The Baramati Sahakari Bank Ltd

Bhigwan Road, Jalochi, Baramat Dist.Pune
413102

1. Secure use of Credit/Debit cards

New technologies have simplified and smoothed business-to-customer experiences with mobile payments, e-wallets, and payment cards. As e-commerce expands, opportunities for fraudulent misuse of payment networks and data theft grow right alongside.

A **payment card** is a device that enables its owner (the cardholder) to make a payment by electronic funds transfer. The most common types of payment cards are **credit cards and debit cards**. A payment card is electronically linked to an account or accounts belonging to the cardholder. These accounts may be deposit accounts or loan or credit accounts, and the card is a means of authenticating the cardholder.

Best Practices for Users to remain safe:

- 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 in order 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 Bank 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.

2. Secure use of ATM

In order to use the ATM secure and safely, following are the best practices to be followed.

a. **Observe the ATM**: Generally ATM can be susceptible to fraud. It is suggested to look at an ATM to make sure a card slot is "legitimate and not tacked on" and there is no hidden camera or keypad overlay installed. The hidden cameras record customer typing in the number, while the more advanced keypad overlay collects pin number and stores it in the device itself or, similar to the skimmer, it sends the information to another storage device.

b. Use of ATMs:

(i) As far as possible use an ATM which is within Bank premises having proper security.

(ii) Avoid using ATMs which are in isolated places, dimly lit locations or on the streets.

(iii) Not to use the ATM where the card reader slot appears to be tampered with, broken, scratched, damaged, sticky with glue, has extra wiring or loose parts around the slot, difficulty in inserting the card etc. These could be signs of skimming machine having been installed.

c. **Cover the keypad while entering your PIN number:** In the instance when the skimmers are undetectable, customer can easily avoid falling victim by covering the keypad with his/her free hand when he/she enters his/her pin number. Doing this simple step could prevent the criminals from recording customers' PIN numbers if they are using the hidden camera method.

By Chief Information Security Officer
The Baramati Sahakari Bank Ltd.