INFORMATIONSBLATT

RAIFFEISEN BANKKARTE (DEBITKARTE)

INFORMATIONEN ZUR BANK

RAIFFEISENKASSE PARTSCHINS GENOSSENSCHAFT
SPAUREGGSTRASSE 12 - 39020 - PARTSCHINS
Tel: 0473/967133
Fax: 0473/967766
E-Mail: rk.partschins@raiffeisen.it
PEC: pec08175@raiffeisen-legalmail.it
Webseite: www.raikapartschins.it

Eintragungsnummer im Bankenverzeichnis bei der Banca d'Italia: 3690.5.0
dem Einlagensicherungsfonds der Genossenschaftsbanken und dem Nationalen Garantiefonds laut Art. 62 LD Nr. 415/96 angeschlossen
Mitglied des institutsbezogenen Sicherungssystems Raiffeisen Südtirol IPS

WAS IST DIE RAIFFEISEN BANKKARTE

Mit der Raiffeisen Bankkarte kann der Kunde je nach den auf der Debitkarte (nachfolgend auch Karte genannt) aktivierten Diensten bzw. Systemen bargeldlos Zahlungen durchführen oder an entsprechenden Geldautomaten Bargeld abheben. Die Belastung erfolgt unmittelbar auf dem Kontokorrent.
Zudem kann der Kunde bei Geldautomaten der Bank, die dazu befähigt sind, Bargeldeinzahlungen tätigen, die auf dem mit der Karte gekoppelten Kontokorrent gutgeschrieben werden. Es ist die Eingabe einer Geheimnummer (PIN) notwendig.

Die Dienste werden über verschiedene Anbieter bzw. Systeme z.B. BANCOMAT®, PagoBANCOMAT® und Maestro abgewickelt:

Bargeldbehebungen und Bargeldeinzahlungen: Behebung und Einzahlung innerhalb der vertraglich vereinbarten Betragsgrenzen an Geldautomaten (ATM und/oder Self-Service Gerät), die mit der Marke BANCOMAT® oder Maestro oder den Marken der anderen Anbieter, die von der Bank mitgeteilt werden, gekennzeichnet sind. Es ist die Eingabe einer Geheimnummer (PIN) notwendig.
Scheckeinlage: Einwurf von Schecks bei den eigens dafür vorgesehenen und gekennzeichneten Self-Service Geräten der eigenen Bank.
Geldwechsel: Wechsel von Banknoten bei den eigens dafür vorgesehenen und gekennzeichneten Self-Service Geräten der eigenen Bank.
Zahlungsdienst: Bargeldlose Zahlung von Waren und Dienstleistungen im Inland innerhalb der vertraglich vereinbarten Betragsgrenzen bei konventionierten Unternehmen. Es ist die Eingabe einer Geheimnummer (PIN) notwendig. Die Zahlung erfolgt über eigene Terminals, die mit der Marke PagoBANCOMAT® oder Maestro oder den Marken der anderen Anbieter, die von der Bank mitgeteilt werden, gekennzeichnet sind.
Fastpay: Bezahlung der Autobahnmaut für Autobahnstrecken, die von konventionierten Gesellschaften oder Körperschaften geführt werden. Die Mautstellen müssen allerdings über geeignete Terminals verfügen, die durch das Markenzeichen Fastpay gekennzeichnet sind. Die Belastung des Kontokorrents erfolgt hier einmal monatlich für die im Vormonat vorgenommenen Zahlungen mit gewichteter, durchschnittlicher Wertstellung.
Fastpay kann, auch für den Ankauf von Fahrscheinen für Bus und Bahn bei allen automatischen Fahrkartenschaltern, die vom Betreiber des öffentlichen Nahverkehrs geführt werden, für die Zahlung von Parkplatzgebühren, usw. aktiviert werden.
Selbstbedienung: Aufladen von Mobiltelefonen durch Verwendung der Raiffeisen Bankkarte und der Geheimnummer (PIN), Druck des Kontoauszuges und anderer Dokumente, sowie Abwicklung eventueller weiterer Dienste.
Zahlungen im Internet: Elektronische Zahlungen in Internetshops mittels Verwendung der Maestro Funktion und von zwei persönlichen Kodexen.
NFC - Kontaktlose Zahlungen: POS Zahlungen im In - und Ausland innerhalb der vereinbarten Betragshöhe, ohne dass zu diesem Zweck die Karte ins POS Terminal eingeführt oder die P.I.N. eingegeben werden müssen.

Zu den Hauptrisiken der Raiffeisen Bankkarte gehört wohl der Missbrauch bzw. die rechtswidrige Verwendung der Karte durch Dritte. Entsprechend muss die Karte und die PIN sorgfältig aufbewahrt werden; besonders die PIN muss geheim bleiben. Im Falle der Entwendung oder des Verlustes der Karte oder der PIN muss der Kunde unverzüglich die Sperre der Karte auf die vertraglich vorgesehene Art und Weise (Anruf Sperrnummer) beantragen. Um diesen Risiken entgegenzuwirken, können auf der Karte folgende Sicherheitsmaßnahmen aktiviert werden:

SMS-Alert-Dienst: SMS-Mitteilung an die vereinbarte Handynummer, falls mit der Karte Behebungen oder Zahlungen über den vereinbarten Betrag durchgeführt werden.

Sperre außereuropäische Länder: Die Raiffeisen Bankkarte ist nur nach entsprechender Anfrage des Kunden für einen begrenzten Zeitraum in Staaten außerhalb Europas aktiviert.

Negative Folgen ergeben sich außerdem aus einem von der Bank verfügten zeitweisen Verbot zur Benutzung der Karte (Sperre) im Falle eines widerrechtlichen oder nicht autorisierten Gebrauchs der Karte seitens des Kunden.

Information im Sinne der Verordnung(EU)2015/751

Verfügbare Zahlungsnetzwerke: BANCOMAT® e PagoBancomat, FastPay, MAESTRO

Technologie und Funktionalität:

	BANCOMAT® e PagoBancomat	**FastPay**	**MAESTRO**
Technologie	Magnetstreifen, Chip und C-less	Magnetstreifen	Magnetstreifen, Chip und C-less
Funktionalität	Behebung ATM und physische POS-Zahlung in Italien		Behebung ATM und physische und virtuelle POS-Zahlung in Italien, in der EU und außerhalb der EU

Fixspesen: siehe unten stehende Kostenposten (Wirtschaftliche Bedingungen)

Variable Spesen: siehe einzelne Kostenposten (Behebung, POS-Zahlung, usw.) laut Informationsblatt zum Kontokorrent, auf das verwiesen wird.

Sicherheitsmerkmale:

Folgendes ist gewährleistet:

- Mastercard und BANCOMAT® Zertifizierungen/Zulassungen für alle Produkte;
- Einhaltung der EMV/ISO-Standards;
- Einhaltung der Mastercard-Standards für RFID-Antenne und Chip für Zahlungen (auch kontaktlose);
- Online-Autorisierungsanfrage für Chip-Transaktionen.

Das Berechtigungssystem stellt die erste Stufe der Kontrolle der Transaktionen dar, wie z.B.:

- PIN-Validierung;
- Verfügbarkeit des mit der Karte verbundenen Plafonds;
- Status der Karte (gesperrt, nicht gesperrt);
- Validierung der Sicherheitselemente der Karte (CVV2, CVC2, 3DSecure);
- Nutzungslimits je nach Art der Ausgaben.

Alle wegen Betrugs bestrittenen Vorgänge werden täglich gemeldet, damit der von SIPAF ("Sistema di prevenzione delle frodi sulle carte di pagamento" - "System zur Betrugsbekämpfung bei Zahlungskarten") vorgesehene Informationsfluss an die Zentrale Stelle für Betrugsbekämpfung (UCAMP - "Ufficio Centrale Antifrode dei Mezzi di Pagamento") vorbereitet wird.

Der Karteninhaber kann die Ausweitung oder Einschränkung der Verwendbarkeit der Karte auf einzelne vordefinierte geografische Gebiete oder weltweit beantragen. Über den Online-Banking-Service werden dem Kunden zur Verfügung gestellt:

- Funktion betreffend die Verwendung der Karte: Deaktivieren/Aktivieren der Möglichkeit, außerhalb Europas Behebungen/Zahlungen mit der Karte am Geldautomaten/POS vorzunehmen;
- 3D Secure: Schutzsystem, identifiziert mit "Mastercard Identity Check", das es ermöglicht, Einkäufe auf Websites zu tätigen, die mit dem Service konventioniert sind, und zwar mittels Verwendung eines Passwortes; außerdem wird dem Kunden ein Identifizierungssatz zugeordnet, der bei der Eingabe des Passwortes angezeigt werden kann, damit eine sichere Website erkennbar ist;
- SMS/E-Mail-Benachrichtigungen: können bei jeder Nutzung der Karte empfangen werden.

Der Informationsaustausch zwischen dem Terminal, den Anwendungszentren und der Bank erfolgt unter Beachtung

aller Sicherheitsstandards.
Treten Situationen auf, bei denen eine Operation, trotz bestehender Möglichkeit, nicht mittels Mikrochip durchgeführt wird, wird eine Fallback-Situation erzeugt. Um das Sicherheitsniveau der Karten zu erhöhen, ist das Funktionieren der Karte im Fallback nicht erlaubt.

WIRTSCHAFTLICHE BEDINGUNGEN

	POSTEN	KOSTEN
SPESEN	Spesen für Ausgabe einer Raiffeisen Bankkarte (BANCOMAT®, PagoBANCOMAT®, Maestro) - umfasst Ausgabe und Verwaltung der Karte	18,00 Euro jährlich (Verwaltung)
	Spesen für Kartenersatz	0,00 Euro
AUSNÜTZUNGS-LIMITS	BANCOMAT®: Betrag pro Tag	1.000,00 Euro
	BANCOMAT®: Betrag pro Monat	2.000,00 Euro
	PagoBANCOMAT®: Betrag pro Tag	1.500,00 Euro
	PagoBANCOMAT®: Betrag pro Monat	1.500,00 Euro
	Bargeldbehebung mit Maestro am ATM: Betrag pro Tag	500,00 Euro
	Bargeldbehebung mit Maestro am ATM: Betrag pro Monat	1.500,00 Euro
	Zahlung mit Maestro am POS: Betrag pro Tag	1.500,00 Euro
	Zahlung mit Maestro am POS: Betrag pro Monat	1.500,00 Euro
	Gesamtbetrag (ATM + POS im In- und Ausland) pro Tag	2.500,00 Euro
	Gesamtbetrag (ATM + POS im In- und Ausland) pro Monat	4.000,00 Euro
	FASTpay: Höchstbetrag pro einzelner Autobahngebühr Betrag für weitere Dienste pro Tag Höchstbetrag pro einzelne Autobahngebühr Brennerautobahn AG	 100,00 Euro 100,00 Euro 113,62 Euro
	NFC - Kontaktlose Zahlungen : Höchstbetrag pro einzelner Zahlung ohne PIN-Eingabe Höchstbetrag von aufeinanderfolgenden und kumulativen Zahlungen ohne PIN-Eingabe Höchstbetrag bei Zahlungen ohne PIN-Eingabe von "NO PIN"-Diensten	 50,00 Euro 150,00 Euro 100,00 Euro
	NO PIN: Höchstbetrag für Autobahngebühr Höchstbetrag für Parkplätze und Garagen Höchstbetrag für Reisetickets	 100,00 Euro 50,00 Euro 25,00 Euro
	Höchstbetrag Bargeld bei Zahlungen mit Cashback	100,00 Euro
	Höchstbetrag PagoBancomat® Transit	25,00 Euro
	Die Ausnützungslimits für die Bargeldbehebungen am Self-Service-Gerät werden im Formular "Zeichnungsberechtigung" festgelegt, auf das zu diesem Zweck verwiesen wird.	
WECHSELKURSE	Auf die Belastungen wird in der Regel der Wechselkurs des nächsten dem Tag der Durchführung der Operation folgenden Bankarbeitstages angewandt.	
WERTSTELLUNG	Tag der Bargeldbehebung Bezahlung mittels POS: Tag des Geschäftsfalles Fastpay: gewichtete durchschnittliche Wertstellung aller Zahlungen des vorangegangenen Monats Bargeldeinzahlungen am ATM und/oder Self-Service Gerät: Tag der Einlage wenn der Kunde ein Verbraucher ist, spätestens am darauffolgenden Bankarbeitstag, wenn der Kunde kein Verbraucher ist	

RÜCKTRITT UND BESCHWERDEN

Rücktritt vom Vertrag

Der Kunde kann vom Vertrag jederzeit zurücktreten, indem er der Bank dies schriftlich mitteilt und die Karte und das ihm ausgehändigte Material zurückgibt.
Die Bank kann von diesem Vertrag oder von einzelnen Diensten jederzeit unter Einhaltung einer Kündigungsfrist von 2 Monaten zurückzutreten. Bei Vorhandensein eines rechtfertigenden Grundes im Sinne des Verbraucherschutzgesetzes Nr. 206/2005 Art. 33 Abs. 3 oder wenn es aus Gründen der Effizienz oder Sicherheit des Dienstes erforderlich ist, kann die Bank vom Vertrag auch ohne Vorankündigung zurücktreten.
Jedenfalls haftet der Kunde für alle Folgen, die entstehen können, wenn die Dienste nach dem Rücktritt der Bank oder in der Zeit, in der die Bank die Nutzung der Dienste durch eine Mitteilung zeitweise verboten hat, trotzdem unter Verwendung der Karte genutzt werden.

Maximalfrist für die Beendigung der Vertragsbeziehung

Die Vertragsbeziehung endet mit der Rückgabe der Karte und des ausgehändigten Materials.

Beschwerden

Der Kunde kann bei der Bank Beschwerde einreichen, auch mittels Einschreiben mit Rückantwort oder auf telematischem Wege (RAIFFEISENKASSE PARTSCHINS GENOSSENSCHAFT, SPAUREGGSTRASSE 12, 39020 PARTSCHINS, PEC08175@RAIFFEISEN-LEGALMAIL.IT, RK.PARTSCHINS@RAIFFEISEN.IT, Fax: 0473/967766).
Sollte der Kunde innerhalb von 60 Tagen bzw. im Falle von Zahlungsdiensten innerhalb von 15 Bankarbeitstagen keine oder eine nicht zufriedenstellende Antwort erhalten haben, kann er binnen 12 Monaten ab Einreichung der Beschwerde einen Rekurs an das Schiedsgericht für Bank- und Finanzdienstleistungen und Operationen (ABF) stellen. Weitere Informationen über die Funktionsweise und die Verfahrensabläufe des ABF kann der Kunde auf der Homepage www.arbitrobancariofinanziario.it einsehen oder bei den Filialen der Banca d'Italia oder der Bank nachfragen.
Der Kunde kann zudem - allein oder gemeinsam mit der Bank - ein Schlichtungsverfahren einleiten, um eine Einigung zu erzielen. Genannter Schlichtungsversuch wird von der Bankenschlichtungsstelle (Conciliatore BancarioFinanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie - ADR; www.conciliatorebancario.it), angestellt.
Die vorherige Inanspruchnahme eines Verfahrens zur außergerichtlichen Streitbeilegung (Mediation bei einer beliebigen dazu ermächtigten Stelle, Mediation bei einer dazu ermächtigten und im Vertrag vereinbarten Stelle oder genanntes Verfahren beim Schiedsgericht für Bank- und Finanzdienstleistungen und Operationen-ABF) ist im Sinne des Art. 5 Abs. 1-bis des Legislativdekrets Nr. 28/2010 verpflichtend, sollte der Kunde beabsichtigen, für einen über die Auslegung und Anwendung des Vertrages entstehenden Streitfall das ordentliche Gericht anzurufen; dies bei sonstiger Unverfolgbarkeit der Klage. Das Mediationsverfahren wickelt sich vor der örtlich zuständigen Mediationsstelle und mit dem Beistand eines Rechtsanwaltes ab.

BEGRIFFSERKLÄRUNG

Bargeldbehebung	Der Kunde hebt Bargeld von seinem Konto ab. Die Raiffeisen Bankkarte ermöglicht die Behebung von Bargeld bei Geldautomaten (ATM - Automated Teller Machine und/oder Self-Service Gerät) im Rahmen der auf dem Kontokorrent verfügbaren Mittel (im hauseigenen Netz).
Zahlungen	Die Raiffeisen Bankkarte ermöglicht, den Erwerb/Kauf von Waren und Dienstleistungen bei konventionierten/angeschlossenen Geschäften im Rahmen der auf dem Kontokorrent verfügbaren Mittel (im hauseigenen Netz).
ATM (Automated Teller Machine)	Technische Einrichtungen für die Benützung der Karten in den vorgesehenen Funktionen (wie z.B. Geldausgabe, Selbstbedienung, Aufladungen, Bareinzahlungen).
POS	Technische Einrichtungen für die Benützung der Karten beim Kauf/Erwerb von Waren und Dienstleistungen (POS - Point of Sale)
Sperre der Debitkarte	Sperre der Karte infolge von Verlust oder Diebstahl
BANCOMAT® **PagoBANCOMAT®** **Maestro**	Markennamen der Anbieter, die in Italien und im Ausland verschiedene Dienste anbieten (Zahlungen, Bargeldbehebungen), die mittels der Raiffeisen Bankkarte in Anspruch genommen werden können. BANCOMAT®: Bargeldlose Zahlungen und Bargeldbehebungen an ATM in Italien. PagoBANCOMAT®: Bargeldlose Zahlungen an POS Geräten in Italien. Maestro: Bargeldlose Zahlungen an POS Geräten und Bargeldbehebungen in Italien und im Ausland.

Raiffeisen

Anleitung
Für eine sichere Nutzung der Raiffeisen Bankkarte bei Zahlungen im Internet

Das gegenständliche Dokument bildet integrierenden Bestandteil des Vertrages zur Raiffeisen Bankkarte - Debitkarte

Bei den Diensten, die es dem Kunden ermöglichen, Zahlungen im Internet durchzuführen, wendet die Bank die besten Maßnahmen der aktuellen Technologie an. Trotz alledem ist es möglich, dass der Kunde Opfer eines Betruges durch elektronische Mittel wird. Folglich ist es, zusätzlich zu den von der Bank getroffenen Sicherheitsmaßnahmen erforderlich, dass der Kunde über ausreichende Kenntnisse verfügt, um die Zahlungen im Internet sicher zu gestalten.

Zu den Hauptrisiken der Debitkarte gehört der Missbrauch bzw. die rechtswidrige Verwendung der Karte durch Dritte. Entsprechend müssen die Karte und das Passwort sowie die Mobiltelefonnummer sorgfältig aufbewahrt werden; besonders das Passwort muss geheim bleiben. Im Falle der Entwendung oder des Verlustes der Karte oder des Passwortes muss der Kunde unverzüglich die Sperre der Karte auf die vertraglich vorgesehene Art und Weise (Anruf Sperrnummer) beantragen.
Negative Folgen ergeben sich außerdem aus einem von der Bank verfügten zeitweisen Verbot zur Benutzung der Karte (Sperre) im Falle eines widerrechtlichen oder nicht autorisierten Gebrauchs der Karte seitens des Kunden.
Schlussendlich kann der Kunde Opfer eines Hackerangriffes werden, welcher über das vom Kunden verwendete Gerät erfolgt und z.B. den Diebstahl der Zugangsdaten, das Erstellen einer Bildschirmkopie, die veränderte Darstellung von Webseiten zwecks unrechtmäßiger Aneignung des Passworts und die Fernsteuerung des Computers bewirkt.
Es kann vorkommen, dass der Kunde eine E-Mail-Nachricht erhält, welche die Graphik einer Webseite imitiert. Diese Mail, welche zum Ziel hat, die Daten des Kunden abzufragen, mit welchem die Zahlungen autorisiert werden, lädt den Empfänger der E-Mail ein, einem in der Nachricht enthaltenen Link zu folgen. Dieser Link führt dann allerdings auf eine gefälschte Seite, welche der offiziellen sehr ähnlich ist, sich aber auf dem von einer anderen Person kontrollierten Server befindet. Diese Art von Betrug über Internet, "Phishing" genannt, kann auch über den Versand einer SMS durchgeführt werden.

Zudem gibt es noch unterschiedliche Angriffsformen, die darauf abzielen, den Computer mit einem Schadprogramm zu infizieren (sogenannter Banking Trojan). Dies kann auf verschiedenste Art und Weise, wie z.B. mittels einer E-Mail mit Anhängen, eines in einer E-Mail enthaltenen Links, welcher auf eine infizierende Webseite führt oder einfach über das Aufrufen einer manipulierten Webseite (sogenannter drive-by-download) erfolgen. Üblicherweise wird der Banking Trojan definitiv auf der Festplatte des Computers installiert. Es gibt aber auch andere Arten von Schadprogrammen, die sich im Systemspeicher des Computers befinden und somit auf der Festplatte keine Spuren hinterlassen. Ist das Schadprogramm einmal auf dem Computer aktiv geworden, stehen der kriminellen Organisation verschiedene Techniken zur illegalen Datenabfrage zur Verfügung, wie z.B. das Abfangen der Eingabefelder (Passwort, Mobiltelefonnummer oder Kreditkartendaten), die Darstellung von manipulierten Webseiten, die Blockierung des Zugangs zum Dienst, die Veränderung der Verbindung zwischen Webadresse und IP-Adresse, die Deaktivierung von installierten Antivirusprogrammen, die Veränderung der eingegebenen Daten (z.B. im Zuge einer Überweisung) und sogar die Fernsteuerung des Computers.

Aus diesen Gründen ist es erforderlich, alle vorbeugenden Maßnahmen zu treffen, die die Durchführung von Aufträgen in einer infizierten Umgebung mit potentiellem Risiko eines Schadprogramms vermeiden. Es wird davon abgeraten, Zahlungen im Internet mit einem nicht bekannten Gerät durchzuführen (z.B. Verwendung eines PCs in einem Internetcafé). Wird der Auftrag von einem eigenen elektronischen Gerät aus durchgeführt, ist es erforderlich, vor Zugriff auf die telematischen Dienste zu prüfen, ob das Gerät über ein mit allen Sicherheitspatches aktualisiertes Betriebssystem, über die aktuellsten Versionen der Benutzersoftware (z.B. Acrobat Reader) und über ein ständig aktualisiertes Antivirusprogramm verfügt.

Die genannten Voraussetzungen bilden Mindestvorkehrungen, die für eine wirksame Abwehr von eventuellen Angriffen Dritter unverzichtbar sind. Es ist außerdem wichtig, dass der Kunde mit der Bank uneingeschränkt zusammenarbeitet und, vor allem im eigenen Interesse, dazu beiträgt, derartigen Angriffen vorzubeugen, indem er **folgende Sicherheitsmaßnahmen trifft und Verhaltensregeln befolgt**.

Im Allgemeinen ist es erforderlich,

- ein aktives und stets aktualisiertes Antivirusprogramm und entsprechende Firewall zu installieren;
- Zahlungen im Internet über eigene Geräte durchzuführen, die periodisch kontrolliert werden;
- das eigene Gerät mit einem Passwort von mindestens acht Zeichen, die nicht problemlos der Person zugeordnet werden können, zu schützen und dieses mindestens halbjährlich zu ersetzen;
- regelmäßig die Kontoauszüge und die über die Internetdienste ausgeführten Aufträge zu kontrollieren.

In Bezug auf die Nutzung des Dienstes ist es notwendig:

- die Debitkarte, das Passwort und die Sicherheitselemente mit höchster Sorgfalt zu verwahren und zu verwenden;
- die Debitkarte, das Passwort und die Sicherheitselemente nicht gemeinsam aufzubewahren;
- die Debitkarte, das Passwort und die Sicherheitselemente nicht an Dritte weiterzugeben;
- den Diebstahl, den Verlust, die Zerstörung oder jegliche andere nicht erlaubte Verwendung der Karte und/oder des Passworts zu melden;
- auf die verschiedenen Arten von potentiellen Hackerangriffen zu achten, unter anderem auf gefälschte E-Mails, gefälschte Mitteilungen bezüglich Ablauf von Fristen, die Aufforderung einen bestimmten Link zu verfolgen;
- nur in vertrauenswürdigen Internetshops einzukaufen und auf das geprüfte Gütesiegel (z.B. Trusted Shop) sowie auf das Vorhandensein des Impressums und der Allgemeinen Geschäftsbedingungen und auf deren Inhalt zu achten;

Es wird empfohlen, die erfolgten Zahlungen im Internet mittels des SMS- und/oder E-Mail-Alert Dienstes zu überprüfen.

Zum Zeitpunkt der Zahlung im Internet ist es notwendig:

- zu kontrollieren, ob das Internetprotokoll "https" und das Symbol des Schlosses, welche charakteristisch für eine geschützte Webseite sind und sich vom Internetprotokoll "http" unterscheiden, in der Status- bzw. Adressleiste aufscheinen;
- zu überprüfen, ob die Internetseite, über die die Zahlung vorgenommen wird, die Logos Verified by Visa und MasterCard® Identity Check™ aufweist;
- zu kontrollieren, ob die Seite des Händlers, auf der Sie mit der Debitkarte einkaufen/zahlen möchten, Sie durch Abfrage des persönlichen Passwortes als rechtmäßigen Karteninhaber identifiziert (3D Secure);
- zu kontrollieren, ob während des Zahlvorgangs der Erkennungssatz angezeigt wird und ob er jenem entspricht, der von Ihnen bei der Registrierung erstellt wurde (erscheint nur, wenn der Verkäufer 3D Secure unterstützt);
- Zahlungen auf Seiten zu vermeiden, die das vorgenannte Sicherheitssystem nicht unterstützen bzw. im Falle einer Zahlung zusätzliche Achtsamkeit und Vorsicht walten zu lassen;
- sich nach anderen Bestellmöglichkeiten (z.B. per Telefon oder Fax) zu erkundigen, wenn keine Verschlüsselung der Seite angeboten wird;
- die Zahlung nicht durchzuführen bzw. abzubrechen und die Bank umgehend zu informieren - auch über die Grüne Nummer, welche auf der Webseite veröffentlicht ist - falls Unregelmäßigkeiten oder mangelnde Funktionstüchtigkeit des Systems festgestellt werden;
- nach Ausführung der Zahlung die Seite zu verlassen.

Bei Verlust oder Diebstahl der Debitkarte ist es erforderlich:

- dass Sie unverzüglich die Sperre der Debitkarte über die Sperrnummer beantragen und den Verlust der nächsten Polizeidienststelle melden;
- dass Sie die Polizeimeldung bei Ihrer Bank abgeben, damit diese eine Ersatzkarte anfordern kann.