Merkblatt „Informationen über Internetzahlungen"

Bezahlen im Internet/sicheres Verfahren 11/2020

apoBank
Bank der Gesundheit

Als Karteninhaber erhalten Sie per Post die von Ihnen beantragte Mastercard Firmenkreditkarte (nachfolgend kurz „Karte" genannt) und mit getrennter Post die persönliche Geheimzahl (PIN) für Transaktionen an Kartenzahlungsterminals und an Geldautomaten. Die Karte kann, wie in Ziffer **3.3** der „Einsatzbedingungen der Mastercard Firmenkreditkarte" (nachfolgend kurz „Einsatzbedingungen") beschrieben, für Zahlungen im Internet verwendet werden.

Durch Ihren Kartenantrag bestätigen Sie, dass Sie über diese Möglichkeit zur Internetzahlung informiert sind und diese akzeptieren bzw. wünschen. Als Karteninhaber haben Sie darauf zu achten, dass die übermittelten Kartendaten verschlüsselt („https://") übertragen werden (vgl. Ziffer **5.4** der Einsatzbedingungen). Bitte setzen Sie die Karte im Internet nur in einer sicheren Umgebung ein (Details siehe nachfolgend unter „Sicherer Karteneinsatz im E-Commerce"). Die Eingabe Ihrer Kartendaten über unverschlüsselte Verbindungen, die Preisgabe Ihrer Kartendaten aufgrund von E-Mail-Anforderungen (z. B. angebliche Sicherheitsüberprüfungen, nicht angeforderte Benutzerkonto-Entsperrungen o. Ä.) oder die Freigabe anderer Geldbeträge oder Empfänger als erwartet, bergen Risiken für sichere Zahlungen. Die Gefahr besteht insbesondere darin, dass Unberechtigte Ihre Kartendaten einschließlich der Autorisierungsdaten ausspähen und für unberechtigte Transaktionen einsetzen können.

Sofern von der Akzeptanzstelle das Kundenauthentifizierungsverfahren Mastercard Identity Check™ (im Folgenden „sicheres Bezahlverfahren") unterstützt und dessen Nutzung durch den Herausgeber gefordert wird, ist dieses von Ihnen als Karteninhaber einzusetzen (vgl. Ziffer **3.3** der Einsatzbedingungen). Bitte registrieren Sie sich daher direkt nach Erhalt Ihrer Karte auf unserer Internetseite für das entsprechende sichere Bezahlverfahren.
Stellen Sie sicher, dass kein anderer Kenntnis von den Kennungen für dieses Bezahlverfahren erlangt (vgl. Ziffer **5.4** der Einsatzbedingungen). Eine gesonderte Beschreibung des Anmelde- und Registrierungsvorgangs zum 3D Secure Verfahren finden Sie auf unserer Internetseite unter www.apobank.de/3d-Secure.
Der Zahlungsrahmen, der Ihnen mit Übersendung der Karte erstmalig mitgeteilt wird und in Abstimmung mit der Bank geändert werden kann, **gilt sowohl für das persönliche Bezahlen in der Akzeptanzstelle wie auch für das Bezahlen im Internet**. Die Internetzahlungsfunktion lässt sich auf Ihren Wunsch in der monatlichen Höhe begrenzen oder deaktivieren.

Sicherer Karteneinsatz im E-Commerce.

Sie können mit Ihrer Karte im Internet Waren und Dienstleistungen bezahlen. Gemäß Ziffer **3.3** der Einsatzbedingungen **dürfen bei einer Kartenzahlung im Internet nur folgende Daten angegeben werden**:

- Ihr Name,
- die Kartenmarke (Mastercard),
- die Kartennummer,
- das Laufzeitende der Karte und
- die auf der Kartenrückseite genannte dreistellige Kartenprüfziffer.

Bitte geben Sie niemals die PIN an, die Sie für Zahlungen an Kartenzahlungsterminals oder zur Bargeldauszahlung am Geldautomaten erhalten haben! Eine auf Ihrem Mobiltelefon erhaltene Nachricht zur Authentifizierung der Zahlung darf nur bestätigt oder die E-Commerce TAN eingegeben werden, wenn Zahlungsempfänger, Betrag und Währung geprüft wurden und mit der freizugebenden Zahlung übereinstimmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt auf seinen Internetseiten (https://www.bsi-fuer-buerger.de) die nachfolgenden **10 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet**:

1. Halten Sie Ihre Software aktuell.
2. Nutzen Sie Virenschutz und Firewall.
3. Legen Sie unterschiedliche Benutzerkonten an.
4. Seien Sie zurückhaltend bei der Weitergabe persönlicher Daten.
5. Verwenden Sie einen aktuellen Webbrowser.
6. Nutzen Sie unterschiedliche Passwörter, die Sie bei Bedarf ändern.
7. Schützen Sie Ihre Daten durch Verschlüsselung.
8. Seien Sie vorsichtig bei E-Mails und deren Anhängen.
9. Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter.
10. Fertigen Sie regelmäßig Sicherheitskopien an.

Berücksichtigen Sie die erheblichen Bedrohungen und Risiken, die mit dem Herunterladen von Software über das Internet verbunden sind, wenn Sie nicht mit hinreichender Sicherheit feststellen können, ob die Software echt ist und nicht manipuliert wurde.
Sofern Sie den Verdacht haben, dass Ihre Kreditkartendaten auf Ihrem Computer ausgespäht wurden, sperren Sie Ihre Kreditkarte sofort telefonisch unter der auf der Umsatzaufstellung mitgeteilten 24-Stunden-Rufnummer (Sperrannahme-Service) **+49 (0) 721 1209 66001**. Lassen Sie Ihre Karte auch unverzüglich sperren, wenn Sie den Verlust der Karte oder missbräuchliche Nutzung der Karte, der Kartendaten oder eines Legitimationsmediums feststellen oder einen entsprechenden Verdacht haben (vgl. Ziffer **5.5** der Einsatzbedingungen). Sofern Sie auf Ihrem mobilen Endgerät eine digitale Karte nutzen und Ihnen das Gerät abhandengekommen ist, sperren Sie diese digitale Karte sofort telefonisch unter der vorstehenden Sperr-Rufnummer. Sie können sich jederzeit auf der Internetseite des BSI unter „Service/Aktuell" über **aktuelle Sicherheitswarnungen** und Sicherheitsupdates informieren.

Information über Umsatzausführung.

Sofern Ihr Arbeitgeber (nachfolgend „Firma") mit der Bank eine gesonderte Vereinbarung zum Online-Banking geschlossen und Ihnen einen Online-Banking- Zugang eingeräumt hat, haben Sie über das Online-Banking bzw. die von der Bank bereitgestellte Banking-App jederzeit die Möglichkeit, die gebuchten Umsätze und den Saldo Ihrer Karte einzusehen.

Information und Kontaktaufnahme im Fall von Missbrauchsverdacht oder neuen Sicherheitsmaßnahmen.

Ihre Karte ist ein sicheres Zahlungsmittel. Vor Betrug schützen Sie auch Präventions- und Monitoringsysteme, die versuchen, Auffälligkeiten beim Karteneinsatz frühzeitig vor dem Hintergrund allgemeiner Erfahrungswerte, aktueller Vorfälle und auch anhand Ihres bisherigen Karteneinsatzes zu entdecken. Es kann daher in Einzelfällen vorkommen, dass eine beabsichtigte Transaktion einer Überprüfung bedarf oder nicht ausgeführt wird. Wir werden die Firma bzw. Sie, bei sicherheitsrelevanten Vorfällen telefonisch, per Brief, über eine Mitteilung auf dem Kontoauszug oder, sofern von der Firma vorgesehen und von Ihnen genutzt, über den elektronischen Postkorb im Online-Banking bzw. der von der Bank bereitgestellten Banking-App informieren. Informationen zu allgemeinen Sicherheitsmaßnahmen (z. B. Warnung vor Phishing-E-Mails) erhalten Sie auch auf unserer Internetseite. Ebenso können Sie Auffälligkeiten, Unregelmäßigkeiten während der Sitzung bei Internetzahlungsdiensten, unerwartete Aufforderungen zur Preisgabe von Karten- oder Legitimationsdaten oder einen Missbrauchsverdacht jederzeit über die Sperr-Hotline **+49 (0) 721 1209 66001** telefonisch melden. Je nach Ergebnis der Abstimmung mit Ihnen kann Ihre Karte wieder eingesetzt und der Zahlungsauftrag ausgeführt werden, oder bei Verdacht auf Missbrauch wird die Karte gesperrt und kostenfrei ersetzt.

Beschreibung der Haftung.

Sofern der Karteninhaber einen Zahlungsauftrag nicht autorisiert hat, nicht vorsätzlich oder missbräuchlich gehandelt hat und alle Sorgfaltspflichten laut Einsatzbedingungen eingehalten hat, haftet die Firma nicht für die nicht autorisierten Umsätze. Andernfalls richtet sich die Haftung nach den in den Bedingungen beschriebenen Regelungen.