كلمة المرور التي كان قد إختارها سابقاً عند التسجيل لدى البنك الذي يتعامل معه.
- ◀ ويمكن لبرمجيات 3D Secure إكتشاف ما إذا كانت البطاقة مسجلة أم أنها تحتاج إلى التسجيل.
- ◀ ويتم إتباع عملية التصريح هذه بخصوص البطاقات غير القادرة على دعم هذه الخدمة.
- ◀ وعند إدخال حامل البطاقة لكلمة المرور يتم تمرير المعلومات إلى البنك الذي يتعامل معه حامل البطاقة للتحقق من صحتها.
- ◀ ويتم بعد ذلك إرسال نتيجة التحقق من كلمة المرور إلى التاجر لإبلاغه ما إذا كانت كلمة المرور التي تم إدخالها صحيحة.
- ◀ وإذا كانت كلمة المرور التي تم إدخالها غير صحيحة، يحتمل أن يكون الشخص المنفذ لعملية الشراء ليس هو حامل البطاقة الصحيح والحقيقي ويتعين على التاجر في هذه الحالة عدم الإستمرار في تنفيذ المعاملة إذ أن المسؤولية تنتقل إلى التاجر.

وتتمثل الميزة الرئيسية بالنسبة للتاجر من عمليات التحقق هذه في إنتقال المسؤولية عن المطالبات بإسترداد المبالغ المدفوعة. وبإستثناء بعض الحالات القليلة، في حالة محاولة التاجر للتحقق من هوية المشتري بإستخدام برمجيات 3D Secure يخسر كل من حامل البطاقة والبنك الذي يتعامل معه الحق في تقديم مطالبة لإسترداد المبالغ المدفوعة على زعم أن حامل البطاقة لم يقوم بتنفيذ المعاملة. ويتم تنفيذ هذه الإجراءات بصرف النظر عما إذا كان التاجر أو البنك الذي يتعامل معه مشتركاً في برمجيات وخدمات 3D Secure إذ أن كل ما يتطلبه الأمر هو قيام التاجر بإستخدام برمجيات 3D Secure ومحاولته التأكد من صحة كلمة المرور المدخلة بواسطة حامل البطاقة. وبالطبع، في حالة ظهور نتيجة سلبية لعملية التحقق من صحة كلمة المرور (إدخال المشتري لكلمة مرور خاطئة) يجب عليك عدم الإستمرار في تنفيذ المعاملة. وفي حالة إستمرارك في تنفيذ المعاملة بعد ظهور نتيجة سلبية لعملية التحقق من هوية حامل البطاقة، فإنك تتحمل المسؤولية عن المطالبة بإسترداد المبلغ المدفوع.

التقليل من المخاطر التي تواجه التجار المتعاملين عبر الإنترنت

قم بحماية معلومات عملائك

نحن ملتزمون في بنك أبوظبي التجاري بموافاة جميع التجار الذين تتعامل معهم بكافة المساعدات الممكنة لتمكينهم من حماية أعمالهم وعملياتهم من التهديدات المتزايدة الناشئة عن ممارسات المجرمين الذين يستخدمون تقنيات متقدمة. ودون شك، فإن هذا يشكل أحد أكبر التحديات التي تواجه التجار ومعاملات الشراء في الوقت الحاضر. إذا كنت أحد التجار الذين لديهم إمكانية الوصول إلى بيانات ومعلومات بطاقات الائتمان أو إمكانية تخزين تلك البيانات والمعلومات بأي شكل من الأشكال أو إذا كنت تستخدم مزود خدمات يقوم بذلك بالنيابة عنك، فإنك تتحمل المسؤولية عن التأكد من الحفاظ على أمن معلومات الدفع الخاصة بعملائك. ومن المهم أن تفهم الإجراءات التي يتعين عليك إتخاذها للتأكد من حماية المعلومات المالية الشخصية شديدة الحساسية.

فكرة: تعرف على أهمية أمن المعلومات وأدرك أنك مسؤول عن التأكد من حماية أمن بيانات ومعلومات عملائك.

متطلبات الموقع الإلكتروني

يجب على جميع التجار الذين يستخدمون خدمات الإنترنت الخاصة بالتجار الإلتزام بمعايير الموقع الإلكتروني لبنك أبوظبي التجاري. ويحتفظ بنك أبوظبي التجاري بحق رفض أو إبطال تفعيل الدخول أو إنهاء استخدام التجار لهذه الخدمة في حالة عدم إلتزامهم بالمتطلبات التالية:

١- يجب أن يلبى الموقع الإلكتروني الخاص بك كافة المعايير التالية:

- ◀ يجب أن لا يكون هناك أي إختلافات جوهريّة بين الأسم التجاري وأسم مُعرف مكان الموقع (URL) إذ أن من شأن ذلك التقليل من إمكانية تعرض حامل البطاقة للإرتباك.
- ◀ إظهار الموقع الإلكتروني لوصف واضح للبضائع والخدمات المعروضة للبيع وبيانات الإلتصال والاسم التجاري وأرقام الهواتف والعنوان ورقم الفاكس حيثما ينطبق، بالإضافة إلى شرح وافٍ لإجراءات الشحن وسياسة/الإطار الزمني لتسليم البضائع.
- ◀ عملة المعاملة: يجوز للتجار الذين يتعاملون مع بنك أبوظبي التجاري تنفيذ معاملاتهم بعملة درهم الإمارات فقط ويمكنهم إستلام المبالغ في حسابات بعملة درهم الإمارات فقط.
- ◀ إظهار إجمالي تكلفة البضائع أو الخدمات المشتراه شاملة كافة رسوم الشحن والعلامات التجارية الخاصة بخطة البطاقة وما إذا كانت خيارات الدفع متاحة. القيود على التصدير (إن وجدت) - الدول التي لا يقوم التجار بالشحن إليها.
- ◀ سياسة واضحة لرد المبالغ/إعادة البضائع وسياسة خصوصية بيانات العملاء - تعلن فيها عن الطريقة التي تنوي إستخدام المعلومات التي حصلت عليها من عملائك. إمكانيات أمن المعلومات وسياسة تحويل بيانات بطاقة الدفع.
- ◀ يجب أن يستخدم اسم الموقع الإلكتروني لكل تاجر صفحات دفع مستقلة. ويكون من الضروري التأكد من عدم وصول الروابط الخاصة بالموقع الإلكتروني إلى موقع آخر يمكن سداد الدفعات فيه فيما يتعلق بالبضائع أو الخدمات المعروضة من خلال الموقع الإلكتروني الأول.
- ◀ جميع المعلومات يجب أن تكون دقيقة من كافة النواحي

٢- يجب أن لا يحتوي الموقع الإلكتروني الخاص بك على:

- ◀ أي شيء يشكل أو يشجع على مخالفة أي قوانين أو أنظمة مطبقة بما في ذلك على سبيل المثال لا الحصر بيع بضائع غير مشروعة أو مخالفة ضوابط التصدير أو قوانين الميسر (الصفحة ١٤).

- ◀ إظهار أي محتويات مخصصة للبالغين فقط أو تنطوي على أفلام إباحية.
- ◀ عرض للبيع بضائع أو خدمات أو استخدام مواد عرض يمكن إعتبارها بواسطة أي شخص عادي مخلة بالآداب أو غير محتشمة أو مسيئة أو خطيرة أو غير مناسبة بأي طريقة أخرى.
- ◀ استخدام صفحات دفع غير معتمدة.
- ◀ الإخفاق في استخدام الشهادات الرقمية لتأسيس جلسة تصفح آمنة في الموقع الإلكتروني.

٣- صفحات الدفع يجب أن تكون معتمدة من قبل بنك أبوظبي التجاري أو من قبل مزود خدمات معتمد معين من قبل بنك أبوظبي التجاري ويجب أن تكون مطابقة لمتطلباتنا الخاصة بأمن المعلومات.

٤- يجب عليك استخدام شهادات رقمية لتأسيس جلسة تصفح آمنة على الموقع الإلكتروني بينك وبين عميلك.

٥- يتعين عليك عدم تغيير أنواع البضائع أو الخدمات المباعة من خلال منفذ البيع الخاص بك دون توجيه إشعار خطي إلى بنك أبوظبي التجاري ومن ثم إستلام موافقة خطية من البنك تؤكد موافقة البنك على هذا التغيير (الصفحة 10).