TeleCash from fiserv.

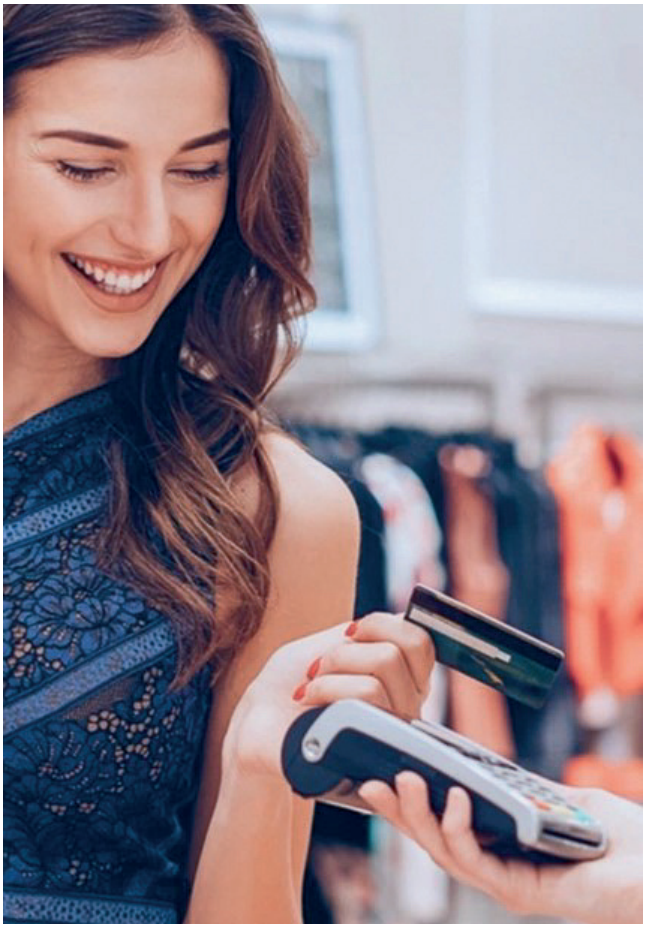
Kartenakzeptanz – so flexibel wie Ihre Kunden

Alles aus einer Hand!

Willkommen in der Welt der Kartenakzeptanz

Kartenakzeptanz – so flexibel wie Ihre Kunden.

TeleCash from Fiserv ist mit mehr als 250.000 Terminal-IDs und 100.000 Kunden einer der größten Netzbetreiber und führenden Dienstleister für den kartengestützten Zahlungsverkehr in Deutschland. Neben Terminals, Netzbetrieb und E-Commerce-Lösungen bieten wir Ihnen als First Data GmbH konzerneigene Acquiringlösungen unter der Marke TeleCash from Fiserv für die Akzeptanz von internationalen Debit- und Kreditkarten in Deutschland, Österreich, der Schweiz und weiteren europäischen Ländern an.
Und das alles aus einer Hand!



Kartenzahlung ist Bargeld weit überlegen.

Mit Ihrer Entscheidung für die Akzeptanz von Kartenzahlungen bieten Sie einer stetig wachsenden Kundengruppe eine bequeme und unkomplizierte Möglichkeit an, Ihre Angebote zu nutzen. Aber natürlich profitieren auch Sie von einer Menge gewinnbringender Vorteile.

Steigerung des Umsatzes

Sie erschließen sich neue Zielgruppen. Kartenzahler neigen zu Spontankäufen und geben darüber hinaus mehr Geld aus als Barzahler, wie internationale Studien belegen. Auf der ganzen Welt erfüllen sich Kartenzahler aller Nationalitäten jeden Tag ihre großen und kleinen Wünsche – sie kaufen Geschenke, bestellen Waren im Internet, verreisen, gehen essen, buchen Hotels, und – ab sofort sind Sie ein Teil dieser Welt und profitieren von der Kaufkraft dieser Kunden.

Erhöhung der Sicherheit

Der Umstieg auf Kartenzahlung bedeutet für Sie eine Erhöhung der Sicherheit. Denn mit der Reduktion des Bargeldes in Ihrer Kasse wird zugleich auch das Diebstahl-, Unterschlagungs-, und Falschgeldrisiko minimiert.

Sicherheit im E-Commerce

Im Fernabsatz ist die Kartenzahlung bei Nutzung der entsprechenden Sicherheitstechnologien die sicherste und schnellste Methode für Sie, Zahlungen Ihrer nationalen und internationalen Kunden entgegenzunehmen. Wenn Sie hier wirklich auf Nummer sicher gehen möchten, haben wir mit unserem Internet Payment Gateway (IPG) die passende Lösung für Sie.
Sprechen Sie uns einfach an.

Senkung der Kosten

Die Kosten für die Kartenakzeptanz sind zu jedem Zeitpunkt überschaubar, nachvollziehbar und im Vergleich zur Bargeldabwicklung gering. Mit dem Umstieg auf Kartenakzeptanz optimieren Sie auf jeden Fall Ihre Kassiervorgänge, denn sie werden wesentlich unkomplizierter und effizienter. Weniger Bargeld bedeutet für Sie auch weniger Aufwand bei der Bargeldabwicklung: Zeit- und kostenintensive Tätigkeiten wie die Herausgabe von Wechselgeld, Geld zählen beim Kassenabschluss, sichere Verwahrung des Geldes über Nacht sowie Ein- und Auszahlungen bei Ihrer Bank werden drastisch reduziert.

Schnellere Abwicklung

Kartenzahlungen lassen sich schnell und bequem durchführen. In der Regel dauern sie nur wenige Sekunden und sind somit um ein Vielfaches schneller als Zahlungen mit anderen Zahlungsmitteln. Sie können damit im gleichen Zeitraum mehr Zahlungen abwickeln und reduzieren so die Wartezeit Ihrer Kunden an der Kasse. Darüber hinaus zahlt Ihr Kunde immer passend – denn mühseliges Kleingeldzählen entfällt.

Mehr Kundenservice

Die meisten Kunden erwarten heute, dass sie bequem mit Karte bezahlen können. Wenn Sie diese Erwartung erfüllen, haben Sie zufriedene Kunden, die natürlich viel lieber bei Ihnen einkaufen, als dort, wo man diesen Service nicht bietet. Kartenakzeptanz ist der Schlüssel zu Ihrem geschäftlichen Erfolg. Denn Sie bieten Ihren Kunden damit größtmögliche Flexibilität und werden darüber hinaus attraktiv für ein modernes und internationales Publikum.

Wie Sie sehen, haben Sie mit der Akzeptanz von Kartenzahlungen die richtige Entscheidung getroffen.

Debitkarten

Debitkarten sind in der Regel direkt mit einem Girokonto verbunden, von dem bei einer bargeldlosen Zahlung oder Bargeldabhebung der entsprechende Betrag innerhalb weniger Tage abgebucht wird.

Kreditinstitute kombinieren in der Regel verschiedene Verfahren auf einer Debitkarte, um deren Flexibilität beim Bezahlen zu erhöhen. Eine Kombination ist zum Beispiel girocard mit Debit Mastercard/Visa Debit. Mit Karten mit der girocard-Funktion in Deutschland ist auch das elektronische Lastschriftverfahren möglich. Für Händler wird es immer wichtiger, neben der girocard am POS auch die Akzeptanz von Debit Mastercard und VISA Debit anzubieten, da es mittlerweile vermehrt Karten gibt, die ausschließlich mit diesen Bezahlverfahren ausgestattet sind.

Maestro, Debit Mastercard

Maestro ist eines der weltweit führenden Debitkarten-Systeme. Händler profitieren bei Autorisierung der Zahlung mittels Karte und PIN von der „Zahlungsgarantie" des Karten-Herausgebers.

Die Debit Mastercard ist das Debitprodukt von Mastercard, das neben dem stationären Handel auch im E-Commerce zum Einsatz kommen kann. Die Debit Mastercard wird zunehmend von Banken ausgegeben und spielt damit eine wichtige Rolle in der Produktfamilie von Mastercard. Karten, die neben dem Maestro bzw. Debit Mastercard Logo das Kontaktlos-Symbol aufweisen, ermöglichen zudem das kontaktlose Bezahlen.

V PAY und VISA Debit

V PAY ist die eigens für Europa konzipierte Chip- und PIN-basierte Debitkarte von VISA, die Händlern bei Autorisierung der Zahlung eine „Zahlungsgarantie" bietet und auch Karteninhabern durch die moderne EMV-Chiptechnologie eine hohe Sicherheit gewährt. Beim Bezahlvorgang liest das Terminal die IBAN/BIC aus dem Magnetstreifen bzw. dem Chip und der Karteninhaber erteilt mit seiner Unterschrift eine Einwilligung zum Lastschrifteinzug von seinem Konto.
Die VISA Debitkarte ist das neue Debitprodukt von VISA, das neben dem stationären Handel auch im E-Commerce zum Einsatz kommen kann. Die VISA Debitkarte wird zunehmend von Banken ausgegeben und spielt damit eine wichtige Rolle in der Produktfamilie von VISA.
Karten, die neben dem V PAY bzw. VISA Debit Logo das Kontaktlos-Symbol aufweisen, ermöglichen zudem das kontaktlose Bezahlen.

Elektronisches Lastschriftverfahren (ELV)

Dies ist die für Akzeptanten bislang kostengünstige Alternative zum girocard- Verfahren in Deutschland. Beim Bezahlvorgang liest das Terminal die IBAN/BIC aus dem Magnetstreifen bzw. dem Chip und der Karteninhaber erteilt mit seiner Unterschrift eine Einwilligung zum Lastschrifteinzug von seinem Konto.

girocard

Das girocard-Symbol wurde 2007 von der Deutschen Kreditwirtschaft als Akzeptanzzeichen eingeführt, um die internationale Akzeptanz deutscher Debitkarten im SEPA-Raum zu erleichtern. Es tritt damit die Nachfolge des bis dahin für das deutsche Debit Zahlungssystem verwandte electronic cash Zeichens an. Händler profitieren bei Autorisierung der Zahlung mittels Karte und PIN von der „Zahlungsgarantie" des Kartenherausgebers. Der Karteninhaber kann in der Regel Beträge bis 50 Euro kontaktlos ohne PIN bezahlen. Bei Beträgen darüber muss der Zahlvorgang per PIN oder mittels biometrischer Merkmale in Verbindung mit digitalen Karten auf dem Smartphone (CDCVM) autorisiert werden.

Kreditkarten

Die meisten Kreditkarten sind weltweit einsetzbar und erlauben die Bezahlung von Waren und Dienstleistungen sowohl im stationären Geschäft als auch im Online-Shop. Der Begriff „Kreditkarte“ wird im internationalen Umfeld für unterschiedliche Bezahlmodelle benutzt.

Im deutschsprachigen Raum steht „Kreditkarte“ für die Möglichkeit einzukaufen, ohne dass der Zahlbetrag bereits wenige Tage später vom Konto abgebucht wird. Der Karteninhaber erhält meist monatlich eine Abrechnung über seine Ausgaben und bezahlt den Abrechnungsbetrag im Anschluss an den Kreditkartenausgeber.

Als Herausgeber von Kreditkarten fungieren oft Banken, die hierfür entsprechend von den Kreditkartenorganisationen lizensiert sind, z. B. Mastercard und VISA. Es gibt aber auch Kartenorganisationen, die ihre Karten ohne die Zwischenschaltung einer Bank oder eines anderen Unternehmens direkt an den Nutzer ausgeben. Dieses Modell trifft auf Diners Club und American Express zu.

Mit den gängigen Kreditkarten kann der Karteninhaber bis zu bestimmten Betragsgrenzen kontaktlos ohne Unterschrift bezahlen. In Deutschland und Österreich liegt dieser Betrag bei bis zu 50 Euro. Bei Beträgen darüber muss der Zahlvorgang per PIN oder Unterschrift bestätigt werden.

Mastercard

Mastercard ist mit Akzeptanzstellen in mehr als 200 Ländern eine der führenden Kreditkarten. Allein in Deutschland gibt es über 17 Millionen Karteninhaber, die ihre Karte am Point of Sale sowie im E-Commerce und im Versandhandel einsetzen können. Für zusätzliche Sicherheit im OnlineHandel sorgt der Sicherheitsstandard „Mastercard Identity Check™“.

Discover

Discover Card ist eine Kreditkarte, die überwiegend in den USA ausgegeben und von über 50 Millionen Karteninhabern genutzt wird. Händler in Deutschland, die Discover Card akzeptieren, profitieren speziell von diesen internationalen Kunden.

VISA

VISA ist mit Akzeptanzstellen in mehr als 200 Ländern und über 17 Millionen Karteninhabern vertreten. Inhaber können mit ihrer VISA-Karte direkt am Point of Sale, im Internet oder im Versandhandel bezahlen. Für zusätzliche Sicherheit im Online-Handel sorgt der Sicherheitsstandard „VISA Secure®“.

VISA Electron

VISA Electron ist eine reine Online-Karte. Da bei dieser Karte die Hochprägung fehlt, kann sie nur an elektronischen Terminals eingesetzt werden, die über Online-Transaktionen abrechnen. Der Karteninhaber legitimiert sich über die Eingabe der PIN oder mit seiner Unterschrift. VISA Electron ist auch im E-Commerce einsetzbar, jedoch nicht für den Versandhandel über Post oder Telefon.

Diners Club

Auch die Inhaber von Diners Club Kreditkarten profitieren von einem unbegrenzten Einsatz ohne festes Ausgabelimit. Die Kunden der ältesten Kreditkarte verfügen über eine überdurchschnittlich hohe Kaufkraft. Diners Club International gehört zum Discover-Network. Zu diesem Netzwerk gehört auch die US-amerikanische Discover-Karte.

JCB

JCB ist eine im asiatischen Raum weit verbreitete Kreditkarte. Rund 140 Millionen Karten werden von ca. 37 Millionen Akzeptanzstellen in ca. 190 Ländern angenommen. Karten von JCB sind in Japan und den USA, aber vor allem in Korea, China, Taiwan, Thailand und Singapur üblich. In Europa empfiehlt sich die Akzeptanz von JCB vor allem in Regionen mit hohem Reiseaufkommen aus diesen Ländern.

American Express

Über 100 Millionen zahlungskräftige Geschäftsleute und Touristen zahlen weltweit mit einer Kreditkarte von American Express. Dabei schätzen sie vor allem, dass ihre Einkäufe nicht durch ein festes Ausgabelimit beschränkt sind. American Express Kunden setzen ihre Karte außer zum Begleichen von Reise- und Bewirtungskosten gerne für spontane Einkäufe ein und geben dabei im Durchschnitt mehr aus als Inhaber anderer Kreditkarten.

UnionPay

Die einzige chinesische Kreditkarte, die auch in der Türkei, Japan und Russland ausgegeben wird, ist mit ca. 9 Milliarden Exemplaren die weltweit mit Abstand meist emittierte Karte. Entsprechend relevant sind die Karten für Handel, Gastronomie und Reisebranche.

Mobile Wallets – der neue Standard fürs Bezahlen

Das verstärkte Hygienebewusstsein und die veränderten Gewohnheiten seit Beginn der Pandemie haben gezeigt, dass kontaktlose Zahlungen stark zunehmen. Die mobilen Payment-Lösungen Apple Pay und Google Pay gehören z. B. in Deutschland zu den beliebtesten kontaktlosen Bezahlmethoden für 18- bis 29-Jährige.

Auch im E-Commerce ermöglichen Google Pay und Apple Pay einen vereinfachten Bezahlprozess. Der simple Check-out verstärkt die Kundenbindung und schafft die Basis für mehr Verkäufe.

Sicherheit am Beispiel von Apple Pay:

Basis der Zahlung mit Apple Pay ist eine hinterlegte Kredit- oder Debitkarte, die entsprechenden Kartendaten werden weder direkt auf dem Apple-Gerät gespeichert noch übertragen. Stattdessen wird der hinterlegten Zahlkarte ein sogenannter Token zugewiesen und auf dem Chip gesichert – und nur dieser Token wird bei einer Transaktion übertragen. Der Kunde authentifiziert sich dann zusätzlich auf seinem iPhone oder seiner Apple Watch per Fingerabdruck und sorgt damit für hohe Sicherheit – für Kunden und Händler gleichermaßen.

Dynamic Currency Conversion (DCC) – Dynamische Währungsumwandlung

Mit der dynamischen Währungsumwandlung DCC fühlen sich Ihre ausländischen Kunden wie zu Hause, denn sie können mit ihrer Kreditkarte gleich in der Heimatwährung bezahlen. Das bedeutet mehr Transparenz und viele Vorteile für Ihre Kunden und für Sie.

Service

Wenn Sie häufig Kunden aus bestimmten Nicht-Euro-Ländern zu Gast in Ihrem Geschäft oder Hotel haben, können Sie ihnen mit DCC, der Dynamic Currency Conversion, einen besonderen Service anbieten: das Bezahlen in der Heimatwährung.

Ablauf

Beim Bezahlen mit VISA oder Mastercard Kreditkarten erkennt Ihr Terminal anhand der Kreditkartennummer das Herkunftsland der Karte und die Währung des Kontos und rechnet den Euro-Betrag automatisch in die Landeswährung des Kunden um. Beide Beträge, der Kurs und die Wechselgebühren werden sowohl auf dem Display des Terminals als auch auf den Zahlungsbelegen ausgewiesen. Die Gutschrift auf Ihrem Konto erfolgt wie gewohnt in Euro.

Die Voraussetzungen

Um DCC anbieten zu können, benötigen Sie ein DCC-fähiges Terminal und einen Kartenakzeptanzvertrag für VISA und Mastercard, der um eine entsprechende Vereinbarung ergänzt wird.

Für wen eignet sich DCC?

DCC ist ideal für alle Händler und Dienstleister, die Kreditkarten akzeptieren und regelmäßiges Kundenaufkommen aus dem Ausland haben – zum Beispiel:

- Flughafen- und Bahnhofshops
- Händler für Luxusgüter
- Autovermietungen
- Hotels und Restaurants
- Händler und Dienstleister im Tourismusgeschäft
- Geschäfte in Grenznähe

Alle Vorteile im Überblick

Für Händler:

- Umsatzbeteiligung - Sie erhalten eine Vergütung für jede DCC Transaktion
- Gutschrift in Euro
- Kundenbindung durch mehr Service

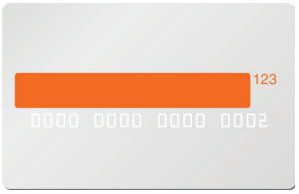
Für Karteninhaber:

- Der angezeigte Betrag ist der endgültige Kaufbetrag
- Tagesaktuelle und marktgerechte Kurse
- Einfachere Spesenabrechnung für Geschäftsreisende
- Keine zusätzlichen Wechselkursgebühren

Die typischen Sicherheitsmerkmale von Kreditkarten

Mastercard

- Die Kreditkartennummer beginnt mit einer „5“, hat 16 Stellen und ist hochgeprägt.
- Die vier klein gedruckten Ziffern unterhalb der individuellen Kartennummer müssen identisch mit den ersten 4 Ziffern der sechzehnstelligen Kartennummer sein.
- Karten für kontaktloses Bezahlen enthalten das Kontaktlos-Symbol.
- Auf dem Unterschriftsfeld auf der Rückseite muss im Hintergrund durchlaufend diagonal „Mastercard“ abgebildet sein.
- Am rechten Rand des Unterschriftsfeldes, hinter der Kartennummer, ist eine 3-stellige Kartenprüfnummer angegeben.



VISA

- Die Kreditkartennummer beginnt mit einer „4“, hat in der Regel 16 Stellen und ist hochgeprägt.
- Die vier klein gedruckten Ziffern unter- oder oberhalb der individuellen Kartennummer müssen identisch mit den ersten vier Ziffern der Kartennummer sein.
- Karten für kontaktloses Bezahlen enthalten das Kontaktlos-Symbol.
- Am rechten Rand des Unterschriftsfeldes, hinter der Kartennummer, ist eine dreistellige Kartenprüfnummer angegeben.

Allgemeine Merkmale Vorderseite:

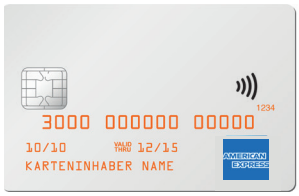
- Kartennummer und Karteninhabername, in der Regel hochgeprägt
- Logo des jeweiligen Kartenprodukts und gegebenenfalls Hologramm
- Ablaufdatum bzw. Gültigkeitszeitraum
- In der Regel EMV-Chip

Allgemeine Merkmale Rückseite:

- Unterschriftsstreifen
- Kartenprüfnummer, in der Regel auf der Rückseite

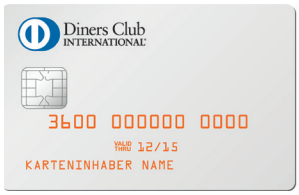
American Express

- Das American Express Logo ist auf der Vorderseite aufgedruckt.
- Die Kreditkartennummer beginnt mit einer „3“, hat 15 Stellen und ist hochgeprägt.
- Die Kartenprüfnummer hat vier Stellen und befindet sich auf der Vorderseite, rechts oberhalb der Kreditkartennummer.
- Auf der Vorderseite steht das Jahr, in dem der Karteninhaber seine Mitgliedschaft bei American Express erworben hat.



Diners Club

- Das Diners Club Logo ist auf der Vorderseite aufgedruckt.
- Die Kreditkartennummer beginnt mit einer „36“, hat 14 Stellen und ist hochgeprägt.
- Auf dem Unterschriftsfeld befinden sich u. a. die dreistellige Kartenprüfnummer und die Diners Club Grafik.



Discover

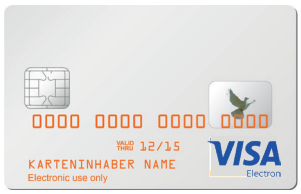
- Das Discover Logo ist entweder auf der Vorder- oder auf der Rückseite aufgedruckt.
- Die Kreditkartennummer beginnt mit 6011, 6400 oder 6500, hat 16 Stellen und ist hochgeprägt.
- Auf geprägten Karten befindet sich ein geprägtes „D".
- Auf dem Unterschriftsfeld befinden sich die letzten vier Ziffern der Kreditkartennummer.
- Rechts neben dem Unterschriftsfeld ist die dreistellige Kartenprüfnummer angegeben

UnionPay

- Die Kreditkartennummer ist 16-stellig und beginnt in der Regel mit 62.
- Die dreistellige Kartenprüfnummer steht rechts im Unterschriftsfeld.

VISA Electron

- Das VISA Electron Logo befindet sich immer entweder auf der Vorder- oder Rückseite. Zudem können das Tauben-Hologramm und das VISA Logo abgebildet sein.
- Der Aufdruck „Electronic use only" (nur für elektronischen Gebrauch) auf der Kartenvorderseite weist darauf hin, dass Electron-Karten nur in Verbindung mit elektronischer Autorisierung verwendet werden dürfen. Dieser Hinweis kann auch in anderen Sprachen erscheinen.
- Das Unterschriftsfeld kann auf der Kartenvorder- oder rückseite stehen. Es ist fortlaufend mit dem Wort „Electron" in blau, rot und gelb bedruckt.



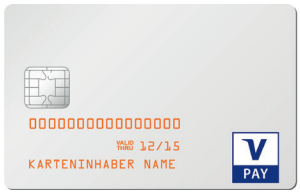
Die typischen Sicherheitsmerkmale von internationalen Debitkarten

Maestro, Debit Mastercard

- Auf der Vorderseite ist das blau-rote Maestro Logo oder das Mastercard Logo mit dem Hinweis Debit aufgedruckt, gegebenenfalls in Verbindung mit anderen Logos, wie zum Beispiel girocard.
- Der Karteninhaber kann seine Zahlung nur durch Eingabe seiner PIN autorisieren; eine Zahlung per Unterschrift ist nicht möglich.
- Auf der Karte ist der Name des Karteninhabers angegeben.

V PAY, VISA Debit

- Auf der Vorderseite ist das V PAY Logo oder das VISA Logo mit dem Hinweis Debit aufgedruckt, gegebenenfalls in Verbindung mit anderen Logos, wie zum Beispiel girocard.
- Die Karte ist mit einem Chip ausgestattet.
- Der Karteninhaber kann seine Zahlung nur durch Eingabe seiner PIN autorisieren; eine Zahlung per Unterschrift ist nicht möglich.
- Auf der Karte ist der Name des Karteninhabers angegeben.



Grundsätzliche Anforderungen an die Datensicherheit

Der sichere Umgang mit vertraulichen Kundendaten ist heute in der öffentlichen Wahrnehmung zu einem sehr wichtigen Thema geworden. Wenn ein Kunde bei Ihnen mit Karte bezahlt, stellt er Ihnen besonders sensible persönliche Daten zur Verfügung. Um diese vor dem Zugriff unberechtigter Dritter zu schützen, ist es daher wichtig, die einschlägigen Bestimmungen der geltenden Datenschutzgesetze sowie des Teledienstegesetzes unbedingt zu beachten.

Darüber hinaus sind im Kartengeschäft spezielle Sicherheitsvorschriften beim Umgang mit Karten- und Transaktionsdaten zu berücksichtigen.

Diese speziellen Regelungen tragen die Bezeichnung „Payment Card Industry Data Security Standard (PCI DSS)". Sie wurden von den führenden Kreditkartenunternehmen Mastercard, VISA, JCB, American Express und Discover gemeinsam aufgestellt, um die Integrität der Zahlungssysteme dauerhaft zu schützen. Im PCI DSS werden Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von Karteninformationen definiert, die maßgeblich zur Missbrauchsbekämpfung und Betrugsvorbeugung beitragen und von allen Teilnehmern beachtet werden müssen.

Als kleine Hilfestellung haben wir für Sie nachfolgend eine kurze Zusammenfassung der wesentlichen Bestandteile des PCI DSS zusammengestellt. Weiterführende Informationen finden Sie auch unter www.pcisecuritystandards.org. Bitte machen Sie sich, auch zu Ihrer eigenen Absicherung, ausreichend mit den Sicherheitsvorschriften vertraut. Sie schützen damit Ihre, wie auch die Reputation aller bei der Durchführung von Kartenzahlungen beteiligten Organisationen und schaffen das grundlegende Vertrauen der Karteninhaber.

Wann sind Sie an die PCI DSS-Vorgaben gebunden?

Der PCI DSS ist für jede einzelne kartengestützte Zahlung anzuwenden. Alle Unternehmen, die Kartendaten speichern, verarbeiten und/oder übermitteln, unterliegen diesen Sicherheitsvorschriften. Sobald Sie Kartendaten auf Ihren eigenen Systemen entgegennehmen, z. B. zur dauerhaften Speicherung, zur kurzfristigen Verarbeitung oder zur Weiterleitung an einen Service-Provider, sind Sie von den Anforderungen betroffen.

Sie sind nur dann von der Verpflichtung zur Einhaltung der Sicherheitsvorgaben befreit, wenn Sie zu keinem Zeitpunkt Kartendaten auf Ihren eigenen Systemen entgegennehmen, speichern und/oder verarbeiten, z. B. wenn Sie sich für den Zahlungsvorgang auf die gesicherte Domain eines externen Bezahldienstleisters bedienen, und Ihre Kunden für den Zahlungsvorgang auf die gesicherte Domain eines zertifizierten Payment Gateways geleitet werden, das die Zahlung außerhalb Ihrer Rechnerumgebung abwickelt.

Wir bestehen auf die Umsetzung der PCI DSS-Anforderungen bei allen Händlern. Stellen Sie daher unbedingt sicher, dass die einschlägigen Vorgaben der Kartenorganisationen von Ihnen und Ihren beteiligten Dienstleistern jederzeit eingehalten werden und dass die sichere Verarbeitung von sensiblen Karten- und Transaktionsdaten gewährleistet ist.

Bitte beachten Sie, dass Ihnen im Falle einer Kompromittierung von Kartendaten in Ihrem Geschäft Reputationsschäden für Sie und die Kartenorganisationen entstehen können. Zudem drohen erhebliche Schadensersatzforderungen durch die Kartenorganisationen – in Form von Untersuchungskosten und Strafen.

Welche Vorgaben macht der PCI DSS?

Der PCI DSS umfasst zurzeit 12 Kapitel. Nachfolgend finden Sie eine kurze Übersicht über die in den Kapiteln beschriebenen Anforderungen:

1. Installation und regelmäßige Aktualisierung einer Firewall zum Schutz von Karten- und Transaktionsdaten
2. Regelmäßige Änderung der Systempasswörter oder anderer Sicherheitseinstellungen, insbesondere keine Verwendung der vom Lieferanten/Hersteller vorgegebenen Initialpasswörter
3. Vermeidung der unnötigen Speicherung von Karten- und Transaktionsdaten; sofern diese unerlässlich ist, muss ein adäquater Schutz gewährleistet sein
4. Verschlüsselte Übertragung von Karten- und Transaktionsdaten in offenen Netzwerken
5. Verwendung und regelmäßige Aktualisierung von Antivirenprogrammen
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen
7. Beschränkung des Datenzugriffs auf Karten- und Transaktionsdaten nach dem Grundsatz „Kenntnis nur wenn nötig"
8. Zuteilung einer eindeutigen Benutzerkennung für jede Person mit Zugang zum Computersystem
9. Restriktive Vergabe von Berechtigungen zum Zugriff auf sensible Karten- und Transaktionsdaten
10. Protokollierung und Überwachung aller Zugriffe auf Netzwerkressourcen sowie auf Karten- und Transaktionsdaten
11. Regelmäßige Überprüfung von Sicherheitssystemen und Prozessabläufen
12. Festlegung unternehmensweiter Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner

Welche Nachweispflichten bestehen für Sie hinsichtlich der Einhaltung der PCI DSS-Vorgaben?

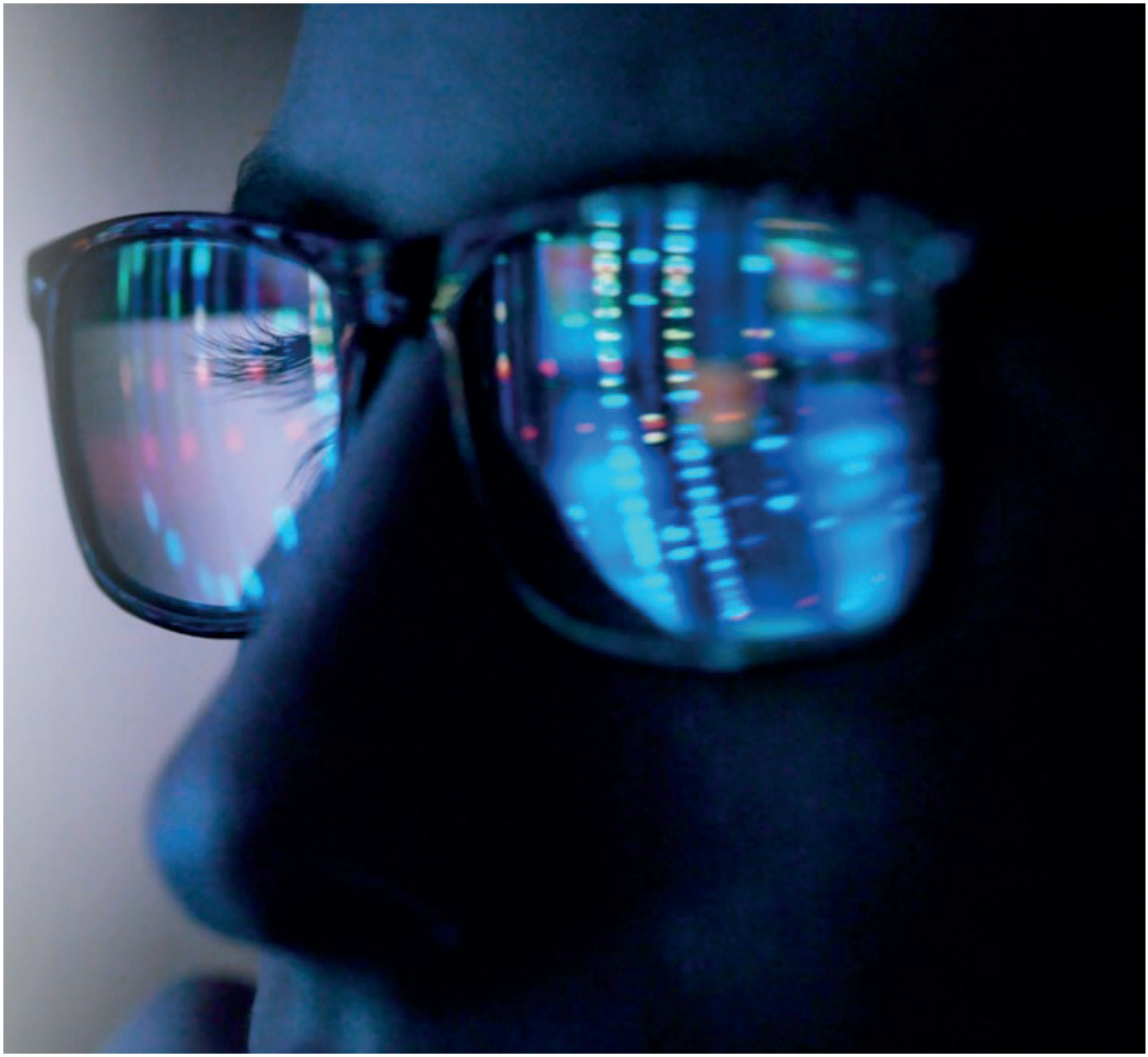
Die Sicherheitsvorgaben gelten als eingehalten, wenn alle Punkte der 12 Kapitel aus dem PCI DSS-Regelwerk umgesetzt und nachweislich eingehalten werden. Für alle Händler ist die Erbringung des Nachweises der Umsetzung der PCI DSS-Standards zwingend erforderlich. In Abhängigkeit vom Umfang der jährlichen Kartentransaktionen müssen Händler unterschiedliche interne und externe Prüfungen (Zertifizierungen) durchführen bzw. durchführen lassen.

Wir helfen Ihnen gerne weiter.

Das PCI DSS-Portal führt Sie durch den gesamten Prozess.

Sollten Sie darüber hinaus weitere Informationen zu Ihrer PCI DSS-Compliance haben, stehen wir Ihnen gerne montags bis freitags von 09:00 bis 18:00 Uhr zur Verfügung:

Deutschland:	+49 6172 8693000
Österreich:	+43 720 880306



Was ist zu tun?

Um die Compliance mit den PCI DSS-Vorgaben sicherzustellen, behalten wir uns – je nach Unternehmensgröße und Vertriebskanal – die Durchführung von regelmäßigen Befragungen bzw. Prüfungen mit entsprechender Zertifizierung vor, gegebenenfalls mit Unterstützung von hierauf spezialisierten Partnern.

Wir empfehlen Ihnen folgende Vorgehensweise:

- Machen Sie sich auf den entsprechenden Informationsseiten der Kartenprodukte mit den PCI DSS-Vorgaben vertraut.
- Speichern Sie Kartendaten nur, wenn es zwingend erforderlich ist. Insbesondere im E-Commerce nutzen Sie die gesicherten Seiten eines Dienstleisters, der PCI Level 1 zertifiziert ist. Lassen Sie sich die Zertifizierung nachweisen. Unser Internet Payment Gateway (IPG) entspricht diesen Vorgaben.
- Schulen Sie Ihr Personal und setzen Sie die Sicherheitsvorschriften in Ihrem Unternehmen um.
- Bereiten Sie die zu treffenden Maßnahmen für den Zertifizierungsprozess vor und führen Sie sie durch.
- Stellen Sie sicher, dass der PCI DSS auch nach der Zertifizierung eingehalten wird.
- Beheben Sie identifizierte Sicherheitslücken oder Schwachstellen schnellstmöglich.
- Erneuern Sie Ihr PCI DSS-Zertifikat in den vorgegebenen Abständen und lassen Sie uns dieses regelmäßig zukommen.

Für weitere Fragen im Zusammenhang mit dem Zertifizierungsprozess stehen wir gerne zur Verfügung.

www.mastercard.de

www.visa.de

www.americanexpress.com

www.dinersclub.de

www.jcbcard.com

www.unionpay.com

Hinweise zum sicheren Umgang mit Kartendaten

Aufbewahrung von Kartendaten

Speichern Sie nur jenen Teil der Kartendaten, der für die Geschäftsabwicklung zwingend erforderlich ist. Gestattet ist die Speicherung von Kartennummer, Karteninhabername und Verfallsdatum. Unter keinen Umständen dürfen nach der Autorisierung der Transaktion vollständige Datensätze des Magnetstreifens oder des Chips der eingesetzten Karten sowie die Kartenprüfnummern gespeichert werden.

Alle Karten- und Transaktionsdaten, die von Kassensystemen oder anderen IT-Systemen gespeichert werden, sind gemäß PCI DSS ausreichend zu verschlüsseln und dürfen nur auf Servern oder anderen Medien gespeichert werden, die nicht direkt mit dem Internet verbunden sind.

Bewahren Sie alle Unterlagen und Datenträger, die Karten- und Transaktionsdaten enthalten (z. B. Autorisierungsprotokolle, Transaktionsberichte, Leistungsbelege, Kundenverträge), nur so lange wie unbedingt nötig auf. Alle vom Karteninhaber erhobenen und gespeicherten Daten dürfen ausschließlich zum Zwecke der Vertragserfüllung genutzt werden und sind gegen den Zugriff unberechtigter Dritter zu sichern sowie in einer sicheren Umgebung aufzubewahren (z. B. im Tresor).

Sobald die Kartendaten nicht mehr benötigt werden, hat eine ordnungsgemäße Vernichtung der Daten/Unterlagen zu erfolgen (gesetzliche Aufbewahrungspflichten bleiben hiervon unberührt). Die Vernichtung hat so zu erfolgen, dass eine Rekonstruktion der Karten- und Transaktionsdaten nicht mehr möglich ist.

Darstellung von Kartendaten

Kartennummern dürfen grundsätzlich nur anonymisiert angezeigt bzw. ausgedruckt werden, um ein Ausspähen von Kartendaten zu verhindern. Kartendaten gelten als ausreichend anonymisiert, wenn mit Ausnahme der ersten sechs und der letzten vier Ziffern der Kartennummer alle Ziffern unkenntlich gemacht („maskiert“) wurden, z. B. 5232 11XX XXXX 2222.

Übertragung von Kartendaten

Grundsätzlich dürfen nur ausreichend verschlüsselte Kartendaten elektronisch übertragen werden. Dies ist beim Einsatz von zugelassenen POS-Geräten und Payment Gateways gewährleistet, wie zum Beispiel bei unseren POS-Terminals oder unserem Internet Payment Gateway (IPG).

Sollten solche Systeme im Einzelfall nicht eingesetzt werden, ist vor der Nutzung eine entsprechende Regelung mit uns erforderlich.

Verarbeitung von Kartendaten durch Dienstleister

Für den Fall, dass Sie sich für die Abwicklung von Kartenzahlungen eines Drittdienstleisters bedienen, sind Sie dennoch zur Sicherstellung der Einhaltung der PCI DSS-Vorgaben verpflichtet. Bitte achten Sie daher bei der Auswahl dieses Partners auf eine entsprechende PCI DSS-Zertifizierung und benennen Sie uns den Partner vorab.

Meldung eines Sicherheitszwischenfalls

Sollten unbefugte Dritte auf Karten- und/oder Transaktionsdaten zugreifen bzw. zugegriffen haben, informieren Sie uns bitte unverzüglich.

Nur bei umgehender Meldung kann das Schadensrisiko durch Einleitung sofortiger Sicherheitsmaßnahmen für alle Beteiligten minimiert werden.

Reklamationen vermeiden

Wie bei jedem Geschäft gibt es auch bei Kartenzahlungen ein paar Dinge, die Sie beachten sollten, um einen reibungslosen Ablauf sicherzustellen. Damit es nicht zu nachträglichen Reklamationen der Karteninhaber kommt, sollten Sie die folgenden Anregungen beachten. Bitte bedenken Sie dabei, dass Reklamationen für Sie mit finanziellen Risiken verbunden sein können. Viele Karteninhaberreklamationen können Sie schon im Vorfeld vermeiden, wenn Sie die in unseren Geschäftsbedingungen beschriebenen Verfahrensweisen und Genehmigungsverfahren einhalten. Schulen Sie unbedingt Ihre Mitarbeiter, damit auch diese mit dem richtigen Verhalten zur Vermeidung von Reklamationen und ungültigen Transaktionen beitragen.

Die häufigsten Reklamationen

Der Karteninhaber erkennt den Umsatz nicht an.

Möglicherweise kann der Karteninhaber den Umsatz auf Basis der auf der Karteninhaberabrechnung aufgedruckten Händlerinformationen nicht eindeutig zuordnen.

Hier können Sie vorbeugen, indem Sie dafür sorgen, dass der Kunde den Kartenumsatz auf seiner Karteninhaberabrechnung eindeutig nachvollziehen kann. Stellen Sie sicher, dass der Name Ihres Geschäftes sowie die entsprechende Händlerniederlassung korrekt und eindeutig auf der Kartenabrechnung erscheinen.

Wir empfehlen:

Bitte bewahren Sie die Umsatzunterlagen als Nachweis für einen eventuellen Reklamationsfall immer sorgfältig auf.

Im Präsenzgeschäft gilt:

Vergleichen Sie stets die Unterschrift auf dem Leistungsbeleg mit der auf der Karte. Abweichende Unterschriften können zu Rückbelastungen führen. Bei Kartenumsätzen, die mit Karte und PIN erfolgen, ersetzt die PIN-Eingabe die Unterschrift.

Der Umsatz wurde dem Karteninhaber mehrfach belastet.

Wahrscheinlich wurde der Umsatz aus Versehen mehrfach bei uns zur Abrechnung eingereicht.

Das passiert dann, wenn Chip oder Magnetstreifen der Karte wiederholt gelesen werden. Bitte führen Sie die Karte nur dann erneut ins Terminal ein, wenn Sie von diesem dazu aufgefordert werden. Sollten Sie in Ausnahmefällen die Einreichung der Umsätze auf nicht elektronischem Wege vornehmen, achten Sie bitte darauf, dass die einzelnen Umsätze nicht mehrfach aufgeführt werden.

Im E-Commerce:

Das kann unter Umständen passieren, wenn die Kartendaten mehrfach in das Payment Gateway eingegeben werden. Sollten Sie in Ausnahmefällen die Einreichung der Umsätze auf nicht elektronischem Wege vornehmen, achten Sie bitte darauf, dass die einzelnen Umsätze nicht mehrfach aufgeführt werden.

Der Kunde hat die Ware/Dienstleistung (noch) nicht erhalten.

Möglicherweise wurde der Umsatz zur Abrechnung bei uns eingereicht, bevor die Ware versandt wurde.

Ihr Kunde sieht auf seiner Kartenabrechnung den Umsatz, obwohl er die entsprechende Leistung hierfür noch nicht erhalten hat. Dies kann zu Reklamationen führen, die leicht vermeidbar sind.

Wir empfehlen:

Reichen Sie die Transaktion erst nach Leistungserbringung, z. B. nach dem Warenversand, ein und bewahren Sie einen eventuellen Liefernachweis gut auf.

Wie Sie Ihre Risiken minimieren können

Lassen Sie jeden Umsatz autorisieren.

Sie erhöhen die Sicherheit, wenn Sie jeden Kartenumsatz von uns genehmigen lassen.

Eine Umsatzautorisierung reduziert das Reklamationsrisiko, da hierbei durch den Kartenherausgeber geprüft wird, ob die Karte gültig ist, keine Kartensperre vorliegt, und der Karteninhaber über genügend finanzielle Mittel verfügt, um den Kauf zu tätigen. Grundsätzlich ist deshalb jeder Umsatz zu autorisieren. Jedoch bedeutet eine Autorisierung noch keine Zahlungsgarantie. Falls Sie eine Ablehnung auf Ihre Autorisierungsanfrage erhalten, sollten Sie die Transaktion nicht durchführen. Nicht genehmigte Umsätze können zu Reklamationen führen – mit hohen finanziellen Risiken für Sie.

Schnelles Handeln lohnt sich.

Reklamiert Ihr Kunde die Ware oder Dienstleistung, sollten Sie sich schnell und direkt mit ihm in Verbindung setzen.

Werden Reklamationen sofort bearbeitet, ist der Kunde zufrieden und Sie können unnötige Rückbelastungen und die hiermit für Sie verbundenen Kosten vermeiden. Es empfiehlt sich, Gutschriften so schnell wie möglich vorzunehmen. Werden Gutschriften nicht zeitnah auf dem Kundenkonto verbucht, kann dies zu einer Reklamation und ggf. Rückbelastung des Umsatzes führen.

Im Falle einer Rückbelastung.

Richtet der Karteninhaber eine Reklamation an seine kartenausgebende Bank, setzen wir uns direkt mit Ihnen in Verbindung. In der Regel werden Sie von uns aufgefordert, einen Nachweis für den fraglichen Kartenumsatz sowie ggf. weitere die Transaktion betreffende Informationen zur Verfügung zu stellen. Bitte beachten Sie, dass wir bei der Bearbeitung von Reklamationen an vorgegebene Fristen der Kartenorganisationen gebunden sind. Damit wir die Reklamation in Ihrem Sinne klären können, lassen Sie uns bitte die angeforderten Unterlagen innerhalb des von uns genannten Zeitrahmens zukommen.

Was Sie im Fernabsatzgeschäft beachten müssen

Holen Sie die richtigen Informationen beim Besteller ein.

Bei der Abwicklung von Fernabsatztransaktionen sollten Sie stets darauf achten, dass Sie mindestens die folgenden Daten vom Besteller abfragen:

- Kartennummer
- Name des Karteninhabers (wie auf der Karte angegeben)
- Ablaufdatum der Karte
- Kartenprüfnummer
- Wohn-, Rechnungs- und/oder Lieferadresse

Zusätzlich zu den oben genannten Daten sollten Sie sich folgende Informationen notieren:

- Kontaktdetails des Karteninhabers (z. B. Telefonnummer oder E-Mail Adresse)
- Tag und Uhrzeit der Bestellung

Fragen Sie den Besteller immer nach der Kartenprüfnummer!

Die Kartenprüfnummer ist ein wichtiger Bestandteil der Kartendaten und dient der Absicherung vor Kartenmissbrauch bei Fernabsatzgeschäften. Über die Kartenprüfnummer wird im Rahmen der Autorisierung geprüft, ob dem Besteller die Karte vorliegt und somit die missbräuchliche Verwendung von Kartendaten ausgeschlossen werden kann. Die Nummer darf unter keinen Umständen in Ihren Systemen gespeichert werden.

Unterstützen Sie die modernen Authentifizierungsverfahren im E-Commerce.

Die von den Kartenorganisationen eingeführten 3D Secure-Verfahren (z. B. Verified by Visa®, Mastercard SecureCode™, American Express SafeKey®, J/Secure™ von JCB) erhöhen die Sicherheit unter anderem bei E-Commerce-Geschäften beträchtlich. Sie ermöglichen über eine Passwortabfrage die Authentifizierung des Karteninhabers während des Bezahlvorgangs. Durch Unterstützung dieses Verfahrens minimieren Sie Ihre Reklamations- und Ausfallrisiken enorm. Zu Ihrer eigenen Sicherheit schreiben wir daher die Nutzung dieser Verfahren im E-Commerce grundsätzlich vor.

Falls Sie ein Payment Gateway nutzen, achten Sie darauf, dass Ihr Anbieter die vorgenannten Anforderungen unterstützt. Auch hier sind Sie auf der sicheren Seite mit unserem Internet Payment Gateway (IPG). Sprechen Sie uns einfach an.

Bewahren Sie die Transaktionsunterlagen gut auf!

Bei schriftlichen Bestellungen, die Sie per Post oder Fax erhalten, ist die Einholung der Unterschrift des Bestellers auf dem Bestellformular erforderlich. Bitte bewahren Sie die zur Transaktion zugehörigen Unterlagen gut auf, um bei einem eventuellen Reklamationsfall einen entsprechenden Nachweis erbringen zu können. Außerdem empfiehlt es sich, Nachweise über die erbrachte Leistung oder Warenlieferung aufzubewahren.

Sicherheitsverfahren im Fernabsatz

Im Präsenzgeschäft, d. h. bei der Kartenakzeptanz direkt am Point of Sale, besteht für den Händler die Möglichkeit, die Echtheit der Karte und die Berechtigung des Karteninhabers unmittelbar zu überprüfen. Händler, die ihre Waren oder Dienstleistungen im Fernabsatzgeschäft – dem sogenannten „Card Not Present-Umfeld" – anbieten, stehen hingegen vor dem Problem, dass weder Karte noch Karteninhaber präsent sind. Die Prüfung auf eventuellen Missbrauch wird dadurch deutlich erschwert, was gleichzeitig auch bedeutet, dass Fernabsatzhändler ein höheres Risiko aus Missbrauchs- und Chargeback-Tatbeständen zu tragen haben.

Um die Zahlungsabwicklung bei Fernabsatzgeschäften sicher zu gestalten und die Risiken zu minimieren, haben die internationalen Kartenorganisationen Sicherheitsverfahren entwickelt, mit denen sich missbräuchliche Karteneinsätze im Internet oder bei telefonischen oder postalischen Bestellungen (sog. MoTo-Geschäfte) reduzieren oder gar verhindern lassen.

Der Einsatz dieser Sicherheitsverfahren hat für Sie als Händler nicht nur den Vorteil, dass Sie sich vor möglichen finanziellen Schäden aus Rückbelastungen schützen. Gleichzeitig belegen auch Studien der Kartenorganisationen, dass gesicherte Transaktionen durchschnittlich wesentlich höhere Umsatzbeträge aufweisen. Außerdem stärken Sie zusätzlich das Vertrauen Ihrer Kunden in Ihr Unternehmen: Denn ein Kunde, der sich beim Einsatz seiner Karte in Ihrem Shop sicher fühlt und dessen Zahlung problemlos abgewickelt wird, bezieht sicherlich nicht nur einmal Waren oder Dienstleistungen von Ihnen.

3D Secure-Verfahren

Händlern, die die 3D Secure-Technologie unterstützen, wird seitens der Kartenorganisationen eine sogenannte Haftungsumkehr („Liability Shift") eingeräumt. Diese minimiert das Rückbelastungsrisiko für Internethändler wesentlich. Denn für Chargebacks, bei denen der Karteninhaber angibt, die Transaktion nicht zu kennen oder nicht getätigt zu haben (diese machen fast 80 % aller Rückbelastungen aus), haftet bis auf wenige Ausnahmen das kartenausgebende Kreditinstitut – unabhängig davon, ob sich der Karteninhaber während des Bezahlvorgangs tatsächlich authentifiziert hat oder nicht.

Um 3D Secure-gesicherte Transaktionen abwickeln zu können, muss ein sogenanntes „Merchant Plug-In" (MPI) in Ihr Online-Zahlsystem integriert werden. Sprechen Sie diesbezüglich einfach Ihren Payment Service Provider an.

Dieser kann Ihnen die entsprechende Software mit Sicherheit bereitstellen. Sie suchen eine sichere Lösung? Gerne empfehlen wir Ihnen unser Internet Payment Gateway (IPG). Sprechen Sie uns einfach an.

Kartenprüfnummer

Die Kartenprüfnummer ist eine dreistellige, teilweise auch vierstellige Nummer, die als Sicherheitsmerkmal auf der Rückseite und bei manchen Anbietern auch auf der Vorderseite der Karte angebracht ist. Mit der Abfrage der Kartenprüfnummer während des Bezahlvorgangs im Internet, aber auch bei telefonischen oder schriftlichen Bestellungen (MoTo), lässt sich überprüfen, ob der Besteller im Besitz der echten Karte ist.

Während der Autorisierungsanfrage wird die vom Kunden angegebene Kartenprüfnummer mit der im System des kartenausgebenden Instituts verschlüsselt hinterlegten Ziffer abgeglichen. Stimmen beide Nummern überein, so kann davon ausgegangen werden, dass die Karte dem Kunden tatsächlich physisch vorliegt. Damit lässt sich die Nutzung missbräuchlich abgegriffener Kartennummern durch unbefugte Dritte verhindern. Studien haben erwiesen, dass sich die Betrugsraten allein durch die Abfrage der Kartenprüfnummer um bis zu 70 % reduzieren lassen.

Was ist zu tun?

Integrieren Sie einfach die Kartenprüfnummer als ein Abfragemerkmal in Ihr Zahlsystem. Dies ist ohne großen technischen Aufwand möglich.

Bitte beachten Sie jedoch, dass die Kartenprüfnummer nach der Autorisierung von Ihnen auf keinen Fall gespeichert und/oder aufbewahrt werden darf – weder papierhaft, noch elektronisch!

Fallen Sie nicht auf Betrüger herein

Jedes Jahr werden Milliarden von Kartentransaktionen getätigt. Obwohl zweifellos die Mehrheit dieser Kartenumsätze durch die rechtmäßigen Karteninhaber erfolgt, kommt es leider hin und wieder vor, dass Karten auch für betrügerische Handlungen missbraucht werden. Sie können aktiv zur Bekämpfung und der Vermeidung von Missbrauch beitragen – achten Sie auf die eindeutigen Zeichen.

Verdächtige Anzeichen im Präsenzgeschäft

Verhält sich Ihr Kunde auffällig?

Auffällig unruhiges und hektisches Verhalten sowie der Versuch, Sie abzulenken, oder die Absicht, Sie zur schnellen Bearbeitung zu bewegen, können Zeichen dafür sein, dass die Karte betrügerisch genutzt wird – hier ist Vorsicht angesagt! Wenn Sie sich unsicher sind, ob es sich bei dem Kunden um den rechtmäßigen Karteninhaber handelt, lassen Sie sich einfach ein gültiges Legitimationsdokument wie Personalausweis, Reisepass oder Führerschein zeigen.

Wirkt die Karte echt?

Wirkt die Karte echt oder können Sie Anzeichen für eine Manipulation der Karte erkennen? Ein verschwommener Druck, eine unebene Prägung oder ein verwischter Unterschriftenstreifen sind erste Hinweise für eine gefälschte oder manipulierte Karte.

Sie erkennen gefälschte Karten auch daran, dass typische Hologramme gar nicht erst vorhanden oder die UV-Sicherheitselemente unter einem UV-Prüfgerät nicht zu erkennen sind. Prüfen Sie bei der Kartenvorlage, ob alle Merkmale ordnungsgemäß vorhanden sind.

Stimmen die Kartendaten mit den Daten auf dem Leistungsbeleg überein?

Kartennummer und Gültigkeitsdatum auf der Karte müssen mit den auf dem Leistungsbeleg gedruckten Daten identisch sein. Ist das nicht der Fall, liegt eindeutig eine Kartenmanipulation vor. Vergleichen Sie die Daten deshalb bitte noch bevor Sie die Karte an den Kunden zurückgeben und lehnen Sie bei Abweichungen die Transaktion ab. Nach Möglichkeit kontaktieren Sie uns bitte in einem solchen Fall.

Unterschrift geprüft?

Geben Sie die Karte erst wieder zurück, wenn Sie die Unterschriften auf dem Beleg und auf der Karte auf ihre Übereinstimmung hin geprüft haben. Bei Kartenumsätzen, die mit Karte und PIN erfolgen, ersetzt die PIN-Eingabe die Unterschrift.

Verdächtige Anzeichen im Fernabsatzgeschäft

Erhöhte Wachsamkeit bei Fernabsatzgeschäften

Im Präsenzgeschäft besteht die Möglichkeit, die Echtheit der Karte und die Berechtigung des Karteninhabers unmittelbar zu überprüfen. Händler, die ihre Waren oder Dienstleistungen im Fernabsatzgeschäft anbieten, stehen hingegen vor dem Problem, dass weder die Karte noch der Karteninhaber präsent sind. Dadurch wird die Prüfung auf eventuellen Missbrauch erschwert. Fernabsatz, also E-Commerce und MoTo, erfordern deshalb erhöhte Wachsamkeit.

Achten Sie auf eindeutige Zeichen

Es gibt eine Reihe von Hinweisen, die auf einen möglichen Betrug hindeuten. In diesen Fällen sollten Sie besonders aufmerksam sein:

- mit derselben Karte werden innerhalb von kurzen Zeitabständen viele Transaktionen getätigt
- Sie verzeichnen plötzlich eine stark erhöhte Transaktionsfrequenz, die nicht durch Ihr übliches Geschäft oder eine Marketingaktion Ihrerseits begründet ist
- plötzliches Auftreten auffällig hoher Transaktionsbeträge
- mit einer Karte werden große Mengen identischer, hochwertiger Waren bestellt
- Waren sollen an die gleiche Adresse gesendet, jedoch mit verschiedenen Karten bezahlt werden oder in mehreren Vorgängen gekauft werden
- Waren sollen an eine Lieferadresse versendet werden, die nicht Ihrem erwarteten Markt entspricht (z. B. bezogen auf die sprachliche Ausrichtung Ihrer Webseite)
- der Besteller äußert den Wunsch, den Rechnungsbetrag auf mehrere Karten zu verteilen

Wir empfehlen:

Setzen Sie Höchstbeträge fest, die mit einzelnen Karten innerhalb eines Tages bezahlt werden dürfen. Kontrollieren Sie, ob es Bestellungen gibt, die mit mehreren und aufeinander folgenden Kartennummern aufgegeben wurden, und überwachen Sie Kartenumsätze nach Kartennummer, Transaktionsanzahl und Transaktionsvolumen. In unserem Internet Payment Gateway (IPG) lassen sich eine Reihe von solchen Parametern voreinstellen.

Merkwürdiges Verhalten bei telefonischen Bestellungen

Vorsicht bei Kunden, die zögern oder unsicher erscheinen, wenn sie im Rahmen der Bestellung nach persönlichen Angaben gefragt werden. Dies ist häufig ein Indiz dafür, dass die Person eine falsche Identität benutzt. Kunden, die scheinbar wahllose Bestellungen aufgeben („Ich nehm' von jedem eins!") stellen ein potenzielles Risiko dar, da die Waren wahrscheinlich nicht für den eigenen Bedarf, sondern für den Wiederverkauf gedacht sind.

Eilzustellungen

Eilzustellungen müssen nicht zwingend einen betrügerischen Hintergrund haben. Sie können aber charakteristisch sein für die Betrugsart „hit and run", bei der leicht verkäufliche Waren erworben werden, um sie schnell weiterzuverkaufen. Bei Eilzustellungen ist es daher sinnvoll zu prüfen, ob Sie diesen Kunden bereits kennen.

Verdächtige Anschriften

Bestellungen, bei denen die Rechnungsanschrift von der Lieferanschrift abweicht, können potenziell risikobehaftet sein, insbesondere wenn der Versand an ein Postfach oder eine Büroadresse oder an eine exotische Anschrift erfolgen soll. Bewerten Sie das Risiko einer Transaktion auf Basis der bestellten Ware, des Warenwertes und der angegebenen Lieferanschrift.

Unser Tipp:

Protokollieren Sie Fälle, bei denen es in der Vergangenheit zu Problemen kam. Bei erneuten Bestellungen mit derselben Karte oder einer identischen Lieferanschrift ist das Auftreten erneuter Probleme überdurchschnittlich hoch.

Das Wichtigste über Rückbelastungen

Beleganforderungen durch das kartenausgebende Kreditinstitut

Hat ein Karteninhaber Rückfragen zu einem Kartenumsatz, so beauftragt er in den meisten Fällen sein kartenausgebendes Kreditinstitut mit der Klärung der Angelegenheit. Das Kreditinstitut wendet sich dann mit der Bitte um einen Nachweis für den fraglichen Kartenumsatz („Retrieval Request") an die entsprechende Abrechnungsstelle – d. h., an uns.

Damit wir den Fall in Ihrem Sinne klären können, benötigen wir Ihre Unterstützung. Da Sie alle vom Kunden unterschriebenen Leistungsbelege aufbewahren, werden Sie im Falle einer Rückfrage eines Karteninhabers von uns kontaktiert. Sie werden dann von uns aufgefordert, uns den entsprechenden Beleg sowie ggf. weitere, die Kartentransaktion betreffende Unterlagen zukommen zu lassen. Sobald uns die benötigten Unterlagen zugegangen sind, leiten wir diese an das Kreditinstitut bzw. an den Karteninhaber weiter.

Bitte beachten Sie, dass die angeforderten Nachweise gemäß den Regularien der internationalen Kartenorganisationen innerhalb einer vorgegebenen Frist beim kartenausgebenden Kreditinstitut eingereicht werden müssen!

Wird diese Frist nicht eingehalten, so wird Ihnen der Kartenumsatz zurückbelastet. Bitte lassen Sie uns deshalb die angefragten Unterlagen – auch in Ihrem eigenen Interesse – innerhalb des von uns genannten Zeitfensters zukommen. Bei hohen Umsatzbeträgen ist es ratsam, die Nachweise per Einschreiben zu versenden.

Rückbelastungen von Kartenumsätzen

Reklamiert ein Karteninhaber einen Kartenumsatz, so wird die entsprechende Transaktion über das kartenausgebende Kreditinstitut an uns zurückgegeben. Sprechen keine formalen Gründe (z. B. Ablauf der Widerspruchsfrist) für eine Ablehnung der Reklamation, so sind wir gemäß den Regularien der internationalen Kartenorganisationen dazu verpflichtet, den Transaktionsbetrag dem Karteninhaber wieder gut zu schreiben.

In diesem Fall belasten wir Ihr Kundenkonto unter Rückrechnung des ursprünglich berechneten Serviceentgelts mit dem entsprechenden Betrag und informieren Sie unverzüglich über diese Rückbelastung („Chargeback").

Diesem Informationsschreiben liegt ein Fragebogen bei, den Sie bitte ausfüllen, sofern Sie Widerspruch einlegen möchten. Bitte beachten Sie auch hier, dass wir den Fall nur in Ihrem Sinne klären können, wenn Sie uns die Unterlagen innerhalb der im Schreiben angegebenen Frist zukommen lassen. Wird der Einspruch nicht innerhalb der genannten Frist eingereicht, so verfällt Ihr Anspruch auf eine erneute Gutschrift des zurückbelasteten Umsatzes.

Im Präsenzgeschäft: Bewahren Sie Leistungsbelege auf!

Bitte beachten Sie, dass es in Ihrer Verantwortung liegt, alle vom Karteninhaber unterschriebenen Leistungsbelege für eine Mindestdauer von 18 Monaten ab Transaktionsdatum aufzubewahren.

Sollten wir auf Basis der von Ihnen zur Verfügung gestellten Unterlagen feststellen, dass die Reklamation des Karteninhabers nicht gerechtfertigt ist, wird das Chargeback von uns an das kartenausgebende Kreditinstitut zurückgegeben („Reversal") und die erneute Gutschrift des Kartenumsatzes zu Ihren Gunsten veranlasst.

Reklamiert der Karteninhaber den Kartenumsatz erneut, so hat das kartenausgebende Kreditinstitut das Recht, eine erneute Rückbelastung des Kartenumsatzes zu veranlassen („Second Chargeback"), d. h., Ihr Konto kann u. U. erneut belastet werden.

Wir geben unser Bestes, um Rückbelastungen erfolgreich und dauerhaft in Ihrem Sinne zu klären. Am einfachsten schützen Sie sich allerdings selbst vor unnötigen Rückbelastungen, indem Sie Kartenumsätze nur nach den in unseren Geschäftsbedingungen beschriebenen Verfahrensweisen abwickeln.

Bitte beachten Sie, dass jedes von uns bearbeitete Chargeback Kosten für Sie verursacht! Es ist also in Ihrem Sinne, Reklamationen schon im Vorfeld zu vermeiden.

Wir empfehlen:

Mit dem Einsatz bestimmter Sicherheitsverfahren, wie z. B. der EMV-Technologie am Point of Sale oder des 3D SecureVerfahrens im E-Commerce, kann ein wirtschaftlicher Schaden für Sie schon im Vorfeld abgewendet werden. Setzen Sie als Händler diese Sicherheitsverfahren ein, so profitieren Sie bei bestimmten Kartenumsätzen von der sogenannten Haftungsumkehr („Liability Shift"), d. h., das kartenausgebende Kreditinstitut muss für die entstehenden Schäden aufkommen.

Richtlinien der Kartenorganisationen hinsichtlich des Chargeback-Aufkommens

Zum Schutz vor der missbräuchlichen Nutzung der Zahlungssysteme wurden seitens der Kartenorganisationen Grenzwerte hinsichtlich des Chargeback-Aufkommens definiert. Die Vorgaben können sich je nach Kartenorganisation unterscheiden. Bei der Einhaltung aller Sicherheitsmechanismen kollidieren Sie jedoch nicht mit diesen Vorgaben.

Bei Überschreitung der definierten Grenzwerte verhängen die Kartenorganisationen Strafzahlungen und Reportinggebühren für überhöhte Rückbelastungsquoten, die verschuldensunabhängig vom Händler, also von Ihnen zu tragen sind.

Was sonst noch wichtig ist

Bitte vergessen Sie nicht, uns über alle wichtigen Änderungen in Ihrem Geschäft zu informieren. Entsprechende Formulare finden Sie in unserem Download-Center unter www.telecash.de

Stammdatenänderungen

Insbesondere gilt das im Fall von Änderungen Ihrer Adresse oder Bankverbindung. In unserem Download-Center unter www.telecash.de liegen hierfür die erforderlichen Formulare für Sie bereit. Bitte füllen Sie diese vollständig aus und lassen Sie sie uns per Post oder Fax zukommen.
Bitte beachten Sie, dass Stammdatenänderungen zu Ihrer eigenen Sicherheit schriftlich bei uns eingereicht werden müssen.

Inhaberwechsel

Benachrichtigen Sie uns bitte rechtzeitig schriftlich darüber, wenn Sie Ihr Geschäft veräußern oder schließen werden. Bitte beachten Sie, dass Sie im Falle des Informationsversäumnisses weiterhin für alle Verpflichtungen der bestehenden Servicevereinbarung haften. Unsere Servicevereinbarung zur Akzeptanz und Abrechnung von Karten ist nicht ohne Weiteres übertragbar. Sollte der neue Geschäftsinhaber an einer Kartenakzeptanz interessiert sein, muss eine neue Servicevereinbarung mit uns abgeschlossen werden.

Änderung des Geschäftszwecks

Bitte beachten Sie, dass Ihre Angaben über Branche und angebotenes Produktsortiment bzw. Serviceleistungen entscheidender Bestandteil unserer Servicevereinbarung sind und dass es Ihnen gemäß unserer allgemeinen Bedingungen nur erlaubt ist, Kartenzahlungen für eben diese Waren und/oder Dienstleistungen entgegenzunehmen.

Bitte teilen Sie uns unverzüglich mit, wenn Sie in eine andere Geschäftsrichtung expandieren und/oder sich Ihre Produktpalette oder Dienstleistungen insoweit verändern, dass Sie nicht mehr mit dem im Serviceantrag angegebenen Geschäftszweck übereinstimmen.

Änderung oder Erweiterung der bestehenden Servicevereinbarung

Sie möchten Ihre Waren oder Dienstleistungen nachträglich über einen zusätzlichen Vertriebskanal vertreiben und Ihren Kunden dabei ebenfalls die Möglichkeit bieten, mit Karte zu zahlen? In diesem Fall beachten Sie bitte, dass der bestehende Vertrag mit uns entsprechend erweitert werden muss.

Möchten Sie eine zusätzliche Filiale eröffnen oder künftig auch Fernabsatzgeschäfte tätigen und hier bargeldlose Zahlungen akzeptieren? Bitte informieren Sie uns rechtzeitig darüber – Ihre Servicevereinbarung muss entsprechend erweitert werden. Dies gilt auch, wenn Sie bisher nur Fernabsatzgeschäfte getätigt haben und nun auch in Ihrem stationären Geschäft Karten akzeptieren möchten.

Sie möchten Ihre Kartenakzeptanz erweitern und noch weitere Kartenmarken akzeptieren? Auch hier muss die bestehende Servicevereinbarung entsprechend erweitert werden.

Wir sind für Sie da

Vertragspartnerservice

Bei allgemeinen Fragen, Anliegen oder Reklamationen wenden Sie sich bitte von Montag bis Freitag in der Zeit von 08:00 bis 18:00 Uhr an unseren Vertragspartnerservice. Bitte halten Sie Ihre Geschäftspartnernummer bereit.

Sie erreichen unseren Vertragspartnerservice unter:
Deutschland: +49 69 7933 9900
Österreich: +43 800 560001 80*

E-Mail: fde-service@fiserv.com

*kostenfrei für Anrufe aus dem lokalen Festnetz, Mobilfunk ggf. abweichend

Genehmigungsservice und Meldung eines Betrugsverdachts

Möchten Sie Transaktionen telefonisch von uns autorisieren lassen oder haben Sie einen Betrugsverdacht, dann wenden Sie sich bitte an unseren Genehmigungsservice. Er steht Ihnen 24 Stunden täglich, auch an Sonn- und Feiertagen, zur Verfügung. Bitte halten Sie Ihre Geschäftspartnernummer und die Kartendaten bereit.

Sie erreichen unseren Genehmigungsservice unter:
Deutschland: +49 69 7933 9930
Österreich: +43 800 560001 40*

E-Mail: fde-autorisierung@fiserv.com

Unsere Anschrift
First Data GmbH
Marienbader Platz 1
61348 Bad Homburg

Kontaktieren Sie uns!

Mehr Informationen:
+49 180 622558800*
info@telecash.de
www.telecash.de

+43 800 005 680**
office@fiserv.at
www.telecash.at

Fiserv, Inc. (NASDAQ: FISV) bewegt Gelder und Informationen, um die Welt, Menschen und Geschäftsprozesse am Laufen zu halten. Als einer der international führenden Anbieter von Zahlungs- und Finanztechnologien hilft das Unternehmen seinen Kunden, erstklassige Ergebnisse zu erzielen. Im Mittelpunkt stehen dabei Innovationen, die vom Account- und Issuer-Processing, über digitale Banklösungen, bis zum Acquiring-Processing, Netzbetrieb sowie Zahlungen im E-Commerce reichen.
TeleCash from Fiserv bietet seit über drei Jahrzehnten maßgeschneiderte und professionelle Lösungen für bargeldlose Zahlungen mit Karten: Am Point of Sale, im E-Commerce für Onlineshops und Apps, bis hin zu Omnichannel-Lösungen. Mit über 250.000 Terminals betreibt TeleCash heute die Bezahllösung für mehr als 100.000 Kunden in verschiedensten Branchen und Vertriebskanälen.

*unabhängig von der Dauer des Anrufes 0,20 EUR aus deutschen Festnetzen und Mobilfunknetzen
**kostenfrei für Anrufe aus dem lokalen Festnetz, Mobilfunk ggf. abweichend

First Data GmbH
Marienbader Platz 1
61348 Bad Homburg

TeleCash
from fiserv.