Sicheres Bezahlen im Internet

Sparkasse Chemnitz
Bahnhofstr. 51, 09111 Chemnitz

Fassung April 2024

1. Allgemeine Hinweise

1.1. Ihre Mastercard/Visa Card (Kreditkarte) bzw. Mastercard Basis/Visa Basis (Debitkarte), bzw. Sparkassen-Card Debit Mastercard (Debitkarte) oder Sparkassen-Card Visa Debit (Debitkarte), nachfolgend „Karte“ genannt, ist mit Kartendaten [16-stellige Primary Account Number (PAN), Kartenprüfnummer (Card Validation Code (CVC)/Card Verification Value (CVV)) und das “Gültig-bis”-Datum] ausgestattet, die einen Einsatz der Karte für Fernzahlungen im Internet (Online-Handel) ermöglichen.

1.2. Geben Sie die Kartendaten Ihrer Karte zum Bezahlen im Internet nur bei Händlern und Dienstleistungsunternehmen an, welche Ihnen absolut vertrauenswürdig erscheinen.

1.3. Achten Sie darauf, dass die Kartendaten ausschließlich verschlüsselt übertragen werden. Dies erkennen Sie daran, dass die Internetadresse mit „https“ beginnt.

1.4. Als weitere Sicherheit nutzen Händler und Dienstleistungsunternehmen bei Fernzahlungen im Internet sogenannte 3-D Secure Verfahren der Kartengesellschaften Mastercard (Mastercard® Identity Check™) bzw. Visa (Visa Secure) als besondere Authentifizierungsverfahren zur Überprüfung der Identität des Karteninhabers oder der berechtigten Verwendung der Karte. Ob ein Händler das für die Karte einschlägige 3-D Secure Verfahren verwendet, wird Ihnen im jeweiligen Bezahlprozess angezeigt.

1.5. Sie können bis zur Höhe Ihres Verfügungsrahmens Einkäufe im Internet tätigen. Sofern Sie ein von Ihrem Verfügungsrahmen eingeschränktes Limit für Interneteinkäufe wünschen, wenden Sie sich bitte an Ihr Institut. Bitte beachten Sie, dass der Verfügungsrahmen für Interneteinkäufe in Einzelfällen auch für das Bezahlen vor Ort bei Handels- und Dienstleistungsunternehmen gelten kann und eine Limiteinschränkung dann für beides gilt.

2. Durchführen einer Fernzahlung im Online-Handel

2.1. Zur Durchführung einer Fernzahlung mit der Karte im Online-Handel werden im Rahmen des Bezahlprozesses im Internet die Daten Ihrer Karte abgefragt. Bitte achten Sie darauf, dass Sie diese nur in einer sicheren Umgebung eingeben (s. Ziffer 1). Andernfalls besteht ein erhöhtes Risiko bei der Übermittlung Ihrer Daten.

2.2. Nutzt ein Händler das 3-D Secure Verfahren, ist es zur Authentifizierung Ihrer Fernzahlung im Internet zusätzlich erforderlich, dass Sie Ihre Karte für das 3-D Secure Verfahren registrieren, z.B. über die S-pushTAN-App bzw. die S-ID-Check-App. Detailinformationen zum Registrierungsprozess Ihrer Karte für 3-D Secure finden Sie auf der Internetseite Ihres Instituts. Sofern Sie Ihre Karte nicht für 3-D Secure registrieren, kann die Fernzahlung im Online-Handel gegebenenfalls nicht durchgeführt werden.

2.3. Ihre Zustimmung (Autorisierung) zu der Fernzahlung erteilen Sie grundsätzlich durch die Eingabe Ihrer Kartendaten in der Bezahlanwendung. Fordert die Bezahlanwendung darüber hinaus Ihre Authentifizierung, müssen Sie die Kartenverfügung zusätzlich über das 3-D Secure Verfahren nach Kontrolle der Ihnen angezeigten Auftragsdaten in der App bestätigen. Mit diesen Schritten ist die Fernzahlung mit Ihrer Karte abgeschlossen.

3. Achten Sie auf Auffälligkeiten/Umsatzreklamation

3.1. Kommt Ihnen im Bezahlprozess im Internet etwas ungewöhnlich vor oder vermuten Sie den Missbrauch Ihrer Kartendaten für Fernzahlungen im Online-Handel oder Ihrer persönlichen individualisierten Authentifizierungselemente, kontaktieren Sie bitte umgehend Ihren Karteninhaberservice. Den Kontakt finden Sie u. a. auf der Rückseite Ihrer Karte.

3.2. Bei Umsatzreklamationen ungewöhnlicher oder missbräuchlicher Fernzahlungsvorgänge wenden Sie sich an den Karteninhaberservice oder Ihr kartenausgebendes Institut. Sie werden schriftlich über die weitere Bearbeitung informiert.

Die Bearbeitung kann unterschiedlich aussehen. Je nach Fallkonstellation wird entweder ein Beleg angefordert, eine Rückbuchung mit Gutschrift vorgenommen oder es werden weitere Unterlagen von Ihnen angefordert. Der Karteninhaberservice wird in Abstimmung mit Ihnen weitere Maßnahmen zur Sicherung Ihrer Karte ergreifen, z. B. die (vorläufige) Sperrung der Karte oder die endgültige Sperrung der Karte und Veranlassung einer Ersatzkartenausstellung.

4. Präventivmaßnahmen Ihres kartenausgebenden Instituts

4.1. Das kartenausgebende Institut ist in den Kartenbedingungen geregelten Fällen berechtigt, die Karte zu sperren oder einen Fernzahlungsvorgang im Online-Handel aufgrund fehlender Autorisierung oder von Sicherheitsbedenken – z. B. wenn keine Authentifizierung erfolgt ist – abzulehnen. Diese Maßnahmen verhindern Betrug und dienen Ihrem Schutz.

4.2. Über eine Sperre werden Sie unverzüglich telefonisch oder schriftlich informiert.

4.3. Für Informationen hierzu steht Ihnen Ihr Karteninhaberservice zur Verfügung. Dort können Sie zudem die Aufhebung der Sperre beantragen bzw. klären, warum es zur Ablehnung der Fernzahlung im Internet kam. Sollten Sie durch diese Maßnahme bei Ihrem Einkauf behindert worden sein, können Ihnen die Mitarbeiter sofort weiterhelfen.

5. Verlust/Kompromittierung der personalisierten Sicherheits-Berechtigungsnachweise oder der individualisierten Authentifizierungselemente des Karteninhabers für 3-D Secure

Wenn Ihr Passwort oder Ihre Kartendaten ausgespäht worden sind oder in falsche Hände geraten, wenden Sie sich unverzüglich an Ihren Karteninhaberservice oder Ihr Institut. Dies gilt auch für Vorfälle während eines Zahlungsvorgangs oder in Sozialen Netzwerken (z. B. Anfrage nach Ihren Zahlungsdaten).

6. Betrugsfall/Missbrauchsverdacht

6.1. Informieren Sie Ihr kartenausgebendes Institut bzw. den Karteninhaberservice bitte unverzüglich, z. B. telefonisch, wenn Sie wissen oder vermuten, dass unbefugte Personen im Besitz Ihrer persönlichen Kartendaten oder Ihrer individualisierten Authentifizierungselemente sind.

6.2. Ihr kartenausgebendes Institut bzw. der Karteninhaberservice stimmen mit Ihnen ab, ob die Sperrung Ihrer Karte erforderlich ist.

6.3. Sofern betrügerische Kartenverfügungen mit Ihrer Karte oder Ihren Kartendaten erfolgen, werden Sie durch Ihr Institut bzw. den Karteninhaberservice umgehend informiert.

7. Schutz Ihrer Daten

7.1. Passwörter, persönliche Angaben und sonstige vertrauliche Daten gehören nur Ihnen und müssen vor dem unbefugten Zugriff anderer Personen geschützt werden. Auch Ihr Kundenberater kennt diese vertraulichen Informationen nicht. Niemand von Ihrem kartenausgebenden Institut wird diese von Ihnen erfragen.

7.2. Bei der Registrierung oder Neuregistrierung für das 3-D Secure Verfahren (Mastercard® Identity Check™ oder Visa Secure) informiert Ihr kartenausgebendes Institut Sie über den genauen Ablauf und die Voraussetzungen einer Zahlung nach diesem Verfahren.
Achten Sie bei der Registrierung oder Neuregistrierung darauf, dass diese im sicheren Umfeld Ihres Instituts erfolgt (z. B. Internetfiliale, Sparkassen-Apps).

7.3. Ihr kartenausgebendes Institut setzt nur sichere und zertifizierte Hard- und Software ein. Achten Sie darauf, dass Sie ggf. Apps, die Sie von Ihrem kartenausgebenden Institut zur Verfügung gestellt bekommen, durch einen sicheren Download erhalten (Apple Store, Google Play Store etc.). Nur diese Programme sind geprüft und sicher. Genaue Hinweise erhalten Sie bei der Registrierung zum jeweiligen Verfahren.

manuell

128 775.000 D0 S-Payment (Fassung Apr. 2024) - v4.0

7.4. Um die Karte für Zahlungen im Internet sicher verwenden zu können, achten Sie bitte auf eine sichere IT-Umgebung. Dazu gehören:

- ein aktuelles Antivirenprogramm
- eine konfigurierte Firewall
- ein aktuelles Betriebssystem mit allen Sicherheitsupdates
- einen aktuellen, mit allen Sicherheitsupdates versehenen Browser
- eine sichere (verschlüsselte) Verbindung zur Website. Diese erkennen Sie am Schlosssymbol in Ihrem Browser sowie daran, dass die Internetadresse mit „https“ beginnt.
- eine sichere Verbindung zum Internet (unverschlüsselte WLAN Verbindungen an öffentlichen Plätzen können von Angreifern kompromittiert werden)

Hinweis: Auch die korrekte Schreibweise der URL in der Adresszeile im Browser ist wichtig. Betrüger können sich Tippfehler zunutze machen, um Sie auf eine ähnliche Seite umzuleiten, wenn Sie Ihre Zahlungsdaten eingeben.

7.5. Laden Sie Dateien und Programme aus dem Internet nur von vertrauenswürdigen Seiten herunter und nur wenn Sie mit hinreichender Sicherheit feststellen können, dass die Software echt ist und nicht manipuliert wurde.

7.6. Geben Sie die für die Durchführung einer Fernzahlung im Online-Handel notwendigen Kartendaten nicht auf unbekannten oder nicht vertrauenswürdigen Seiten ein.

8. Künftige Informationen/Anfragen

8.1. Ihr kartenausgebendes Institut wird Sie über Änderungen im Internetzahlungsverkehr oder weitere Sicherheitshinweise nur über einen gesicherten Kommunikationsweg informieren. Dazu zählen nur Ihr elektronisches Postfach im Online-Banking, eine gesicherte Website, Nachrichten am Kontoauszugsdrucker oder der Postweg. Andere Nachrichtenwege (mündlich, telefonisch, E-Mail, SMS etc.) sind nicht vertrauenswürdig.
Wenn Ihnen eine Nachricht verdächtig vorkommt, setzen Sie sich bitte umgehend mit Ihrem kartenausgebenden Institut in Verbindung.

8.2. Für alle weiteren Anfragen steht Ihnen der Karteninhaberservice zur Verfügung. Den Kontakt finden Sie auf der Rückseite Ihrer Karte. Darüber hinaus wenden Sie sich gerne auch an Ihren Kundenberater bei Ihrem kartenausgebenden Institut.

manuell

128 775.000 D0 S-Payment (Fassung Apr. 2024) - v4.0