JOKER ONLINE MASTERCARD®

Instructions for Using and Managing Your Online Card

1. Purpose and scope

This document explains how to apply for, activate, access, use and discontinue the Joker Online Mastercard®, and how to obtain assistance regarding it. The product is a prepaid virtual Mastercard intended for online purchases. It is not a consumer-credit product.

2. Service channels and availability

Channel	What it is used for	Availability	How to access
Internet banking / online customer account	Register and activation; sign in; view balance and transactions; download transaction records; manage personal details; load funds; request higher limits; retrieve card details.	The website is intended for online self-service. Each feature is technically available 24 hours a day, every day of the year, subject to planned maintenance, outages, security controls and processing cut-offs.	https://www.jokerkartenwelt.bankdimare.com/ and /Account/Login
Customer support / written contact	Queries, card concerns, suspected fraud, complaints and general assistance.	Monday - Friday: 09:00 - 18:00 (except Public Holidays in Germany) Saturday closed Sunday closed	Customer Support and Contact Us links on product website: jokercard@bankdimare.com

3. Applying for and activating the card

1. Purchase Joker Online Mastercard® from a participating retailer, such as Netto Marken-Discount and Kodi.
2. Go to the product website and select “Karte aktivieren” / Activate Card, or use the registration page supplied with the product.
3. Enter the requested registration information and create your credentials. You must be at least 18 years old.
4. Complete activation and identity verification. Verification is required before the card can be loaded and used for online purchases.

5. After successful registration, card details are provided partly on the website and partly by SMS to the registered mobile number as a security measure.

4. Accessing and using the online account

Sign in using your registered email address or mobile number and password. Within the personal account, you can:

- Check the available balance;
- Load funds onto the card using supported methods;
- View transactions and download transaction information as a PDF;
- Manage personal information under Settings;
- Request an increase to applicable card limits; and
- Retrieve card details, subject to the product's security process and any applicable fee.

Making an online purchase

Use the card number, expiry date, cardholder name and CVV at an online merchant that accepts Mastercard. Sufficient loaded balance must be available, including to cover any applicable fees. The card is virtual: it is not intended for cash withdrawals or physical point-of-sale purchases.

Loading funds and limits

The card can be loaded by top-up card or bank transfer after successful verification. Always consult the current Fees and Limits pages before acting. Product limits and fees can change, and the contractual information takes precedence over this guide.

5. Help, queries and service interruptions

If an online action does not work:

1. Check that the website address is correct and that your internet connection and browser are functioning;
2. Do not repeatedly submit a payment or top-up if the result is unclear;
3. Review account transactions and pending items;
4. Use the verified customer-support channel and provide the date, approximate time, action attempted and any non-sensitive error message;
5. Never send your password, full card number, CVV or one-time security code by ordinary email.

Planned maintenance, unplanned outages, security controls, scheme or payment-system interruptions, and third-party dependencies may temporarily affect features. *Note: No dedicated service-status page is available for the website or its individual services. During an outage or service interruption, you will therefore not be able to consult a status page to check which services are affected, follow updates on the disruption or find an estimated restoration time.*

6. Suspected fraud or Unauthorised activity

1. Stop the transaction or session if it is still in progress.
2. Do not reveal passwords, CVV, card details or SMS/one-time codes to anyone.
3. Sign in only through the official website, review recent activity and change your password if compromise is suspected. You should also contact the Bank if concerned with unauthorized activity with your card.
4. Provide only the information requested through an authenticated or approved channel. Keep relevant messages, merchant details and transaction timestamps.

5. Follow the Bank's instructions regarding card blocking/replacement, disputed transactions and any police report.

PHISHING WARNING
Never divulge passwords and PIN numbers to anyone, including persons purporting to be employees of Bank DiMare Limited. Bank DiMare Limited will NEVER request this kind of information from its customers. PIN numbers and passwords are personal and should be known by the owner only.

7. Security and operational resilience

Safeguards include authenticated online access and split delivery of card details between the website and the registered mobile number. "We maintain appropriate technical, organisational and security measures designed to protect customer funds, personal data and payment transactions against unauthorised access, fraud, cyber threats and operational disruption.

Security controls include, where applicable:

- Strong Customer Authentication (SCA) for account access and electronic payment transactions.
- Encryption of customer data during transmission and storage.
- Continuous monitoring of transactions and systems to detect fraud, suspicious activity and cybersecurity threats.
- Secure user authentication, including multi-factor authentication where required.
- Access controls and segregation of duties to protect sensitive systems and data.
- Regular security testing, vulnerability assessments and penetration testing.
- Incident management procedures for the identification, containment, investigation and remediation of operational and security incidents.
- Business continuity and disaster recovery arrangements designed to ensure the availability and recovery of critical services during disruptions.
- Third-party risk management and oversight of service providers supporting the card programme and online platform.

While the Bank implements measures intended to maintain a high level of security and resilience, customers should also take reasonable steps to protect their security credentials and notify the Bank immediately of any suspected unauthorised use, fraud or security incident.

The Bank maintains a framework for ICT risk management and operational resilience designed to comply with applicable legal and regulatory requirements, including PSD2, DORA, data protection legislation and relevant regulatory guidance.

8. Personal data and the Data Protection Officer

Personal data must be handled in accordance with Regulation (EU) 2016/679 (GDPR), applicable Maltese data-protection law and the current Bank DiMare privacy notice. The Privacy Policy can be found here.

The Bank processes personal data for the purposes of providing and administering its prepaid card services, complying with legal and regulatory obligations, preventing fraud, managing risk, and improving the Bank's services.

Further information regarding the categories of personal data processed, the applicable legal bases, recipients and transfers of personal data, retention periods, security measures, your rights under data protection law, your right to lodge a complaint with the competent supervisory authority, and the contact details through which you may exercise your rights or raise privacy-related queries is available in the Privacy Policy on the website.

DPO AND BREACH CONTACT

Bank DiMare's Data Protection Officer is Vincent Valletta who can be contacted directly at data.officer@bankdimare.com. Report any suspected personal-data breach promptly. Provide enough information to help the Bank identify and contain the incident, but do not send unnecessary sensitive data.

9. Discontinuing use of the service

If you wish to stop using your card and/or terminate the product:

1. Stop using the card and cancel any recurring merchant arrangements linked to it.
2. Review pending transactions and download any transaction records you require.
3. Contact Customer Support using the verified channel and request closure/termination in accordance with the Terms and Conditions.
4. Ask how any remaining balance will be returned. Cancellation itself is not charged, but transferring the remaining balance to a bank account may carry a fee. Check the current Fees page.
5. Complete any identity, fraud-prevention or account-closure checks requested by the Bank.
6. Retain closure confirmation. Do not assume that deleting browser data or ceasing to log in closes the account.

10. Contact directory

Purpose	Verified route	Availability
Online account and product information	https://www.jokerkartenwelt.bankdimare.com/	Website access; feature availability requires confirmation This is available 24/7 except in case of maintenance or unplanned outages.
Login	https://www.jokerkartenwelt.bankdimare.com/Account/Login	Online; subject to availability
Customer support	https://www.jokerkartenwelt.bankdimare.com/customer-support	Monday - Friday: 09:00 - 18:00 Saturdays, Sundays and German Public Holidays: Closed
Emergency fraud/card blocking	https://www.jokerkartenwelt.bankdimare.com/Account/ChangeCardStatus	Online; 24/7/365
Data Protection Officer / personal-data incident	data.officer@bankdimare.com	Monday - Friday: 09:00 - 18:00 Saturdays, Sundays and Maltese Public Holidays: Closed

Complaints	https://www.jokerkartenwelt.bankdimare.com/Complaints	The Bank will send a written acknowledgement of receipt of your complaint within two (2) working days of receiving it. The Bank will take all reasonable steps to resolve the complaint within fifteen (15) working days. Where this is not possible, the customer will be informed accordingly and provided with an indication of when the matter is expected to be resolved.