CITIZENCREDIT
CO-OPERATIVE BANK LTD
(A Scheduled Multi-State Bank)

Best Practices to secure Debit/ Credit Cards

✓ Download our mobile app CCB Mobile from Playstore to **Block your Rupay Debit card** to avoid fraudulent transactions and **Unblock the card only while using it**.

✓ While making online transactions with credit/debit card, **user must only use card at established and reputed sites** as there are less chances of card fraud on a reliable website.

✓ Always ensure that the **address of the website** where transactions to be done, **starts with "https://" and not "http://"**

✓ Always perform online financial transactions from a **secure computer system updated with latest security updates/patches**, anti-virus and anti-spyware software and personal firewall.

✓ **Change** your card **PIN** (Personal Identification Number) **periodically.**

✓ **Do not disclose any personal information online** like your date of birth, billing address, etc., on the Internet because that can be misused to unlock your account password.

✓ **Never share card details over the phone** or with anyone in person as it is easier way for others to get access to your credit card confidential information and make the online transactions.

✓ **Do not send card and account details through e-mail** to prevent from malicious use by others

✓ **Regularly check account statement related to the card** and notify the card company in case of any discrepancy.

✓ **Ensure whether your card is enabled/disabled for International use**, disable if it is not necessary. Check with your bank for any additional options such as restricting the usage of cards on different payment channels viz., PoS/ATM/E-Commerce or Domestic/International usage time-to time through bank’s own interface/app.

✓ **Never leave your card unattended.**

✓ **Keep card help line** phone numbers with you **for any kind of assistance.**

✓ Download our mobile app CCB mobile from Playstore to **Block your Rupay Debit Card** to avoid fraudulent transactions and **Unblock the card only while using it**.

Best Practices for users

- ✓ **Ensure that you have your strong passwords** for all accounts. Use of non-dictionary words is also advised. Do not share your password with others.
- ✓ **Shop with companies/websites you know**. If the company is unfamiliar, investigate their authenticity and credibility. Conduct an internet search for the company/website name.
- ✓ Websites having click and wrap agreements, privacy policies, **by reading these policies one knows about the uses of information by websites**. Websites do sell this information. Some major social networking sites use or sell information (not personal data) about you to display advertising or other information they believe might be useful to you. Therefore, it is advised that one should read the privacy policies of websites before getting into it.
- ✓ **Minimum amount of information should only be disclosed** such as screen name should not give a clue to the identity of the user.
- ✓ **Avoid posting personal information** such as your address, phone numbers, e-mail address, license number, Aadhar No, birth date, birth place, location for any given day, school's name of kids, and family details.
- ✓ While posting photos, **avoid providing details** of where you live, work or go to college. Also, do not post photos depicting negative or inappropriate behaviours, remember you are writing your own history and it will continue to exist in the cyber world.
- ✓ **Look for encryption**, before making any sort of digital payment, look for signs that show whether the website is encrypted or not. To do this, look for two things: the trusted security lock symbols and the extra "s" at the end of http in the URL or web address bar.
- ✓ **Avoid connecting with strangers** since you don't know that your information could be used in a way you didn't intend.
- ✓ **Verify emails and links in emails** you supposedly get from your social networking site. These are often designed to gain access to your user name, password, and ultimately your personal information. These mails could be phishing emails too. Do not click on any links without identifying the genuineness. In case the link seems to be a genuine website, do not click, copy and paste in the address bar
- ✓ Keep your **anti-virus and software updated**.
- ✓ **Own your online identity** - Check privacy and security settings and set it to your comfort level for information sharing
- ✓ **Secure your login** - Use strongest authentication tools wherever available and applicable, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are always not enough to protect key accounts like email, banking and e-wallets.