Händlerservice

Maßnahmenkatalog zur Erkennung und Reduzierung von Betrug im E-Commerce

Version: 2.4 vom 02.08.2011

Rechtlicher Hinweis

Händlerservice

Inhaltsverzeichnis

1 Vorbemerkung

Die Verfahren mit der höchsten Sicherheit, bei weltweiter Einsatzmöglichkeit, sind die von den Kartenorganisation MasterCard und Visa entwickelten 3D-Secure-Verfahren, bei denen sich die Karteninhaber vor der Autorisierung bei Ihrer Bank authentifizieren. Nahezu sämtliche Kartenherausgeber in Deutschland haben inzwischen auf dieses Verfahren umgestellt. Händler, die dieses Verfahren nicht anbieten, sehen sich daher einem nicht unerheblichen Haftungsrisiko gegenüber. Wir empfiehlen aus diesem Grund jedem Händler für sein E-Commerce-Geschäft die Nutzung dieses Verfahrens. Nähere Informationen erhalten Sie unter www.s-haendlerservice.de/3d-secure.

Wenn Sie dieses Verfahren noch nicht nutzen oder Ihre Kunden noch nicht registriert sind, sollten Sie folgende Hinweise beachten. Diese Maßnahmen können Betrug nicht vollkommen verhindern, jedoch dazu beitragen, betrügerische Transaktionen zu erkennen und zu minimieren. Ziel dabei ist es, weder Umsätze zu verhindern, noch gegenüber allen Kunden misstrauisch zu sein. Es geht um das richtige Maß an Eigenverantwortung und kaufmännischer Sorgfalt, um das Risiko jeder einzelnen Transaktion zu beurteilen.

2 Betrugserkennung

2.1 Definieren Sie Ihr Risiko

Sie sollten sich im Vorfeld Gedanken machen, ob und wie Ihr Angebot für potentielle Betrüger interessant sein könnte und Maßnahmen dagegen entwickeln. So gehen Sie systematisch vor und erkennen Schwachstellen frühzeitig. Die folgenden Fragen sind nur als Anregung gedacht und erheben keinen Anspruch auf Vollständigkeit.

2.1.1 Warensortiment

Welche Waren vertreiben Sie (virtuell/physisch)?

Welchen Wiederverkaufswert haben Ihre Waren? Vertreiben Sie Markenartikel?

Besteht eine hohe Nachfrage und ist der Wiederverkauf damit einfach?

In welchem Preissegment bewegen sich Ihre Waren?

Welche Verluste sind im Preis einkalkuliert?

2.1.2 Kunden

Welches Klientel haben Sie – Alter, Zielgruppe?

Liefern Sie an Privatkunden oder Firmenkunden?

2.1.3 Lieferland

Gibt es Einschränkungen oder liefern Sie weltweit? Bitte beachten Sie hierzu auch die Hinweise zu Risikoländern (www.s-haendlerservice.de/e-commerce).

2.1.4 Branche

Zählt Ihre Branche zu einer Risiko-Branche (z.B. Markenartikel)?

2.2 Tätergruppen

In Abhängigkeit vom Warenwert kann i. d. R. in zwei Tätergruppen unterschieden werden:

1. Täter, die durch Einsatz gestohlener Karten bzw. Kartendaten hochwertige bzw. große Mengen an Waren zum Weiterverkauf erlangen wollen. Hier handelt es sich in der Regel um hohe Transaktionsbeträge.
2. Täter, die mit gefälschten oder gestohlenen Karten- bzw. Kartendaten kostenlos virtuelle Dienste/Services erlangen wollen. Hier handelt es sich meist um niedrige Transaktionsbeträge.

Der wirtschaftliche Schaden ist bei der ersten Tätergruppe sehr hoch, da hochwertige Waren physisch verschickt werden. Da es sich bei der zweiten Gruppe eher um virtuelle Waren/Dienstleistungen handelt, sind die Verluste i. d. R. geringer. Allerdings spielt hier der Bearbeitungsaufwand eine Rolle.

2.2.1 Rückbelastungen im Betrugsfall

In beiden vorgenannten Betrugsfällen kommt es zur Rückabwicklung der Transaktionen (Chargeback), wenn der Karteninhaber nicht eindeutig identifiziert werden konnte. Eine Bestellung per E-Mail oder Fax, selbst eine Kopie der Kreditkarte in Verbindung mit einer Ausweiskopie reichen nicht aus. Damit es nicht so weit kommt, sollten Sie auf folgendes achten:

2.3 Maßnahmen vor der Bestellung

Generell sollten die Schutzmaßnahmen dem individuellen Transaktionsverhalten angepasst werden. Maßnahmen, die für alle Transaktionen gleich sind, lassen sich schnell durchschauen und sind damit wirkungslos.

2.3.1 Registrierung

Bieten Sie Ihren Kunden die Möglichkeit der Registrierung an. Sie dient nicht nur der Kundenpflege, sondern stellt eine Hemmschwelle dar. Sie sollte so umfangreich sein, dass weder eine Software (Robots) noch Täter mit ausgeprägtem Spieltrieb ohne Konsequenzen die Registrierung einfach durchführen können. Gleichzeitig soll sie ehrliche Kunden nicht abschrecken.

2.3.1.1 Adressdaten

Akzeptieren Sie nur vollständige Adressen, schließen Sie „Donald Duck & Co“. aus. Nutzen Sie bestehende Blacklists oder legen Sie Liste an. Definieren Sie Länder, in die Sie nicht liefern. Wenn dennoch eins dieser Lieferländer bei der Registrierung angegeben wird, geben Sie keinen Hinweis und lassen die Registrierung erfolgreich abschließen (Roboter). Sie können im späteren Bezahlvorgang diese Lieferländer automatisch durch die Blacklist ablehnen lassen.

Vergleichen Sie z.B. die Geo-IP-Adresse mit dem Lieferland, akzeptieren Sie keine mobilen Rufnummern und lassen Sie keine freien E-Mail Adressen zu (z.B. @gmx, @hotmail).

Der Name des Kunden in der Registrierung, der Name des Karteninhabers und des Empfängers sollten identisch sein (zumindest bei der Erstbestellung).

2.3.2 Limitierungen

Definieren Sie Limits in Betrag und Menge für Erstbestellungen und Limits für zusätzliche Kontrollen bei Folgebestellungen.

Lassen Sie höchstens eine Fehleingabe bei der Kartennummer zu (ggf. über Einstellungen beim Payment Service Provider). Wenn Sie nach einer Ablehnung die Eingabe einer weiteren Kartennummer zulassen, führen Sie zusätzliche Prüfungen durch.

2.3.3 Kundenhistorie

Vergleichen Sie anhand früherer Bestellungen das Kundenverhalten. Berücksichtigen Sie auch erhaltenen Beleganforderungen oder Rückbelastungen und ordnen Sie diese Ihren Kunden zu.

2.3.4 Erklärungen

Stellen Sie auf Ihrer Webseite klar, dass Betrug und Betrugsversuche verfolgt und zur Anzeige gebracht werden.

2.4 Maßnahmen während der Bestellung

2.4.1 Was wird bestellt

Vergleichen Sie übliche Mengen mit der aktuellen Bestellung. Werden z.B. alle möglichen Konfektionsgrößen bestellt oder technische Komponenten, die nicht zusammenpassen? Prüfen Sie die Bestellfrequenz, weicht diese vom üblichen Kundenverhalten ab? Im Zweifel warten Sie mindestens 45 Tage, bis Sie die nächste Bestellung zulassen. In der Regel erhalten Sie in dieser Zeit im Fall eines Missbrauchs die Rückbelastung durch die Bank.

2.4.2 Querverbindungen

Prüfen Sie, ob die Angaben bei der Registrierung bereits in anderer Kombination bei Ihnen verwendet wurden. Stimmen einzelne Werte überein, erzeugen Sie bei jedem Treffer in Abhängigkeit von der Wahrscheinlichkeit einen Wert und addieren Sie diesen am Schluss. So erhalten Sie einen Score-Wert, zu dem Sie in Abhängigkeit von dessen Höhe weitere Maßnahmen definieren können.

Vorname + Nachname

Anschrift

Telefonnummer (mobile Rufnummern sind als kritisch einzustufen)

Karteninhaber-Name

E-Mail Adresse

IP-Adresse

Username

Kennwort

elektronischer Fingerprint des User-PC's

2.4.3 Zusätzliche Prüfung

Im Zweifel halten Sie die Lieferung lieber zurück. Klären Sie z.B. durch einen Telefonrückruf, ob es sich um den Besteller handelt. Lassen Sie sich vom Kunden zusätzlich ein Fax mit Identitätsnachweisen schicken, oder ein Bild (Kopie) der Karte zusammen mit der Bestellnummer. Fragen Sie nach zusätzlichen Details zur Person, z.B. Geburtsdatum, Ort, Ausweisnummer oder auch nach dem Namen der Karten ausgebenden Bank.

2.5 Maßnahmen bei Abschluss der Bestellung

2.5.1 Lieferung

Lassen Sie Lieferungen an Zweitadressen nur für Stammkunden zu. Betrüger versuchen immer schnellstmöglich an die Ware zu kommen, daher achten Sie besonders auf Bestellung mit Expresslieferung. Unterbinden Sie nach Rücksprache mit dem Logistik-Unternehmen die Auslieferung durch Ablegen an der Tür, Garage etc. Lassen Sie keine Lieferung an Firmenadressen ohne Ansprechpartner und dem Vermerk „eigenhändig" zu. Liefern Sie nicht an offizielle Gebäude (Postlagernd, Bahnhöfe, Hotels) oder ungenaue/suspekte Adressen, die spätere Nachforschungen unmöglich machen. Auch Packstationen können ein Indiz für eine betrügerische Bestellung sein.

2.5.2 Historie

Führen Sie eine Kundenhistorie, in die Sie auch Rückbelastungen einfließen lassen. Vermerken Sie nicht zustellbare Lieferungen. Speichern Sie abgelehnte Autorisierungsanfragen. Beachten Sie dabei, dass weder die vollständige Kartennummer noch die Kartenprüfnummer gespeichert werden dürfen. Arbeiten Sie stattdessen mit Ihren Kunden- oder Rechnungsnummern, die Sie bei jeder Transaktion einfach mitschicken.

2.5.3 Aktualisierung der Blacklist

Wenn Sie negative Erfahrungen gemacht haben, aktualisieren Sie Ihre persönliche Blacklist, um einen erneuten Kauf auszuschließen.

Grundsatz

Lassen Sie nur solche Bestellungen zu, die Sie auch selbst durchgeführt hätten und bei denen Sie ein gutes Gefühl haben. Denken Sie immer daran, dass das wirtschaftliche Risiko letztendlich bei Ihnen liegt.