Payment Services

Sicherheitstipps für Mail-/Phone-Order

Der Diebstahl und missbräuchliche Einsatz von Kartennummern verursachen auch im Mail-/Phone-Order Geschäft jedes Jahr einen beträchtlichen finanziellen Schaden. Solche Fälle sind jeweils mit grossem administrativen Aufwand verbunden. Wir möchten Ihnen mit den nachfolgenden Informationen helfen, sich vor Kartenbetrügern besser zu schützen.

Die Betrüger gehen oft nach dem gleichen Muster vor:

- Per Fax, E-Mail oder Telefon wird eine grosse Bestellung aufgegeben. Die Lieferung soll per Express oder über einen Paketkurier zu Lasten des Bestellers umgehend geliefert werden. Die Lieferadresse befindet sich dabei meistens im Ausland. Oft wird die Lieferung auch in ein Hotel oder postlagernd verlangt.
- Die Bezahlung erfolgt oftmals über mehrere Karten.

Gemäss den Vertragsbedingungen für das Distanzgeschäft sind Sie verpflichtet, für jede Transaktion eine Autorisation einzuholen. Die Autorisation bestätigt aber nur die Gültigkeit der Karte und die Bonität des Karteninhabers zum fraglichen Zeitpunkt.

Ob es sich beim Besteller um den rechtmässigen Karteninhaber handelt oder ob jemand anderes mit seiner Karte und seinen Daten eine unrechtmässige Bestellung macht, kann nicht zweifelsfrei überprüft werden.

Aus diesem Grund lehnen die Kartengesellschaften bei Bestellungen per Fax oder Telefon jegliche Haftung ab.

Das Risiko liegt bei Ihnen

Während die Betrüger die Ware in Empfang nehmen, weigern sich die rechtmässigen Karteninhaber, die Belastungen zu akzeptieren. Dies ist für den betroffenen Vertragspartner oftmals sehr unangenehm: Einerseits hat er den Verlust der Waren zu beklagen, andererseits erhält er eine Rückbelastung über den gesamten Betrag.

Folgende Tipps sollen Ihnen helfen, das Risiko zu minimieren:

1. Kartenakzeptanz

Die Annahme von Bestellungen ist gemäss Kartenakzeptanzvertrag nur per Fax und per Telefon oder über einen Webshop zulässig. Erhalten Sie per E-Mail Bestellungen, welche Kartendaten enthalten, informieren Sie den Absender, dass diese Art der Bestellung unzulässig ist.

Löschen Sie die Kartennummer vor dem Versenden Ihrer Antwort aus dem E-Mail. Drucken Sie das E-Mail aus und löschen Sie dieses aus dem «Posteingang» sowie aus dem Ordner «Gelöschte Objekte».

2. Physisch vorhandene Kartendaten

Stellen Sie sicher, dass Papierunterlagen mit vollständig angezeigten Kartennummern nie unbeaufsichtigt sind und werfen Sie diese nicht in den Abfalleimer. Vernichten Sie die Unterlagen mit einem Aktenvernichter, so dass keine Informationen rekonstruiert werden können.

Entsorgen Sie nicht mehr benötigte Unterlagen mit Kartendaten fortlaufend.

3. Übermittlung von Kartennummern

Bevor Sie Kartennummern übermitteln, überlegen Sie sich, ob der Empfänger zwingend die vollständige Kartennummer benötigt. Falls nicht, senden Sie die Kartennummer in folgender Darstellung: XXXX XXXX XXXX 1234. Diese Darstellung der Kartennummer wird als PAN-Truncation bezeichnet.

Verzichten Sie grundsätzlich auf die Übermittlung von Kartennummern per E-Mail. Teilen Sie Kartendaten per Telefon oder Fax mit.

4. Internet-Bestellungen

Online-Shop-Betreibern empfehlen wir, die neuen Standard-Sicherheitslösungen «Verified by Visa» und «MasterCard SecureCode» mit der entsprechende Zahlsoftware (Merchant Plug-In, MPI) einzusetzen. Mit diesen Verfahren kann das Betrugsrisiko wesentlich reduziert werden.[1]

Haben Sie ein eigenes Bestellformular, so stellen Sie sicher, dass dieses den Vorgaben von PCI DSS entspricht (keine Abfrage von CVC2/CVV2). Überprüfen Sie den Bestellablauf auf die Übermittlung sowie gegebenenfalls auch die (Zwischen-)Speicherung von Kartendaten.

5. Prüfung der Bestellung

Seien Sie vorsichtig bei Bestellungen über unüblich hohe Mengen und Beträge, bei einem hohen Bestellrhythmus oder bei E-Mail-Adressen von Gratisprovidern, wie yahoo.com, gmx.com oder hotmail.com.

6. Prüfung der Lieferadresse

Prüfen Sie die Lieferadresse ganz genau, wenn diese nicht mit dem Wohnsitz des Bestellers übereinstimmt.

Von Lieferungen in Entwicklungsländer, vor allem nach Afrika, Fernost und Südamerika, sowie in Länder der ehemaligen GUS raten wir Ihnen dringend ab, ausser es besteht eine Ihnen bekannte und etablierte Geschäftsbeziehung.

Seien Sie zudem vorsichtig bei Lieferungen an eine Postfachadresse oder in ein Hotel.

7. Risiko abschätzen

Würden Sie die Lieferung auch gegen Rechnung vornehmen? Die Kreditkarten bzw. Debitkarten wie Maestro sind ein sehr praktisches Zahlungsmittel, aber kein Inkasso-Instrument.

Sie wissen am besten, wie Ihre Geschäftsfälle in der Regel ablaufen. Wenn Sie Zweifel haben, das Geschäft aber dennoch gerne machen möchten, empfehlen wir, sich betreffend einer Exportrisikogarantie an Ihre Hausbank zu wenden.

[1] Für die Kartenbrands Diners Club und Discover wird kein Merchant Plug-In benötigt.

110.0174.01 INT_DE/02.2016

Ihren lokalen Ansprechpartner finden Sie unter: www.six-payment-services.com/kontakt

SIX Payment Services AG
Hardturmstrasse 201
Postfach
CH-8021 Zürich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxemburg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Wien
Österreich