Advisory to all prepaid card customers to use prepaid cards in a secured manner

- While making transactions at POS and ECOM with Prepaid card, use card at established and reputed merchant and websites as there are less chances of card fraud on a reliable merchant's POS and 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. because that can be misused to unlock your account or reset password.

- Never share card details over the phone or with anyone in person.

- Do not share card details / personal or financial information through e-mail.

- Do not use Public Wi-Fi networks for accessing email, online banking and Prepaid Card accounts or any other sensitive data for that matter.

- Regularly check card statement and notify the Bank in case of any discrepancy.

- Block your prepaid card temporarily, when not in use by logging on to Prepaid Customer Portal (https://prepaid.onlinesbi.com).

- Never leave your card unattended.

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

- Approach local law enforcement agency for reporting of fraud in addition to Banks.

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.

- It is advised that one should read the privacy policies of websites before getting into it.

- Minimum amount of information should only be disclosed and clue to the identity of the user should not be given.

- Avoid posting personal information such as your address, phone numbers, e-mail address, license number, Aadhaar 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 behaviors, 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 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.

- 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.

Procedure in cases of identity theft

- Ensure that you have changed your passwords for all accounts. Contact your banks/wallets to freeze your accounts so that the offender is not able to access your financial resources

- Get your cards blocked and find out that if there have been any unauthorized transactions. Close accounts so that future transactions are denied

- Approach local law enforcement agency for reporting of fraud in addition to banks/wallets

- If your personal information has been stolen through a banks/e-wallets/intermediaries data breach (when an offender hacks into a database of accounts to steal information), you will likely be contacted by the banks/e-wallets/intermediaries whose data was compromised with additional instructions, as appropriate.

Do's and Don'ts of Prepaid Card Transactions.

Do's

- Conduct your ATM transactions in complete privacy, never let anyone see you entering your Personal Identification Number (ATM Password)

- After completion of transaction ensure that welcome screen is displayed on ATM screen

- Ensure your current mobile number is registered with the bank so that you can get alerts for all your transactions

- Beware of suspicious movements of people around the ATM or strangers trying to engage you in conversation

- Check if the card given to you by the merchant after completion of the transaction is your card

- Look for extra devices attached to the ATMs that looks suspicious

- Inform the bank if the Prepaid card is lost or stolen, immediately, report if any unauthorized transaction

- Check the transaction alert SMSs and bank statements regularly

- If cash is not dispensed and ATM does not display "cash out" please report to the Bank on the number mentioned in the Notice Board

- Memorize your PIN number

- Always visit your Bank's website by typing the URL in the address bar, i.e. type https://prepaid.onlinesbi.com for accessing SBI Prepaid Cards website

- Bank never asks to verify your account information through an e-mail/SMS.

Don’ts

- Do not write your PIN on the card

- Do not take help from strangers or handover your card to anyone for using it

- Do not disclose your PIN to anyone, including bank employees and family members

- Do not allow the card to go out of your sight when you are making a payment

- Avoid speaking on the mobile phone while you are transacting

- Do not click on any link that has come through an email from an unknown source. It may contain malicious code or could be a 'Phishing Attack'

- Do not provide your personal sensitive information on a webpage which have come up as a pop-up window

- Never provide your login or transaction passwords over the phone or in response to any unsolicited request over email/SMS/call

- Always remember that your Passwords, PINs, Card Numbers, etc. are strictly confidential and are not known even to employees/service personnel of the Bank. You should therefore never divulge such information even if asked for.