Sicherheit bei der Akzeptanz von Kreditkartenzahlungen im Fernabsatz

Was bedeutet Fernabsatz?

Im Allgemeinen beschreibt die Bezeichnung Fernabsatz, dass der Kunde mit seiner Karte nicht vor Ort beim Händler ist und die Kartendaten seiner Karte nicht an einem Terminal ausgelesen werden.

MoTo-Zahlung:

Der Händler erhält die Kreditkartendaten seines Kunden über das Telefon, per Fax oder per Email. Nun kann der Händler durch Eingabe der Kartendaten über ein stationäres Terminal oder ein Online Bezahlsystem eine Belastung auf der Karte seines Kunden veranlassen.

E-Commerce-Zahlung:

Hier ist der Online-Shop des Händlers direkt mit einem virtuellen Terminal verbunden. Der Kunde gibt selbst seine Kartendaten ein und veranlasst somit selbst die Abbuchung von seiner Kreditkarte.
Sofern Sie Zweifel an einer Bestellung haben, führen Sie die Bestellung nicht aus! Fragen Sie bei der Bestellung immer nach der Kartenprüfnummer (CCV - auf der Rückseite der Karte) und teilen Sie diese bei der Genehmigungsanfrage (sofern diese über die Autorisierungshotline durchgeführt wird) mit.

Werden Sie aktiv!

Der Onlineversandhandel eröffnet viele Möglichkeiten, birgt aber auch Risiken, denen Sie als Betreiber eines Shops vorbeugen können, indem Sie die folgenden Tipps befolgen.

Prüfen Sie jede eingehende Bestellung sorgfältig!

Schließen Sie im Vorfeld besonders kritische Länder für den Warenversand aus:

Afrika: Elfenbeinküste, Nigeria, Ghana, Ägypten
Asien: Indonesien, Philippinen, Malaysia
Osteuropa: Rumänien, Bulgarien, Litauen, Kasachstan, Ukraine, Balkanstaaten (ehem. Jugoslawien), Ungarn
Westeuropa: Großbritannien (hier speziell Großraum London), Niederlande (hier speziell Rotterdam/Amsterdam/Hakfort)

Ziehen Sie Rückschlüsse aus dem Verhalten des Bestellers!

- Die Versandanschrift hat keinen Bezug zum Karteninhaber (Versand ins Ausland an eine Postbox).
- Der Kunde möchte den Rechnungsbetrag auf mehrere Kreditkarten aufteilen.
- Auf einer Bestellung stehen mehrere Kartennummern mit gleichen oder unterschiedlichen Namen.
- Der Besteller kündigt im Vorfeld bereits Probleme an, wi e z .B. : „sollte die Karte nicht funktionieren, dann schicke ich Ihnen die Kartennummer meiner Frau“.
- Die Versandkostenhöhe spielt keine Rolle – es muss nur schnell gehen.
- Der Besteller möchte unbedingt die Tracking-ID des Spediteurs (Hinweis: die Ware soll abgefangen werden).
- Ungewöhnlich hohe Bestellmengen oder Bestellwerte.
- Der Kunde möchte Ihnen keine Telefonnummer mitteilen, oder ist nie telefonisch erreichbar.

Grundsätzlich trägt der Händler im Fernabsatzbereich das Risiko, wenn ein Karteninhaber seine Zahlung bestreitet (s. g. Chargeback). Der Kunde hat ein Reklamationsrecht von bis zu 210 Tagen. Sofern es sich z. B. um eine gestohlene Karte handelte und Sie hierdurch Opfer eines Kartenmissbrauches geworden sind, wird Ihnen der Zahlbetrag zurückbelastet.

Fragen Sie die CCV-Kartenprüfnummer ab!

Sie befindet sich auf der Kartenrückseite und ist i.d.R. dreistellig. Mit der Beantwortung dieser Frage erhöht sich die Wahrscheinlichkeit, dass Ihr Gegenüber der rechtmäßige Kartenbesitzer ist.

Setzen Sie das Sicherheitsverfahren 3D-Secure ein!

Der Handel im Internet verläuft anonym. Das heißt: Sie als Händler wissen nicht, wer der Kunde ist, der einen Kauf durch die Angabe einer Kreditkartennummer beglichen hat. Mit der 3D-Secure-Technologie Verified by VISA und MasterCard Secure-Code schützen Sie sich als Online-Händler vor dem Missbrauch von Kreditkarten oder falsch angegebenen Kartennummern. Zur Zahlungsfreigabe gibt der Kunde je nach freigeschaltetem Verfahren seiner kartenherausgebenden Bank ein persönliches Passwort ein, oder er erhält zur Freigabe der Transaktion eine TAN-Nummer auf sein privates Handy. Dies dient Ihnen als Nachweis eines autorisierten Einkaufs und ist vergleichbar mit einer Unterschrift des Kunden.

Wird eine Transaktion unter 3D-Secure-Bedingungen durchgeführt, genießen Sie als Händler eine weitgehende Zahlungsabsicherung für Kartenumsätze. **Weitere Informationen zu 3D-Secure finden Sie auf unserer Website!**

First Cash Solution GmbH, Okenstr. 7, D-77652 Offenburg,
Telefon: +49 (0) 7805 91696 0, Fax: +49 (0) 7805 91696 197,
mail@1cs.de, www.1cs.de

Die Zertifizierung für PCI DSS ist bei der Akzeptanz von Kreditkarten obligatorisch.

Der Sicherheitsstandard für die Aufbewahrung und Weiterverarbeitung sensibler Kartendaten schützt alle am Zahlungsprozess beteiligten Parteien wirksam vor Betrug. Sobald Sie Kreditkarten in Ihrem Unternehmen akzeptieren, sind Sie dazu verpflichtet, sich zertifizieren zu lassen. Um eine einheitliche Vorgehensweise bei der Umsetzung dieser Sicherheitsanforderungen zu ermöglichen, haben sich die Kreditkartenorganisationen Visa, MasterCard, American Express, Discover und JCB auf einen gemeinsamen Sicherheitsstandard geeinigt, den „Payment Card Industry (PCI) Data Security Standard (DSS)“ (aktuelle Version: 3.1, Stand April 2015).

PCI DSS umfasst sowohl technische als auch organisatorische Maßnahmen. Die Einhaltung dieser zwölf Anforderungen ist von allen Akzeptanzstellen und Service Providern sicherzustellen und gegebenenfalls nachzuweisen:

1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
2. Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
3. Schutz gespeicherter Karteninhaberdaten
4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
5. Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen
6. Entwicklung und Wartung sicherer Systeme und Anwendungen
7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf
8. Zugriff auf Systemkomponenten identifizieren und authentifizieren
9. Physischen Zugriff auf Karteninhaberdaten beschränken
10. Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
11. Regelmäßiges Testen der Sicherheitssysteme und -prozesse
12. Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal

Jetzt zertifizieren!

Die First Cash Solution stellt Ihnen einen komfortablen und unkomplizierten Service zur Verfügung. Auf www.pci.1cs.de registrieren Sie sich und werden dann durch den kompletten Zertifizierungsprozess geleitet.
Ausführliche Informationen zu PCI DSS finden Sie auf unserer Website www.1cs.de.

Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)

Wenn Sie als Händler mit sensiblen Zahlungsdaten in Berührung kommen - dies ist insbesondere dann der Fall, wenn Sie oder Ihr IT-Dienstleister Kreditkartendaten mit Zahlungsanwendungen verarbeiten und damit in den Anwendungsbereich des SAQ C des PCI-DSS fallen-, ist die Einhaltung der MaSI-Vorgaben sicherzustellen. Hierzu können eventuell weitere Sicherheitsmaßnahmen in der von Ihnen eingesetzten IT-Infrastruktur notwendig sein.

Auf unserer Website www.1cs.de finden Sie eine Hilfestellung, damit Sie Ihren Pflichten nachkommen können.

Falls Sie weitere Fragen zum Thema MaSI haben, erhalten Sie ergänzende Informationen auf der Internet-Seite der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) www.bafin.de.

First Cash Solution GmbH, Okenstr. 7, D-77652 Offenburg,
Telefon: +49 (0) 7805 91696 0, Fax: +49 (0) 7805 91696 197,
mail@1cs.de, www.1cs.de