JOKER ONLINE MASTERCARD®

Anleitung zur Nutzung und Verwaltung Ihrer Online-Karte

1. Zweck und Geltungsbereich

Dieses Dokument erläutert, wie Sie die Joker Online Mastercard® beantragen, aktivieren, darauf zugreifen, sie nutzen sowie ihre Nutzung beenden können, und wie Sie Unterstützung dazu erhalten. Bei dem Produkt handelt es sich um eine virtuelle Prepaid-Mastercard für Online-Einkäufe. Es handelt sich nicht um ein Verbraucherkreditprodukt.

2. Servicekanäle und Verfügbarkeit

Kanal	Verwendungszweck	Verfügbarkeit	Zugang
Internetbanking / Online-Kundenkonto	Registrierung und Aktivierung; Anmeldung; Guthaben und Transaktionen einsehen; Transaktionsbelege herunterladen; persönliche Daten verwalten; Guthaben aufladen; höhere Limits beantragen; Kartendaten abrufen.	Die Website ist für die eigenständige Online-Nutzung vorgesehen. Jede Funktion steht technisch an jedem Tag des Jahres rund um die Uhr zur Verfügung, vorbehaltlich geplanter Wartungsarbeiten, Ausfälle, Sicherheitsmaßnahmen und Annahmeschlusszeiten für die Verarbeitung.	https://www.jokerkartenwelt.bankdimare.com/ und /Account/Login
Kundenservice / schriftliche Kontaktaufnahme	Anfragen, Anliegen zur Karte, Betrugsverdacht, Beschwerden und allgemeine Unterstützung.	Montag - Freitag: 09:00 - 18:00 Uhr (außer an gesetzlichen Feiertagen in Deutschland) Samstag geschlossen Sonntag geschlossen	Kundenservice und Kontakt-Links auf der Produktwebsite: jokercard@bankdimare.com

3. Beantragung und Aktivierung der Karte

1. Kaufen Sie die Joker Online Mastercard® bei einem teilnehmenden Einzelhändler, beispielsweise Netto Marken-Discount oder Kodi.

2. Rufen Sie die Produktwebsite auf und wählen Sie „Karte aktivieren“ aus oder verwenden Sie die mit dem Produkt bereitgestellte Registrierungsseite.
3. Geben Sie die erforderlichen Registrierungsdaten ein und erstellen Sie Ihre Zugangsdaten. Sie müssen mindestens 18 Jahre alt sein.
4. Schließen Sie die Aktivierung und die Identitätsprüfung ab. Die Verifizierung ist erforderlich, bevor die Karte aufgeladen und für Online-Einkäufe verwendet werden kann.
5. Nach erfolgreicher Registrierung werden die Kartendaten aus Sicherheitsgründen teilweise auf der Website und teilweise per SMS an die registrierte Mobiltelefonnummer übermittelt.

4. Zugriff auf das Online-Konto und dessen Nutzung

Melden Sie sich mit Ihrer registrierten E-Mail-Adresse oder Mobiltelefonnummer und Ihrem Passwort an. In Ihrem persönlichen Konto können Sie:

- das verfügbare Guthaben prüfen;
- die Karte mit den unterstützten Methoden aufladen;
- Transaktionen einsehen und Transaktionsinformationen als PDF herunterladen;
- persönliche Daten unter „Einstellungen“ verwalten;
- eine Erhöhung der geltenden Kartenlimits beantragen; und
- Kartendaten unter Einhaltung des Sicherheitsverfahrens für das Produkt und gegebenenfalls gegen eine Gebühr abrufen.

Einen Online-Einkauf tätigen

Verwenden Sie die Kartennummer, das Ablaufdatum, den Namen des Karteninhabers und den CVV bei einem Online-Händler, der Mastercard akzeptiert. Es muss ausreichend aufgeladenes Guthaben vorhanden sein, auch zur Deckung etwaiger Gebühren. Die Karte ist virtuell: Sie ist nicht für Bargeldabhebungen oder Einkäufe an physischen Verkaufsstellen vorgesehen.

Guthaben aufladen und Limits

Die Karte kann nach erfolgreicher Verifizierung per Aufladekarte oder Banküberweisung aufgeladen werden. Informieren Sie sich stets auf den aktuellen Seiten zu Gebühren und Limits, bevor Sie eine Aktion durchführen. Die für das Produkt geltenden Limits und Gebühren können sich ändern. Die vertraglichen Informationen haben Vorrang vor dieser Anleitung.

5. Hilfe, Anfragen und Serviceunterbrechungen

Wenn eine Online-Aktion nicht funktioniert:

1. Prüfen Sie, ob die Website-Adresse korrekt ist und Ihre Internetverbindung sowie Ihr Browser funktionieren;
2. Lösen Sie eine Zahlung oder Aufladung nicht wiederholt aus, wenn das Ergebnis unklar ist;
3. Prüfen Sie die Kontotransaktionen und ausstehenden Vorgänge;
4. Nutzen Sie den verifizierten Kundenservicekanal und geben Sie das Datum, die ungefähre Uhrzeit, die versuchte Aktion und etwaige Fehlermeldungen ohne vertrauliche Informationen an;
5. Senden Sie Ihr Passwort, Ihre vollständige Kartennummer, den CVV oder einen einmaligen Sicherheitscode niemals per gewöhnlicher E-Mail.

Geplante Wartungsarbeiten, ungeplante Ausfälle, Sicherheitsmaßnahmen, Unterbrechungen im Kartensystem oder in Zahlungssystemen sowie Abhängigkeiten von Drittanbietern können Funktionen vorübergehend beeinträchtigen. *Hinweis: Für die Website oder ihre einzelnen Dienste steht keine gesonderte Statusseite zur Verfügung. Bei einem*

Ausfall oder einer Serviceunterbrechung können Sie daher keine Statusseite aufrufen, um zu prüfen, welche Dienste betroffen sind, um aktuelle Informationen zur Störung zu verfolgen oder eine voraussichtliche Wiederherstellungszeit zu erfahren.

6. Betrugsverdacht oder nicht autorisierte Aktivitäten

1. Brechen Sie die Transaktion oder Sitzung ab, falls sie noch läuft.
2. Geben Sie Passwörter, den CVV, Kartendaten oder SMS-/Einmalcodes an niemanden weiter.
3. Melden Sie sich ausschließlich über die offizielle Website an, prüfen Sie die jüngsten Aktivitäten und ändern Sie Ihr Passwort, wenn Sie vermuten, dass Ihre Zugangsdaten kompromittiert wurden. Wenden Sie sich auch an die Bank, wenn Sie Bedenken wegen nicht autorisierter Aktivitäten mit Ihrer Karte haben.
4. Übermitteln Sie nur die angeforderten Informationen über einen authentifizierten oder zugelassenen Kanal. Bewahren Sie relevante Nachrichten, Händlerangaben und Zeitstempel der Transaktionen auf.
5. Befolgen Sie die Anweisungen der Bank zur Sperrung bzw. zum Ersatz der Karte, zur Beanstandung von Transaktionen und gegebenenfalls zur Erstattung einer Anzeige bei der Polizei.

PHISHING-WARNUNG
Geben Sie Passwörter und PINs niemals an andere Personen weiter, auch nicht an Personen, die behaupten, Mitarbeitende von Bank DiMare Limited zu sein. Bank DiMare Limited wird ihre Kunden NIEMALS nach solchen Informationen fragen. PINs und Passwörter sind persönlich und sollten ausschließlich der jeweiligen Person bekannt sein.

7. Sicherheit und operationelle Resilienz

Zu den Schutzmaßnahmen gehören ein authentifizierter Online-Zugang und die getrennte Übermittlung der Kartendaten über die Website und die registrierte Mobiltelefonnummer. „Wir unterhalten angemessene technische, organisatorische und sicherheitsbezogene Maßnahmen, die darauf ausgelegt sind, Kundengelder, personenbezogene Daten und Zahlungstransaktionen vor unbefugtem Zugriff, Betrug, Cyberbedrohungen und Betriebsunterbrechungen zu schützen."

Zu den Sicherheitsmaßnahmen gehören, soweit anwendbar:

- Starke Kundenauthentifizierung (SCA) für den Kontozugriff und elektronische Zahlungsvorgänge.
- Verschlüsselung von Kundendaten bei der Übertragung und Speicherung.
- Kontinuierliche Überwachung von Transaktionen und Systemen zur Erkennung von Betrug, verdächtigen Aktivitäten und Cybersicherheitsbedrohungen.
- Sichere Benutzerauthentifizierung, einschließlich Multi-Faktor-Authentifizierung, soweit erforderlich.
- Zugriffskontrollen und Funktionstrennung zum Schutz sensibler Systeme und Daten.
- Regelmäßige Sicherheitstests, Schwachstellenbewertungen und Penetrationstests.
- Verfahren für das Vorfallmanagement zur Erkennung, Eindämmung, Untersuchung und Behebung von Betriebs- und Sicherheitsvorfällen.
- Vorkehrungen zur Geschäftsfortführung und Notfallwiederherstellung, die darauf ausgelegt sind, die Verfügbarkeit und Wiederherstellung kritischer Dienste bei Störungen sicherzustellen.
- Management von Drittparteirisiken und Überwachung der Dienstleister, die das Kartenprogramm und die Online-Plattform unterstützen.

Die Bank setzt Maßnahmen um, die ein hohes Maß an Sicherheit und Resilienz gewährleisten sollen. Kunden sollten jedoch ebenfalls angemessene Vorkehrungen zum Schutz ihrer Sicherheitsmerkmale treffen, und die Bank unverzüglich über jeden Verdacht auf eine nicht autorisierte Nutzung, versuchten Betrug oder möglichen Sicherheitsvorfall.

Die Bank unterhält ein Rahmenwerk für das IKT-Risikomanagement und die operationelle Resilienz, das auf die Einhaltung geltender gesetzlicher und aufsichtsrechtlicher Anforderungen ausgelegt ist, einschließlich PSD2, DORA, datenschutzrechtlicher Vorschriften und einschlägiger aufsichtsrechtlicher Leitlinien.

8. Personenbezogene Daten und Datenschutzbeauftragter

Personenbezogene Daten müssen gemäß der Verordnung (EU) 2016/679 (DSGVO), dem geltenden maltesischen Datenschutzrecht und den aktuellen Datenschutzhinweisen von Bank DiMare verarbeitet werden. Die Datenschutzerklärung finden Sie hier.

Die Bank verarbeitet personenbezogene Daten, um ihre Prepaid-Kartendienstleistungen bereitzustellen und zu verwalten, gesetzliche und aufsichtsrechtliche Verpflichtungen zu erfüllen, Betrug zu verhindern, Risiken zu steuern und ihre Dienstleistungen zu verbessern. Weitere Informationen zu den Kategorien der verarbeiteten personenbezogenen Daten, den geltenden Rechtsgrundlagen, den Empfängern und der Übermittlung personenbezogener Daten, den Aufbewahrungsfristen, den Sicherheitsmaßnahmen, Ihren datenschutzrechtlichen Rechten, Ihrem Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde sowie den Kontaktdaten, über die Sie Ihre Rechte ausüben oder datenschutzbezogene Fragen stellen können, finden Sie in der Datenschutzerklärung auf der Website.

KONTAKT ZUM DATENSCHUTZBEAUFTRAGTEN UND BEI DATENSCHUTZVERLETZUNGEN
Der Datenschutzbeauftragter Ansprechperson von Bank DiMare ist Vincent Valletta. Sie können ihn direkt über data.officer@bankdimare.com anschreiben. Melden Sie jeden Verdacht auf eine Verletzung des Schutzes personenbezogener Daten unverzüglich. Stellen Sie ausreichende Informationen bereit, damit die Bank den Vorfall erkennen und begrenzen kann, übermitteln Sie jedoch keine unnötigen sensiblen Daten.

9. Beendigung der Nutzung des Dienstes

Wenn Sie Ihre Karte nicht mehr nutzen und/oder das Produkt kündigen möchten:

1. Stellen Sie die Nutzung der Karte ein und kündigen Sie alle damit verknüpften Vereinbarungen mit Händlern über wiederkehrende Zahlungen.
2. Prüfen Sie ausstehende Transaktionen und laden Sie alle benötigten Transaktionsbelege herunter.
3. Kontaktieren Sie den Kundenservice über den verifizierten Kanal und beantragen Sie die Kontoschließung bzw. Kündigung gemäß den Allgemeinen Geschäftsbedingungen.
4. Erkundigen Sie sich, wie ein etwaiges Restguthaben zurückerstattet wird. Die Kündigung selbst ist kostenlos; für die Überweisung des Restguthabens auf ein Bankkonto kann jedoch eine Gebühr anfallen. Informieren Sie sich auf der aktuellen Gebührenseite.
5. Durchlaufen Sie alle von der Bank verlangten Prüfungen zur Identität, Betrugsprävention oder Kontoschließung.
6. Bewahren Sie die Bestätigung der Kontoschließung auf. Gehen Sie nicht davon aus, dass das Konto durch das Löschen von Browserdaten oder dadurch geschlossen wird, dass Sie sich nicht mehr anmelden.

10. Kontaktverzeichnis

Anliegen	Verifizierter Kontaktweg	Verfügbarkeit
Online-Konto und Produktinformationen	https://www.jokerkartenwelt.bankdimare.com/	Zugriff auf die Website; die Verfügbarkeit der Funktionen muss bestätigt werden Dies steht rund um die Uhr zur Verfügung, außer bei Wartungsarbeiten oder ungeplanten Ausfällen.
Anmeldung	https://www.jokerkartenwelt.bankdimare.com/Account/Login	Online; vorbehaltlich Verfügbarkeit
Kundenservice	https://www.jokerkartenwelt.bankdimare.com/customer-support	Montag - Freitag: 09:00 - 18:00 Uhr Samstags, sonntags und an gesetzlichen Feiertagen in Deutschland: geschlossen
Betrugsnotfall / Kartensperrung	https://www.jokerkartenwelt.bankdimare.com/Account/ChangeCardStatus	Online; rund um die Uhr, an 365 Tagen im Jahr
Datenschutzbeauftragter / Vorfall im Zusammenhang mit personenbezogenen Daten	data.officer@bankdimare.com	Montag - Freitag: 09:00 - 18:00 Uhr Samstags, sonntags und an gesetzlichen Feiertagen in Malta: geschlossen
Beschwerden	https://www.jokerkartenwelt.bankdimare.com/Complaints	Die Bank sendet Ihnen innerhalb von zwei (2) Arbeitstagen nach Eingang Ihrer Beschwerde eine schriftliche Eingangsbestätigung. Die Bank unternimmt alle angemessenen Schritte, um die Beschwerde innerhalb von fünfzehn (15) Arbeitstagen zu klären. Ist dies nicht möglich, wird der Kunde entsprechend informiert und erhält eine Angabe dazu, wann voraussichtlich mit einer Klärung zu rechnen ist.