VECTRON

POS Acquiring

Benutzerhandbuch für Händler

Version 1.1 Januar 2024

Inhaltsverzeichnis

1. Überblick

1.1. Zweck des Dokuments

Das vorliegende Benutzerhandbuch ist eine Schulungsunterlage und eine Sammlung hilfreicher Tipps und Empfehlungen. Der Zweck des Dokuments besteht darin, wichtige Grundlagen und Informationen, etwa zur Minimierung von Kartenbetrug, zu vermitteln. Das Benutzerhandbuch sollte deshalb auch allen mit Zahlungsvorgängen betrauten Angestellten, insbesondere dem Kassenpersonal, aber auch dem Führungs- und Leitungspersonal, zur Verfügung gestellt werden und von diesen gelesen werden.

1.2. Definitionen und Abkürzungen

Im Benutzerhandbuch werden zur Beschreibung der Inhalte vereinzelt Abkürzungen und Fachbegriffe verwendet, welche nachfolgend erklärt werden.

Acquirer

(englisch *to acquire sth.*, dt. *etw. erwerben, ankaufen*)

Möchte ein Händler für seine Kunden elektronische Bezahlverfahren wie etwa Kartenzahlung anbieten, so benötigt er einen sogenannten Acquirer. Der Acquirer ist das Unternehmen, das im Namen des Händlers die jeweilige Kaufsumme über die Karten der Kunden abrechnet und die eingezogenen Beträge regelmäßig an den Händler ausbezahlt. Der Acquirer stellt dabei ein Verbindungselement zwischen dem Händler und den Kartenorganisationen wie etwa Visa und Mastercard dar und betreut die Händler als kaufmännischer Partner.

Autorisierung

Eine Autorisierung im Kontext von Kartenzahlungen ist eine Genehmigung einer Kauftransaktion durch das kartenausgebende Institut. Durch eine solche Genehmigung wird sichergestellt, dass die Kaufsumme innerhalb des Verfügungsrahmens der eingesetzten Karte liegt und diese nicht gesperrt ist. Dazu führt das Zahlungsterminal in der Regel eine elektronische und automatisierte Genehmigungsanfrage bei der kartenausgebenden Bank des Käufers durch. Der Autorisierungsprozess läuft nahezu verzögerungsfrei ab und zeigt das Ergebnis der Prüfung auf dem Zahlungsterminal an.

Chip

Der Chip auf einer Zahlungskarte hat prinzipiell dieselbe Funktion wie der Magnetstreifen, denn er ist ebenfalls ein Speicherort für die Kartennummer. Da der Chip jedoch einen integrierten Mikroprozessor für die Verschlüsselung der Kartennummer einsetzt, bietet er Karteninhabern sehr hohen Schutz gegen Datendiebstahl und Kartenfälschung.

Issuer

(englisch *to issue sth.*, dt. *etw. ausstellen, emittieren*)

Der Issuer ist das Finanz- oder Kreditinstitut, das eine Zahlungskarte ausgibt. Das kartenausgebende Institut verrechnet in diesem Zusammenhang die getätigten Umsätze mit dem jeweiligen Karteninhaber und stellt sie diesem in Rechnung. Der Issuer bietet dem Karteninhaber auch häufig mit dem Einsatz der Karte verbundene Dienstleistungen wie Reiseversicherungen oder Sammelsysteme mit Punkten - sogenannte Loyalty-Programme - an.

Kartenorganisation

Eine Kartenorganisation wie beispielsweise Visa oder Mastercard stellt ein weltweites Zahlungsnetzwerk zur Abwicklung von Kartenzahlungen zur Verfügung, über das ein Acquirer oder ein vergleichbares Finanzinstitut Kartentransaktionen abwickeln kann.

NFC

Nahfeldkommunikation (englisch **N**ear **F**ield **C**ommunication)

Methode zur drahtlosen Datenübertragung, mit der zwei elektronische Geräte innerhalb kurzer Distanz eine Kommunikation herstellen können. NFC-Chips sind heute in nahezu allen Zahlungskarten und Smartphones integriert, um kontaktloses Bezahlen zu ermöglichen.

PAN

Kartennummer (englisch **P**rimary **A**ccount **N**umber)

Die PAN bezeichnet die auf der Vorderseite von Kredit-, Debit- oder Prepaidkarten aufgedruckte 12- bis 19-stellige Kartennummer. Obwohl die

englische Bezeichnung ‚Primary Account Number' es vermuten lässt, handelt es sich bei der PAN nicht um die Kontonummer des tatsächlich mit der Karte verknüpften Bankkontos. Vielmehr dient die PAN einer eindeutigen Identifizierung der Karte inklusive des kartenausgebenden Instituts. Die Kartennummer ist entweder hochgeprägt oder auf der Karte aufgedruckt.

PCI

Payment Card Industry

Die Organisation PCI (*genauer: PCI SSC – Payment Card Industry Security Standards Council*) ist ein weltweites Forum für unterschiedliche Unternehmen und Interessensgruppen aus der Zahlungsverkehrsbranche. Der Auftrag der Organisation besteht darin, technische Sicherheitsstandards und Regelwerke für Zahlungen weltweit zu entwickeln und anzuwenden. Ein solcher Sicherheitsstandard ist der sogenannte *PCI-DSS (Payment Card Industry Data Security Standard)*, der sich auf die sichere Abwicklung von Kreditkartentransaktionen bezieht. Mitglieder des PCI Security Standards Council sind in der Regel Unternehmen, die Kartendaten speichern, verarbeiten und übertragen, einschließlich den Unternehmen für den Betrieb von Geldautomaten, POS-Terminals sowie die Ausgabe von Kredit-, Debit- und Prepaidkarten.

PIN

Geheimzahl oder Persönliche Identifikationsnummer

Eine PIN ist eine Zahlenfolge, die in der Regel nur einer Person bekannt ist und welche zur Authentifizierung dieser Person gegenüber einem elektronischen System genutzt wird. Im Kontext elektronischer Kartenzahlungen ist die PIN eine vierstellige Sicherheitsnummer, die mit einer Bezahlkarte verknüpft ist. Der Karteninhaber verwendet die PIN beispielsweise bei Auszahlungen am Geldautomaten oder beim Bezahlvorgang mit einer Karte am POS, um sich als rechtmäßiger Karteninhaber zu authentifizieren.

POS / MPOS

Verkaufsstelle / Mobile Verkaufsstelle (englisch **P**oint **o**f **S**ale, **M**obile **P**oint **o**f **S**ale)

Eine Verkaufsstelle (POS) ist eine Kasse, die sich typischerweise in einem Ladenlokal oder einer Filiale befindet, oder eine Einrichtung, an welcher Käufe und Transaktionen stattfinden können. Häufig wird der Begriff POS auch für das tatsächliche elektronische Kassensystem verwendet, einschließlich dessen Hard- und Software, Barcodescanner, Touchscreen-Anzeigen, sowie dem Belegdrucker. Eine Mobile Verkaufsstelle (MPOS) ist ein mobiles Gerät (Smartphone, Tablet), das ebenfalls die Funktionen eines klassischen POS-Terminals ausführen kann.

PSP

Zahlungsdienstleister (englisch **P**ayment **S**ervice **P**rovider)

Ein Zahlungsdienstleister ist typischerweise ein Unternehmen, das Händlern die technische Integration von unterschiedlichen Bezahlverfahren wie etwa Visa und Mastercard in deren POS-Systeme ermöglicht, indem der PSP für den Händler eine Verbindung zu den Acquirern herstellt. In der Regel führt der PSP dabei eine Partnerschaft mit einem Acquirer.

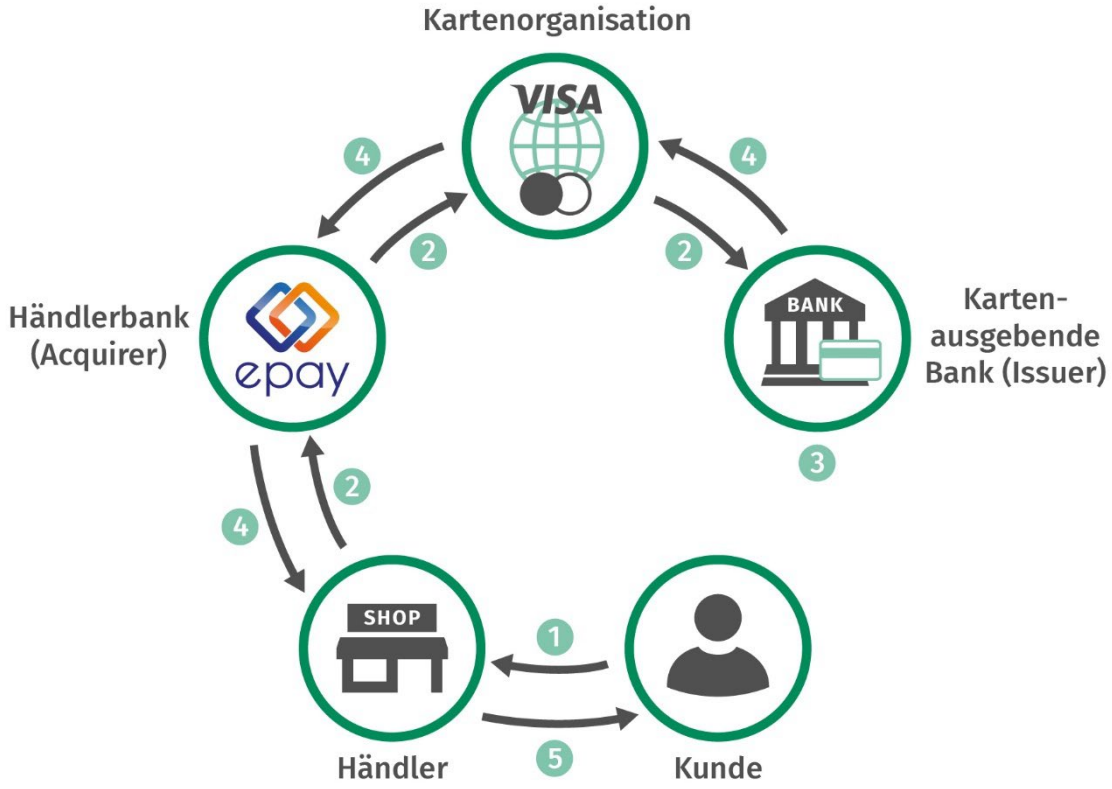
2. Kartenakzeptanz

2.1. Grundlagen der Kartenakzeptanz

Der Kartenakzeptanzprozess besteht vereinfacht dargestellt aus der **Autorisierung**, bei welcher dem kartenausgebenden Institut (Issuer) eine Anfrage zur Genehmigung der Kartenzahlung gesendet wird, und dem **Clearing-Prozess**, bei dem der Acquirer den Transaktionsbetrag über die Kartenorganisation beim Issuer einzieht und verrechnet.

2.1.1. Die Autorisierung

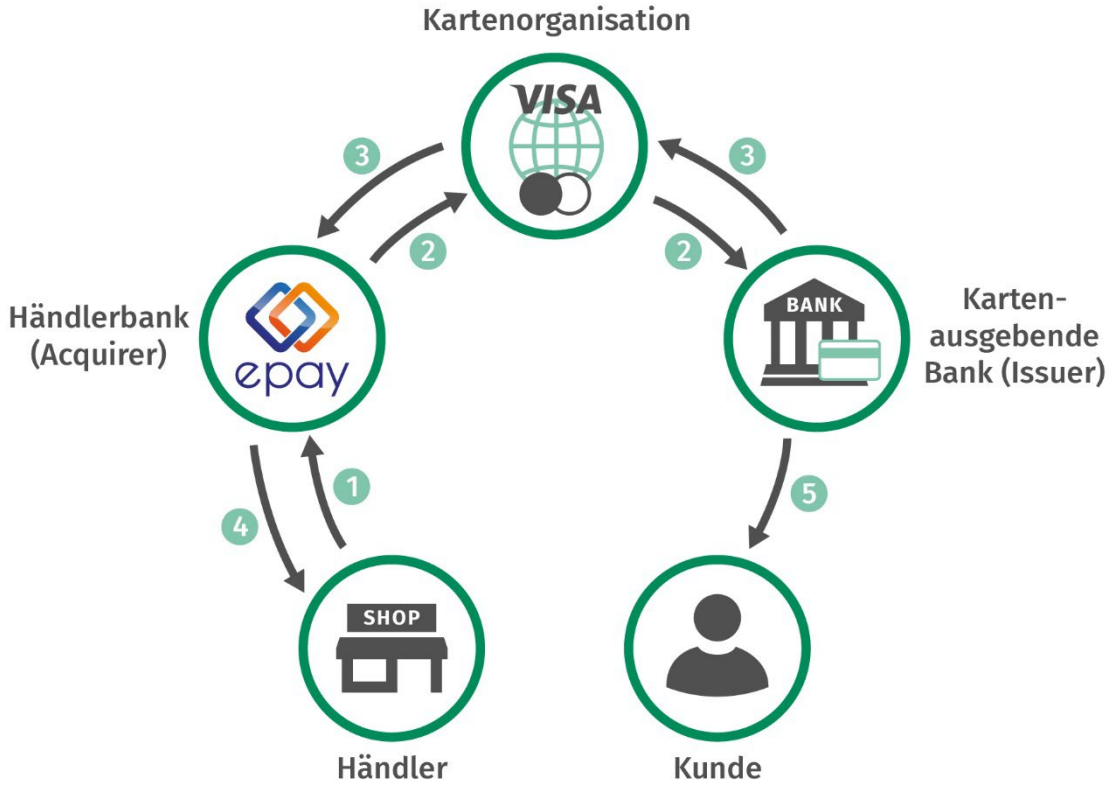
Die nachfolgende Abbildung verdeutlicht den Prozess einer Kartenautorisierung.



1. Der Kunde legt die Zahlungskarte vor. Der Händler prüft die bei ihm vorgelegte Zahlungskarte, um sicherzustellen, dass es sich um eine echte Karte handelt. Die Transaktions- und Kartendaten werden am Terminal erfasst, entweder durch Einstecken der Karte in das Lesegerät des Terminals oder bei kontaktlosem Bezahlen durch Halten der NFC-fähigen Karte an das Terminal.
2. Das Terminal übermittelt die Transaktionsdaten zum Zweck einer Autorisierung an transact, von wo aus die Daten über die jeweilige Kartenorganisation zur Prüfung an den Issuer weitergeleitet werden.
3. Es folgt eine sekundenschnelle Prüfung durch den Issuer, die entweder eine Genehmigung oder eine Ablehnung der Kartenzahlung zur Folge hat.
4. Der Issuer sendet die Antwort auf die Autorisierungsanfrage über das Netzwerk der Kartenorganisation zurück an transact, von wo aus das Ergebnis der Autorisierung an das Terminal des Händlers übermittelt wird.
5. Der Kauf wird bei erfolgreicher Autorisierung abgeschlossen.

2.1.2. Der Clearing- und Abwicklungsprozess

Während der Clearing- und Abrechnungsphase einer Kartenzahlung werden die Transaktionsdaten vom Acquirer zum Issuer übermittelt, um nun den tatsächlichen Geldtransfer zu veranlassen. Dabei wird die Transaktionssumme auf der Seite des Issuers vom Konto des Karteninhabers belastet und über die Systeme der jeweiligen Kartenorganisation zum Acquirer transferiert, der den Betrag anschließend dem Händler gutschreibt. Die nachfolgende Abbildung verdeutlicht diesen Vorgang.



1. Das Terminal führt einen Kassenschnitt durch und übermittelt die gespeicherten Transaktions- und Kartendaten an transact.
2. transact sendet die Transaktionsdaten für eine Verrechnung an die jeweilige Kartenorganisation.
3. Die Kartenorganisation belastet den jeweiligen Issuer und leitet die Transaktionssumme (abzüglich Gebühren) an den Acquirer weiter.
4. transact nimmt eine Auszahlung an den Händler vor. Der Clearing-Prozess ist damit abgeschlossen.
5. Anschließend belastet die kartenausgebende Bank das Konto des Karteninhabers mit dem Kaufbetrag.

! Wichtig

Ein ordnungsgemäßer und fristgerechter Kassenschnitt ist erforderlich, damit der Clearing- und Abwicklungsprozess gestartet werden kann. Ein nicht ausgeführter Kassenschnitt führt dazu, dass keine Auszahlung der Transaktionssummen erfolgen. Die Anleitung zur Durchführung eines Kassenschnitts finden Sie in der Betriebsanleitung Ihres Terminals.

2.2. Sichere Zahlungsabwicklung mit Karten

2.2.1. Echtheitsprüfung einer Karte

Vor einer Kartenzahlung sollte der Händler weder Zweifel an der **Echtheit und Gültigkeit einer Karte** haben noch an der Tatsache, dass der zahlende Kunde tatsächlich der **rechtmäßige Karteninhaber** ist. Sollten sich dennoch Zweifel ergeben, wird dringend empfohlen, eine Prüfung von Sicherheitselementen auf der Karte vornehmen und, soweit anwendbar, eine Legitimationsprüfung des Karteninhabers. Die nachfolgenden Punkte zeigen, welche Sicherheitsprüfungen an einer Karte vorgenommen werden können:

- Die Karte muss zum Zeitpunkt der Transaktion gültig sein. Das auf der Vorderseite aufgedruckte **Gültigkeitsdatum** darf deshalb nicht in der Vergangenheit liegen.
- Die Karte darf nicht beschädigt sein, also keine sichtbaren **Risse oder Schnitte** aufweisen.
- Sowohl der **Magnetstreifen** als auch der **Chip** dürfen **nicht überklebt oder herausgelöst** sein.
- Das **Unterschriftsfeld** auf der Rückseite der Karte darf keine Anzeichen von nachträglicher Veränderung wie etwa einer Überklebung durch ein abweichendes Unterschriftsfeld aufweisen. Erkennbar ist eine solche Veränderung beispielsweise daran, dass ein echtes Unterschriftsfeld nicht hervorsteht und häufig eine feine Sicherheitsprägung aufweist.
- Zudem darf das **Unterschriftsfeld nicht leer** sein.
- Sofern im Unterschriftsfeld auf der Rückseite der Karte eine **vierstellige Nummer** aufgedruckt ist, ist diese typischerweise identisch mit den **letzten vier Ziffern** der Kartenummer auf der Vorderseite.
- Bei Debitkarten ist die Kartennummer nicht hochgeprägt.
- Hat der Händler Zweifel an der Identität des Karteninhabers, sollte er den Karteninhaber auffordern, sich durch Vorzeigen eines Ausweisdokuments zu legitimieren. Der Händler überprüft in diesem Fall anhand des Ausweisdokuments, ob der Name auf der Karte und der Name auf dem Ausweis übereinstimmen.

! Wichtig

Wenn Ihnen oder dem Kassenpersonal sich der Verdacht aufdrängt, dass eine ihnen vorgelegte Karte gefälscht oder verfälscht ist oder dass ein Kartenmissbrauch oder ein unbefugter Karteneinsatz vorliegt, verlangen Sie von dem Karteninhaber die Vorlage eines amtlichen Lichtbildausweises und lehnen bei fehlender Übereinstimmung des Karteninhabers mit dem Ausweisinhaber die Kartenakzeptanz ab. Bitten Sie den Kunden darum, ein anderes Bezahlverfahren zu nutzen.

2.2.2. Honour-All-Cards Regel

Die Honour-All-Cards Regel (deutsch sinngemäß *„Regel zur Akzeptanz aller Kartenprodukte“*) stellt eine wichtige Grundlage für die Funktionsweise des Kartensystems dar. Die Regel stammt von den Kartenorganisationen und schreibt vor, dass ein Händler alle Kartenprodukte desselben Kartensystems (beispielsweise VISA) akzeptieren muss, unabhängig davon, um welchen Kartentyp (Kredit-, Debit-, Prepaid- oder Geschäftskarte) es sich handelt. Durch diesen Standard können sich zum einen die Kunden darauf verlassen, dass ihre Karten weltweit angenommen werden und zum anderen haben Händler die Zusicherung, dass eine Zahlung unabhängig vom Kartenprodukt ausgeführt wird.

Für Händler mit Geschäftssitz innerhalb des Europäischen Wirtschaftsraums (EWR) gilt diesbezüglich eine Besonderheit: Die EU-Verordnung 2015/751 erlaubt es Händlern mit Sitz im EWR seit 2015, von der Honour-All-Cards-Regel abzuweichen und frei zu wählen, welche Kartentypen einer Kartenorganisation sie akzeptieren wollen, solange es sich um eine Karte handelt, die innerhalb des EWR ausgegeben wurde. Für alle Karten, die nicht innerhalb des EWR ausgegeben wurden, behält die Honour-All-Cards Regel jedoch ihre Gültigkeit.

! Wichtig

Sollten Sie sich dafür entscheiden, für die innerhalb des Europäischen Wirtschaftsraums ausgestellten Karten von der Honour-All-Cards Regel abzuweichen und nicht alle Kartentypen einer Kartenorganisation zu akzeptieren, sind Sie nach der EU-Verordnung (Verordnung (EU) 2015/751 Artikel 10) verpflichtet, die Karteninhaber unmissverständlich darüber zu informieren, und zwar auf dieselbe Weise, wie Sie die Karteninhaber über die Akzeptanz anderer Karten des Kartenzahlverfahrens informieren. Diese Information ist am Geschäftseingang und an der Ladenkasse deutlich sichtbar anzuzeigen.

3. Die häufigsten Gründe für abgebrochene Zahlungen

Die nachfolgende Tabelle fasst die häufigsten Gründe zusammen, weshalb Kartenzahlungen nicht erfolgen können oder abgebrochen werden.

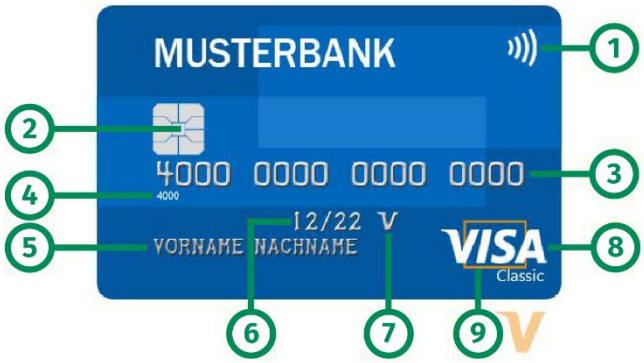
Grund für Scheitern / Abbruch der Zahlung	Lösungsvorschlag
Die Karte ist nicht lesbar	Zunächst sollte überprüft werden, ob entweder der Magnetstreifen oder der Chip der Karte verunreinigt sind. Eine Reinigung der betroffenen Stellen kann dazu führen, dass die Karte wieder lesbar ist. Sind Magnetstreifen oder Chip dagegen sichtbar beschädigt, können die Kartendaten nicht mehr über diese Speichermedien ausgelesen werden. Ist die Karte für kontaktloses Bezahlen geeignet, sollte diese Methode verwendet werden.
Die Karte ist abgelaufen	Der Karteninhaber ist darum zu bitten, mit einem anderen akzeptierten Zahlungsmittel zu bezahlen.
Der Karteninhaber kennt die PIN nicht	Der Karteninhaber ist darum zu bitten, mit einem anderen akzeptierten Zahlungsmittel zu bezahlen. Ist die Karte bereits in das Terminal eingeführt und die Authentifizierung ausgelöst worden, wird das Terminal ohne PIN-Eingabe nach einer bestimmten Zeit einen Timeout-Fehler anzeigen und den Vorgang abbrechen.
Der Karteninhaber gibt mehr als zweimal eine falsche PIN ein	Die Karte kann in diesem Fall nicht erneut zur Zahlung eingesetzt werden. Der Karteninhaber ist darum zu bitten, mit einem anderen akzeptierten Zahlungsmittel zu bezahlen.
Der Karteninhaber hält sich nicht an die Anweisungen auf dem Terminal	Der Karteninhaber muss die Anweisungen auf dem Terminal befolgen, damit die Kartenzahlung richtig verarbeitet werden kann. Besonders bei Nichteinhaltung der Anweisungen ‚Karte einschieben' und ‚Karte herausziehen' können Lesefehler die Folge sein.
Die Autorisierungsanfrage wird mit einer Ablehnung des Zahlungsvorgangs durch den Issuer beantwortet	In Folge der Ablehnung durch den Issuer wird die Transaktion automatisch abgebrochen. Der Karteninhaber nimmt seine Karte entgegen und ist über die Ablehnung zu informieren. Sofern der Karteninhaber Auskunft über die genauen Ablehnungsgründe wünscht, sollte dieser an seinen Issuer verwiesen werden (Kontaktdaten und Telefonnummer des kartenausgebenden Instituts sind i.d.R. auf der Kartenrückseite aufgedruckt).
Das POS-Terminal hat Verbindungsprobleme	Es wird empfohlen zu prüfen, ob ein zu schwaches WLAN-Signal, beschädigtes LAN-Kabel oder lose Steckverbindungen Grund für die Verbindungs-probleme sind und ob diese Mängel behoben werden können. Andernfalls steht Ihnen unser Technischer Support gerne zur Verfügung.

4. Merkmale gültiger Karten

4.1. Visa

Vorderseite

1. Kontaktlos-Symbol
2. Chip
3. Kartennummer (16-stellig) – häufig hochgeprägt
4. Ist an dieser Stelle eine vierstellige Zahl aufgedruckt, müssen diese mit den ersten vier Stellen der Kreditkartennummer übereinstimmen
5. Name des/der Karteninhabers/in – häufig hochgeprägt
6. Ablaufdatum (MM/JJ) – häufig hochgeprägt
7. Hochgeprägtes Visa-Sicherheitszeichen (optional)
8. Visa-Logo – unterschiedliche Ausrichtungen und auch eine vertikale Platzierung sind möglich
9. Fluoreszierendes Sicherheitszeichen „V“ über dem Visa-Logo, nur sichtbar unter UV-Licht (optional)



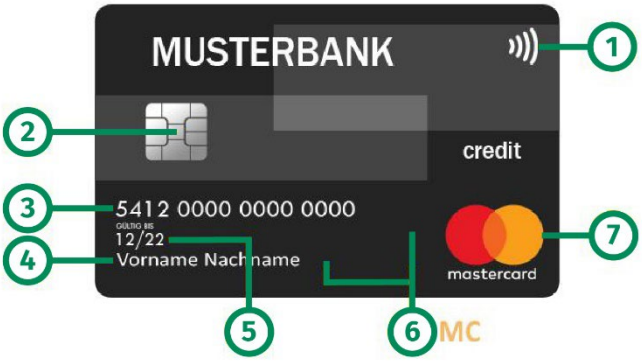
Rückseite

10. Magnetstreifen
11. Hologramm, teilweise auch als holografischer Magnetstreifen – Das Hologramm ist häufig auch auf der Vorderseite der Karte zu finden
12. Unterschriftsfeld, teilweise mit Visa-Schriftzug entweder bedruckt oder unter UV-Licht erkennbar
13. Die letzten vier Stellen der Kartennummer auf dem Unterschriftsfeld (optional)
14. Kartenprüfnummer (CVV2)

4.2. Mastercard

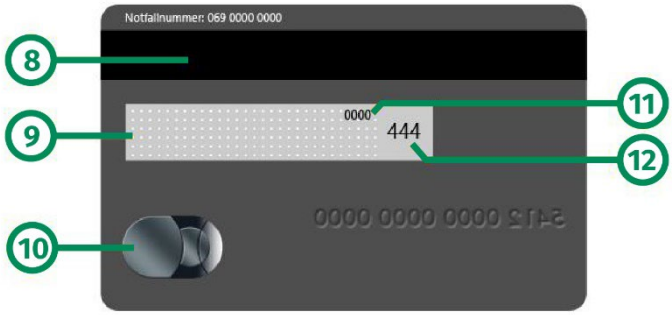
Vorderseite

1. Kontaktlos-Symbol
2. Chip
3. Kartennummer (16-stellig) – häufig hochgeprägt
4. Name des/der Karteninhabers/in – häufig hochgeprägt
5. Ablaufdatum (MM/JJ) – häufig hochgeprägt
6. Fluoreszierendes Sicherheitszeichen „MC“, nur sichtbar unter UV-Licht (optional)
7. Mastercard-Logo – unterschiedliche Ausrichtungen und auch eine vertikale Platzierung sind möglich



Rückseite

8. Magnetstreifen
9. Unterschriftsfeld, teilweise mit Mastercard-Schriftzug entweder bedruckt oder unter UV-Licht erkennbar
10. Hologramm - Häufig auch auf der Vorderseite der Karte
11. Die letzten vier Stellen der Kartennummer auf dem Unterschriftsfeld (optional)
12. Kartenprüfnummer (CVV2)



5. Häufige Methoden von Kartenmissbrauch und Betrug

Der Umgang mit Zahlungskarten und Kartendaten sollte im gesamten Unternehmen klar geregelt sein. Es liegt in der Verantwortung des Händlers, dass alle Informationen berücksichtigt und Sicherheitsregeln von allen Mitarbeitern befolgt werden, um Betrug zu minimieren.

5.1 Allgemeine Betrugsrisiken

Die Tabelle führt beispielhaft einige Betrugsgefahren auf, die sowohl von außerhalb als auch innerhalb des Unternehmens drohen.

Betrugsrisiko von außerhalb des Unternehmens	Betrugsrisiko von innerhalb des Unternehmens
• Ein Käufer gibt vor der Zahlung an, der Chip auf der Karte würde nicht funktionieren und bittet um manuelle Eingabe der Kartennummer in das Terminal • Ein Käufer bittet darum, gegen Belastung der Karte am Terminal eine Bargeldauszahlung zu erhalten und plant, der Belastung zu widersprechen • Ein Käufer verwendet wissentlich eine ungültige (abgelaufene oder gesperrte) Karte • Ein Käufer legt eine missbräuchlich angefertigte Karte vor, deren Magnetstreifen die Kartendaten einer heimlich kopierten Zahlungskarte beinhaltet	• Eine von Kunden liegen gelassene Karte wird nachträglich erneut belastet • Auf die Karten von Freunden und Familie werden Gutschriften ausgeführt und mit gefälschten Belegen (beispielsweise über einen Umtausch) gestützt • Die Karte eines Kunden wird unbemerkt durch ein zweites Lesegerät gezogen, um die Kartendaten auszuspähen (Skimming)

5.2. Skimming – Das Abgreifen von Kartendaten

Skimming (engl. für „Abschöpfen“) bezeichnet das illegale Auslesen von Kartendaten durch unbefugte Personen mit Hilfe spezieller Vorrichtungen. Durch einen solchen Späh-Angriff erlangen die Betrüger die auf dem Magnetstreifen von Karten gespeicherten Kartendaten wie etwa die PAN. Diese Daten prägen die Betrüger danach häufig auf neue Kartenrohlinge oder überschreiben damit die Magnetstreifen von gestohlenen Karten. Die zu den Karten gehörenden PINs erlangen die Betrüger oft durch separaten Einsatz versteckter Kameras oder Tastenauflagen. Solche betrügerisch erstellten Karten können anschließend für Zahlungen oder Bargeldabhebungen eingesetzt werden. Dies geschieht typischerweise im nicht-europäischen Ausland, weil dort keine Verpflichtung zur Verwendung des EMV-Chips besteht und Kartenzahlungen oft nur auf Grundlage des Magnetstreifens und der PIN erfolgen. Erst wenn der rechtmäßige Eigentümer, die nicht von ihm veranlasste Abbuchung bemerkt, wird dieser eine Rückbelastung veranlassen.

Skimming-Angriffe gibt es sowohl auf Geldautomaten als auch auf POS-Terminals. Für Angriffe auf Geldautomaten setzen die Betrüger in der Regel kleinste und gut getarnte Lesegeräte über oder in die echten Kartenleseschlitze der Originalgeräte, wodurch die Daten auf dem Magnetstreifen beim Einsetzen einer Karte durch die Fremden ausgelesen werden können. Für Angriffe auf POS-Terminals können prinzipiell dieselben Veränderungen an den Geräten vorgenommen werden wie an Geldautomaten. In zahlreichen Fällen setzen die Betrüger jedoch noch ausgefeiltere Methoden ein. Die Betrüger beschaffen sich durch Diebstahl weit verbreitete Originalgeräte und manipulieren diese intern, sodass diese von außen nicht verdächtig wirken. Um die manipulierten Geräte

anschließend bei einem Händler zum Ausspähen von Karten einzusetzen, können die Kriminellen folgendermaßen vorgehen:

- Ein Betrüger gibt sich als ein Techniker des Terminalherstellers aus und besteht darauf, einen Geräteservice am Terminal des Händlers durchzuführen.
- Mehrere Betrüger handeln gemeinschaftlich, wobei eine Person das Kassenpersonal ablenkt und die andere das POS-Terminal von der Kasse absteckt und gegen ein baugleiches, manipuliertes Gerät austauscht.
- Ist der Laden für einen kurzen Zeitraum gänzlich unbewacht, kann ein Betrüger die Geräte auch ohne Ablenkung und Tricks austauschen.

Zahlende Kunden können in einem solchen Fall nicht erkennen, ob das jeweilige POS-Terminal ordnungsgemäß funktioniert oder ob es manipuliert wurde. Die manipulierten Geräte speichern die Daten aller eingesetzten Karten sowie die eingetippten PINs auf einer zusätzlichen Speichereinheit ab. Nach einigen Tagen tauschen die Betrüger das Gerät erneut aus und haben dadurch Zugriff auf die ausgespähten Daten.

6. Sicherheitshinweise und Tipps zur Vermeidung von Betrug

Betrügerische Handlungen kommen auf verschiedenste Weise vor. Die folgenden Sicherheitshinweise ermöglichen es dem Händler und vor allem dessen Kassenpersonal, bei Zahlungsvorgängen sichere Abläufe zu etablieren, um Betrug zu minimieren.

! Wurde ein Betrug bemerkt

Haben Sie einen vermuteten oder nachweislichen Betrug erkannt, informieren Sie bitte unverzüglich transact darüber. Sie erreichen uns hierzu unter der Telefonnummer +49 89 899 643 20. Zur Einschätzung eines Betrugsfalls können unsere Spezialisten auch zusätzliche Informationen oder Dokumente bei Ihnen anfordern.

6.1. Empfehlungen für das Kassenpersonal

Gut informiertes und wachsames Kassenpersonal bildet eine sehr starke Absicherung gegen betrügerische Zahlungsvorgänge. Die nachfolgenden Abschnitte fassen die wichtigsten Kontrollen und Prüfverfahren zusammen.

6.1.1. Best Practice für den Bezahlvorgang mit Karten

1. Wir empfehlen grundsätzlich, bei Veranlassung von Kartenzahlungen auf die Anweisungen auf dem Kartenterminal zu achten und entsprechende Anweisungen zu befolgen. Insbesondere bei Autorisierungsanfragen ist auf die **Rückmeldung** (Genehmigung oder Ablehnung) auf dem POS-Terminal zu warten, bevor der Vorgang abgeschlossen werden kann.

2. Sofern bei Kartenzahlung eine Authentifizierung des Karteninhabers mittels PIN-Eingabe erfolgt, stellt dies ein relativ hohes Sicherheitsniveau dar. Die Prüfung von Sicherheitsmerkmalen der eingesetzten Karte empfehlen wir bei PIN-Eingabe nur dann, wenn sich Zweifel an der Echtheit einer Karte ergeben sollten.

3. Wird der Karteninhaber jedoch mittels einer Unterschrift authentifiziert, hat dieser den Zahlungsbeleg in Gegenwart des Händlers auf der Vorderseite zu unterzeichnen. Der Händler vergleicht danach die **Unterschrift auf dem Zahlungsbeleg** mit der **Unterschrift auf der Rückseite der Karte** und überprüft dabei, ob eine deutliche Übereinstimmung vorhanden ist.

4. Ist das **Unterschriftsfeld leer** oder es liegen **Zweifel an der Identität des Karteninhabers** vor, sollte der Kunde um Vorlage eines Legitimationsdokuments gebeten werden und ein Namensabgleich erfolgen. Handelt es sich bei dem Kunden nicht um den tatsächlichen Karteninhaber, ist die Transaktion abzulehnen oder nachträglich zu stornieren, sofern bereits erfolgt.

5. Bei Authentifizierung eines Karteninhabers mittels Unterschrift empfehlen wir zudem, die Karte auf einige Sicherheitsmerkmale zu überprüfen. Eine Auflistung möglicher Sicherheitsprüfungen ist im Abschnitt 2.2.1 (Echtheitsprüfung einer Karte) zu finden. Wir empfehlen bei einer Prüfung, den Karteninhaber lediglich darum zu bitten, die Karte gut sichtbar vorzuzeigen, jedoch nicht aus der Hand zu geben.

! Sollte die Unterschrift abweichen

Es ist nicht so ungewöhnlich, dass sich Unterschriften im Laufe der Zeit etwas verändern. Leichte Abweichungen können deshalb vorkommen. Ist jedoch die Unterschrift des Käufers auf dem Zahlungsbeleg nur sehr schwer oder gar nicht mit der Unterschrift auf der Karte in Einklang zu bringen, sollten Sie den Käufer um eine Legitimation bitten:

- Sie oder Ihr Kassenpersonal bittet den Kunden um Vorlage eines Legitimationsdokuments (in der Regel Personalausweis) oder eines anderen personalisierten Dokuments (Führerschein)
- Der Name auf der Karte wird mit dem Namen auf dem Legitimationsdokument abgeglichen
- Sind beide Namen identisch, kann die Zahlung unverändert verarbeitet werden
- Weichen der Kartenname und Name auf dem Legitimationsdokument ab, sollten Sie sowohl die veranlasste Transaktion umgehend stornieren als auch die Ware nicht übergeben oder die Dienstleistung nicht erbringen. Ihr Kassenpersonal informiert darüber den Vorgesetzten.

Daneben gelten ein paar allgemeine Sicherheitsregeln

- Der Kunde darf niemals danach gefragt werden, seine PIN bekanntzugeben
- Kunden sollten Notizen ihrer PIN niemals für andere sichtbar ablesen oder im Laden liegen lassen
- Karten sollten am POS-Terminal nicht für die Auszahlung von Bargeld akzeptiert werden
- Der Umtausch von Waren, die ursprünglich per Karte bezahlt wurden, sollte nur durch eine Erstattung des Kaufbetrags auf die ursprüngliche Karte des Kunden vorgenommen werden.

6.1.2. Tipps zur Vermeidung von Skimming

Um Skimming zu verhindern, sollte das Kassenpersonal routinemäßig darauf achten, dass sowohl das eingesetzte POS-Terminal als auch dessen Umgebung keine Anzeichen von Manipulation aufweisen:

- Das POS-Terminal weist keine sichtbaren Veränderungen auf (unveränderte Gehäuseteile, keine Aufbruchspuren oder Beschädigungen, keine aufgeklebte Tastaturauflage, keine unbekannten Anbauteile, unveränderte Anzahl und Art von Anschlusskabeln, gegebenenfalls vorhandenes Stahlkabel oder sonstige Sicherheitsvorrichtung sind unbeschädigt)

- In der Nähe des POS-Terminals sind keine versteckten Kameras angebracht (Für moderne Kameras reichen heutzutage kleinste Löcher in Kisten oder ähnlichen Objekten)

- Darüber hinaus sollten Personen mit auffälligem Verhalten an den jeweiligen Vorgesetzten gemeldet werden. Dazu zählen beispielsweise Personen, die sich im Laden aufhalten und dabei erkennbar für Sicherheitskameras oder POS-Terminals interessieren. Auch könnten mehrere Personen zusammen-gehören und versuchen, das Kassenpersonal abzulenken, um ungestörten Zugang zu einem POS-Terminal zu erhalten. Auch auffällig wäre, wenn sich eine fremde Person ohne vereinbarten Termin als Servicetechniker ausgeben und Zugang zu einem Terminal verlangen würde, ohne dass sich dieser als autorisierter Techniker ausweisen kann.

! Verdächtige Handlungen melden

Das Personal kann Skimming-Angriffe vermeiden oder zumindest reduzieren, indem es **ungewöhnliche oder verdächtige Situationen wachsam verfolgt und unverzüglich dem Vorgesetzten meldet.**

- Das Personal hat Veränderungen am POS-Terminal oder der unmittelbaren Umgebung festgestellt
- Das Personal beobachtet Personen, die sich verdächtig verhalten oder eine Straftat begehen
- Eine fremde Person gibt sich ohne vorherige Terminvereinbarung als Servicetechniker des Terminalherstellers aus und verlangt Zugriff auf ein Gerät oder eine Sicherheitskamera
- Das POS-Terminal fehlt

Wurde ein POS-Terminal möglicherweise manipuliert, bitten wir Sie um unverzügliche Benachrichtigung unseres Technischen Supports unter der Tel. +49 89 899 643 20.

Falls dem Personal verdächtige Handlungen durch fremde Personen auffallen, sollte der jeweilige Vorgesetzte über die Beobachtungen informiert werden.

6.2. Organisatorische Empfehlungen für den Händler

Neben den routinemäßigen Prüfungen durch das Kassenpersonal empfehlen wir unseren Händlern auch die Anwendung einiger allgemeiner und organisatorischer Maßnahmen, die sich zu einem wichtigen Rahmen einer wirksamen Betrugsprävention zusammenfügen.

Schulung des Personals: Der Händler sollte dafür sorgen, dass sein Personal, insbesondere das Kassenpersonal, über alle gängigen Sicherheitsanweisungen und -vorkehrungen des Händlers geschult und informiert ist. Das Personal soll vor allem einen sicheren Umgang bei der Annahme von Kartenzahlungen (siehe Abschnitt 6.1.1) verinnerlichen, mit den gängigsten Kartentypen und deren Sicherheitsmerkmalen (siehe Abschnitt 4) vertraut sein sowie auf Betrugsversuche (siehe Abschnitt 5) vorbereitet sein und verdächtiges Verhalten melden. Die Schulungsinhalte können den Mitarbeitern entweder durch eine separate Schulungsveranstaltung oder durch Aushändigung des vorliegenden Handbuchs vermittelt werden.

Interne Verfahren: Es sind Fälle bekannt, in denen Kriminelle auch auf Mitarbeiter zugehen und diese entweder bestechen oder bedrohen, damit diese bestimmte Unterstützungshandlungen durchführen. Die Mitarbeiter sollten dabei unbedingt wissen, wie sie sich in bestimmten Situationen zu verhalten haben, beispielsweise wenn sie verdächtige Personen beobachten oder wenn sie bedroht werden. Der Händler sollte seinen Mitarbeitern für diese Zwecke besonders klare Anweisungen erteilen (idealerweise als Flyer oder E-Mail für späteres Nachlesen) und Verantwortlichkeiten für die Entgegennahme von Hinweisen festlegen.

Terminal-Sicherheit: Es ist wichtig, dass der Händler, insbesondere das Kassenpersonal, die eingesetzten POS-Terminals vollständig kennt und damit vertraut ist, um Veränderungen an den Geräten schnell erkennen und zeitnah reagieren zu können. Es ist zudem empfehlenswert, die eingesetzten POS-Terminals mit Hilfe bestimmter Sicherheitsvorkehrungen (Stahlseil, etc.) fest im Kassenbereich zu verankern und gegen Diebstahl zu sichern. Werden Terminals über einen längeren Zeitraum nicht verwendet, sollten diese vor jeglichem Zugriff durch Kunden und Mitarbeiter geschützt aufbewahrt werden.

Service-Termine: Der Händler sollte unbedingt sicherstellen, dass alle Besuche von Servicetechnikern oder Handwerkern vom Personal immer an den jeweiligen Vorgesetzten oder die Filialleitung verwiesen wird. Servicetermine sollten stets im Voraus vereinbart worden sein. Servicetechniker sollten darum gebeten werden, sich auszuweisen. Falls ein Termin nicht vereinbart worden ist oder die Berechtigung des Servicetechnikers unklar ist, sollte der Serviceprovider angerufen und um Bestätigung gebeten werden.

7. Dokumentation

7.1. Chargebacks

Bei einem Chargeback handelt es sich um eine von einem Karteninhaber veranlasste Rückbelastung einer bereits erfolgten Kartentransaktion. Dabei wird die ursprüngliche Kartenzahlung nachträglich rückgängig gemacht, dem Händler also belastet. Ein Chargeback kann verschiedene Ursachen haben. In erster Linie führt Kartenmissbrauch dazu, dass der eigentliche Karteninhaber der Belastung widerspricht. Es können aber auch Fehler wie Doppelverarbeitungen oder technische Probleme beim Transaktionsprozess zu Chargebacks führen. Doch es kann auch passieren, dass ein Karteninhaber ohne rechtmäßige Grundlage ein Chargeback veranlasst. Um dadurch keinen finanziellen Verlust zu erleiden ist es ratsam, gegen solche unrechtmäßigen Chargebacks vorzugehen und diesen zu widersprechen, indem der Händler einen sogenannten *Chargeback-Dispute* bei seinem Acquirer veranlasst.

Um im Falle eines Chargeback-Disputes vorbereitet zu sein, ist es empfehlenswert, sowohl sämtliche Kaufbelege (Auftragsbestätigungen, Verträge, Übergabeprotokolle, Lieferscheine, Quittungen, etc.) als auch die Ausdrucke des POS-Terminals (Zahlungsbeleg, Tagesabschluss-Beleg, etc.) aufzubewahren. Die Aufbewahrungsdauer muss dabei jedoch im Einklang mit den jeweils anwendbaren Datenschutzgesetzen stehen. Der nachfolgende Infokasten beinhaltet Beispiele von Dokumenten und Belegen, die eine ordnungsgemäße Erfüllung des Vertrags seitens des Händlers nachweisen und dadurch unberechtigte Chargebacks anfechten können:

! Bei Chargeback-Disputes hilfreiche Dokumente

- Kopie des Kassenbelegs oder Vertrags
- Kopie einer Auftragsbestätigung, falls vorhanden
- Ein Exemplar der Rückgabe- und Umtauschrichtlinie, gegebenenfalls mit Nachweis, wie Kunden über diese informiert werden
- Beschreibungen und Fotos der in Frage stehenden Ware sowie Angaben zur Übergabe an den Kunden
- Jegliche Nachweise darüber, dass die Ware dem Kunden ordnungsgemäß übergeben oder ausgeliefert worden ist (Schriftverkehr, Empfangsbestätigung, etc.)
- Bei Versand von Waren sollten Liefernachweise (Sendungsnummern, Lieferbestätigung, etc.) schriftlich dokumentiert werden, da Paketdienste diese oft nur bis zu 6 Monaten speichern
- Nachweis, dass der Kunde die Zahlung mit seiner Unterschrift selbst authentifiziert hat (Zahlungsbeleg mit Unterschrift des Kunden)
- Jegliche Nachweise darüber, dass der Kunde die Ware tatsächlich erhalten hat (E-Mails, sonstige Kommunikation, etc.)
- Bei Service-Dienstleistungen gegebenenfalls ein Nachweis, dass der Kunde Leistungen auch selbst genutzt hat oder eine Dienstleistung tatsächlich erbracht worden ist (Abnahmeprotokoll, etc.)
- Bei Reiseveranstaltungen gegebenenfalls ein Nachweis, dass der Kunde die fraglichen Reiseleistungen tatsächlich genutzt hat (gescannte Bordkarte, zusätzliche Käufe in Verbindung mit der gebuchten Reise wie etwa ein Sitzplatz-Upgrade oder Zusatz-Gepäck, etc.)
- Nachweis, dass die identische Zahlungskarte bereits zuvor bei dem Händler vorgelegt wurde für einen Warenkauf, der unbestritten war
- Sonstige Nachweise und Indizien

7.2. Anforderung von Belegen durch transact

Im Falle eines Chargeback-Disputes kann transact bestimmte Nachweisdokumente bei dem Händler anfordern und zur Prüfung an den Issuer weiterleiten. Eine solche Anforderung von Belegen wird transact per E-Mail vornehmen. Erhält der Händler eine Nachricht mit der Anforderung von Nachweisdokumenten, sollte dieser innerhalb der angegebenen Frist möglichst eindeutige, gut leserliche (Scans in hoher Qualität) und aussagekräftige Nachweise über die betreffende Kartenzahlung an transact senden. Zur Sicherstellung eines reibungslosen Verfahrens wird folgende Vorgehensweise empfohlen:

1. Notieren Sie die auf einer Anfrage angegebene Frist für die späteste Einreichung und stellen Sie sicher, dass diese nicht überschritten wird

2. Prüfen Sie die Transaktionsdetails und ordnen Sie der Transaktion den zugrunde liegenden Vorgang zu. Eine Beleganforderung enthält in der Regel folgende Angaben:
    a) Kartennummer der Transaktion in teils geschwärzter Form
    b) Die Nummer (Terminal ID) des eingesetzten POS Terminals
    c) Datum und Uhrzeit zu welcher die Transaktion erfolgt ist
    d) Betrag und Währung der Transaktion
    e) Transaktions-ID / Seriennummer der Transaktion auf dem Transaktionsbeleg

3. Prüfen Sie, welche Dokumente von Ihnen angefordert werden (Kassenbeleg, etc.)

4. Bereiten Sie die entsprechenden Dokumente vor. Sie können die an der Prüfung beteiligten Parteien zusätzlich unterstützen, indem Sie Scans, Fotos oder sonstige Dateien aussagekräftig benennen und prüfen, ob die Inhalte gut leserlich sind und zum Vorgang passen.

5. Senden Sie die angeforderte Dokumentation an die vorgegebene E-Mail-Adresse.

6. Speichern Sie eine Kopie des gesamten Vorgangs für Ihre Unterlagen ab.

! Wichtig

Beantworten Sie Beleganforderungen bitte auch dann, wenn die entsprechende Nachweisdokumentation nicht vorhanden ist. Achten Sie besonders auf fristgemäße Beantwortung. Erfolgt eine zu späte Rückmeldung, kann ein Chargeback in der Regel nicht mehr angefochten werden.

Stellt sich nach Prüfung des Chargeback-Disputes heraus, dass das Chargeback tatsächlich ohne rechtliche Grundlage ausgelöst worden ist, das heißt die Ware oder Dienstleistung wurde vertragsgemäß übergeben oder erbracht, so wird das Chargeback im Normalfall abgewiesen und der Händler erhält schließlich wieder eine Gutschrift.

8. Reduzierung von Chargebacks

Folgende Tipps können bei der Reduzierung von Chargebacks helfen. Nicht nur sind Chargebacks mit Gebühren verbunden und die Beantwortung von Beleganforderungen zeitaufwendig; sollten Chargebacks sogar unberechtigter Weise erfolgt sein, erleidet der Händler häufig einen Verlust in Höhe des Rechnungsbetrags, sofern er keine Nachweise einreicht. Die größte Gefahr allerdings stellen Chargebacks dar, wenn deren Anteil am Gesamtumsatz einen bestimmten Grenzwert (siehe Vertragsbedingungen) überschreitet. In diesem Fall kann ein Händler durch die Kartenorganisation in ein sogenanntes Chargeback-Programm aufgenommen werden. Dabei kann es auch zu gesonderten Zusatzgebühren für alle weiteren Chargebacks kommen. Wir stellen deshalb einige Tipps zur Verfügung, um bei diesem Problem die Oberhand zu behalten:

! Tipps zur Reduzierung von Chargebacks

1. Informieren Sie Ihre Kunden darüber, wie sie sich im Falle von Umtausch, Reklamationen oder Beschwerden zu verhalten haben. In solchen Fällen sollten sich die Kunden immer zuerst an Sie wenden. Eine Umtausch- oder Reklamationsrichtlinie kann beispielsweise am Ladeneingang oder im Kassenbereich für alle Kunden sichtbar angebracht werden.

2. Sofern Warenversand erfolgt, sollten Kunden jederzeit wissen, wann die gekaufte Ware bei Ihnen ankommt. Besonders viel Transparenz ist dann gefordert, falls es zu Lieferschwierigkeiten kommen sollte. Kunden sollten über jede Art von absehbarer Leistungsstörung informiert werden, um das Risiko von Chargebacks zu reduzieren.

3. Stellen Sie sicher, dass Kunden Sie auf den Kartenabrechnungen sofort wiedererkennen. Es ist wichtig, dass die Karteninhaber auch nach längerer Zeit in der Lage sind, auf Grundlage der kurzen Beschreibung auf der Kartenabrechnung eine Verbindung zu Ihrem Unternehmen und der erbrachten Leistung herzustellen. Falls der Text auf der Kartenabrechnung keinerlei Ähnlichkeit mit Ihrem Firmennamen hat, erhöht das die Gefahr von Chargebacks, da Kunden möglicherweise eine fremde und unzulässige Abbuchung vermuten. Den Text, mit welchem Ihr Unternehmen auf Kartenabrechnungen erscheint, haben Sie im Antragsformular festgelegt.

4. Prüfen Sie, ob Ihre Kassen- oder Transaktionsbelege übersichtlich aufgebaut und gut lesbar sind. So sollte zum einen Ihr Firmenname gut lesbar auf dem Kassen- oder Transaktionsbeleg zu sehen sein, damit Kunden Ihren Beleg später auch eindeutig einer Abbuchung auf ihrer Karte zuordnen können. Zum anderen sollten Sie Firmenlogos und Marketingnachrichten nicht im Bereich der Transaktionsdaten aufdrucken, um diese nicht unleserlich zu machen.

5. Achten Sie insgesamt darauf, dass Belege, die Sie Kunden geben, störungsfrei gedruckt worden sind. Rote Streifen auf dem Belegpapier zeigen an, dass die Rolle zu Ende ist. Geben Sie Belege mit roten Streifen nicht an Kunden, weil das die Leserlichkeit beeinflussen kann, sondern wechseln Sie die Rolle. Prüfen Sie nach dem Drucken der Belege auch, ob die Tinte kräftig ist.

6. Ebenfalls trägt auch geschultes Personal dazu bei, Chargebacks zu reduzieren, indem das Kassenpersonal die Grundregeln sicherer Kartenzahlungen einhält:
   - Echtheitsprüfung der Karte, Prüfung Karteninhaber
   - Unterschriftsprüfung auf dem Zahlungsbeleg
   - Händigen Sie dem Kunden eine Kopie des Zahlungsbelegs (Kundenbeleg) aus, behalten Sie das unterschriebene Original (Händlerbeleg)

9. Die häufigsten Fehler-Codes auf dem POS-Terminal

Fehlercode	Text auf dem Display oder dem Beleg des POS-Terminals Beschreibung des Fehlers
03	"VU-Nummer nicht bekannt" oder "Systemfehler" Die Vertragsnummer ist nicht freigeschalten. Bitte rufen Sie unseren Technischen Support (Tel. 089 899 643 20) an.
05	"Keine Genehmigung" oder "Vorgang abgelehnt" Die Transaktion wurde nicht genehmigt.
12	"Transaktion ungültig" Die Transaktion wurde nicht genehmigt.
13	"Betrag ungültig" oder "Vorgang nicht mgl." Die Zahlung wurde abgelehnt, weil der Betrag zu hoch bzw. das Limit der Karte erreicht wurde.
14	„Kartennummer ungültig“ Die Kartennummer ist ungültig.
21	"Systemfehler" oder "Vorgang nicht mgl." Aktion abgelehnt, da die Bezugstransaktion nicht gefunden wurde.
33	"Karte ungültig" oder "Karte verfallen" Das Gültigkeitsdatum der Karte ist abgelaufen.
34	"Transaktion ungültig oder nicht möglich" Es liegt ein Verdacht auf Manipulation vor.
40	"Funktion ungültig" Die Zahlung wurde nicht autorisiert. Evtl. ist die Vertragsnummer des Acquirers nicht freigeschalten. Bitte rufen Sie unseren Technischen Support (Tel. 089 899 643 20) an.
43	"Karte einziehen" oder "Transaktion nicht mgl." Die Karte wurde als gestohlen gemeldet.
55	"Geheimzahl falsch" Die Geheimzahl wurde falsch eingegeben. Vorgang bitte mit der richtigen Geheimzahl wiederholen.
56	"Karte ungültig" Der Karteninhaber ist darum zu bitten, sich mit seiner Hausbank / Kartengesellschaft in Verbindung zu setzen.
58	"Terminal unbekannt" oder "Terminal nicht zugelassen" Die Vertragsnummer ist nicht freigeschalten. Bitte rufen Sie unseren Technischen Support (Tel. 089 899 643 20) an.
62	"Karte nicht zugelassen" Die Karte ist gesperrt. Der Karteninhaber ist an seine Hausbank oder Kreditkartengesellschaft zu verweisen.
64	"Storno abgelehnt" oder "Betrag abweichend" Der Transaktionsbetrag weicht von der Bezugstransaktion ab. Storno bitte mit richtigem Betrag wiederholen.
89	"Systemfehler" Terminal initialisieren, bitte OK-Taste drücken oder unseren Technischen Support (Tel. 089 899 643 20) anrufen.