CYBER SECURITY MEASURES FOR CUSTOMERS

Precautions While Using ATM/Debit Card:

- Always keep card in your custody
- Sign on the back of the new card as soon as you get it.
- It is recommended that 3-digit CVV2 number present at the back of the ATM/debit card should be scratched to make it unreadable and memorized by the user.
- Cancel any unwanted or expired cards by contacting the card-issuer and cutting up the unwanted or expired card in at least two pieces.
- In case card is lost, immediately contact the concerned branch or customer care center (1800-180-7777(toll free)) to hotlist user card, to avoid any misuse of card by anyone.

.

Suggestions For Handling PIN:

- While receiving the PIN please ensure that the envelope and the security document are not tampered with. In case of tampering contact call center immediately and do not use PIN.
- Do not keep the PIN along with the card. Always memorize the PIN and destroy the PIN mailer.
- Change ATM/ Debit card PIN through PNB ATM, immediately at first use.
- Change PIN number at frequent intervals or when it seems to have been compromised/ shared.
- Do not choose a PIN that can be obviously associated with user- e.g. telephone number, birthday, street number or popular sequence numbers (1111, 1234 etc). Choose a random combination of number.
- Never write down or record user PIN or other security information on card or at a place easily accessible by others.
- Do not reveal user PIN or any security information on card to anyone. Neither the Bank nor any Authorized Agencies will ever ask you to disclose your PIN. In case of any such happening please note the particulars of the caller and report to the call center executive (1800-180-7777(toll free)) and cyber crime agencies.

Precautions While Using At ATMs:

- Do not conduct any transaction on ATM, if you found the surroundings suspicious. Look out for suspicious devices on ATMs or pinpads.
- Do not accept help from strangers/guards and never allow yourself to be distracted
- Always ensure while doing transactions, no one is present around ATM machine.
- If there is anything unusual about the ATM machine, or there are signs of tampering of machine, do not use the ATM machine and report to Bank immediately.
- Use your body to block the view of user transaction. Especially while entering PIN and withdrawing the cash.
- While paying the utility bills on ATM check the transactions details with the billed amount, customer ID on original bill. Keep the transaction slip safe so that it can be referred to if the paid amount appears as arrears in next billing cycle.
- Don`t discard receipts and mini-statements or balance inquiry slips which contain important information. User gets a receipt every time user makes an ATM transaction.
- Tear up or preferably shred user cash machine receipt, mini-statement or balance enquiry when disposing them off.
- After completing transaction, remember to take your card back.
- If the ATM machine does not return the card, report its loss immediately to user Bank/branch.

Precautions While Using Cards For Point Of Sale(POS):

- While making payment at POS always ensures that the card is swiped in your presence only.
- Do not share PIN or any security information related details with anyone.

- Always check Debit card when returned after purchase.
- Insist for a copy of the receipt and retain it till the account statement is checked.

Safety Measures For Phishing:

DO`s:

- It is recommended to type the full URL of bank`s website yourself on the web-browser
- Use secured webpage`s URL, i.e. URL should begin with "https".
- Check for padlock icon, a de-facto standard, displayed somewhere on web-browser, representing the site`s security certificate. Click (or double-click) on icon to check the security certificate – address on the certificate conforms to the address in address bar. The certificate should ensure the identity of the website and the current day`s date should be within the validity dates of the certificate.
- Keeps an eye on the transactions happening through your bank account.

DON`Ts:

- Do not respond if you receive spam mail or an e-mail that may appear to have been sent by the bank asking you to click a link for accessing your Internet banking account. Inform the bank immediately about such e-mails.
- Do not click a link in an e-mail message and instant messages from strangers to access internet banking.
- Never share your account credentials through e-mail.
- Bank never asks for user id and password, hence don`t share it with anyone including bank`s call center and branch staff.

Safety Measures For Vishing Scams:

Vishing Scams make use of Voice over Internet Protocol (VoIP), which allows people to talk over their computer lines and messaging on cell phones. Scammers leave the automated message saying the person`s bank account has been compromised, deleted or closed and asked for their account credentials over phone.

- Do not reveal account/card credentials on e-mails/phone/message. Bank does not ask for any such details from their customers
- Immediately inform and seek confirmation from the Bank by calling on Bank`s phone numbers, appearing on Debit card or bankor published on the official website about any such call/message received by you -asking your account/card credentials.

Computer Safety Measures:

- Always protect computer by installing up-to-date antivirus software that is capable of protecting system from viruses and Trojan horses.
- Always log-in computer as a "user" not as "administrator", so that unauthorized software e.g. Trojan does not get installed automatically at your computer.
- Protect computer from malicious Intrusions and attacks by enabling the windows firewall.
- Keep Web browser and operating system up-to-date with software updates.
- Scan system regularly using up-to-date antivirus software for malware, spyware, virus and Trojans.
- Prefer using recent version of web-browser and make sure web browser is set to the highest level of security notification and monitoring.

Safety Measures While Using Debit Cards For Online Shopping/E-Commerce Transactions:

- Be sure of the website address before using the website for online shopping. Always type the website address into the address bar or bookmark the websites that are frequently used.
- Never enter, confirm or update card related details in a pop-up window.
- Shop only from secured and reputed websites- ensure that the security icon, the locked padlock or unbroken key symbol, is appearing in the bottom right of web browser window before sending your card details.

- Click on the security icon to ensure that the retailer has a valid encryption certificate – the address on this certificate should conform to the address on the address bar. The certificate should ensure the identity of the website and the current day`s date should be within the validity dates of the certificate.
- Users must not respond to online offers that require user`s account details "for verification".
- Users must fully aware of any payment commitments that he is entering into, including instructions for a single payment or a series of payments
- It is advised to save the transaction receipts of utility payments on your hard disk which be printed as well. It can be referred to in case of mismatch with Internet transaction history or the already paid bill may reappear in next billing cycle.
- User should register for SMS alerts through ATM/Branch, for receiving alerts of specific transactions done through Debit card.
- The beginning of the retailer`s Internet address will change from `http` to `https` when a purchase is made using a secure connection.
- User must use trusted sites only, for example sites user know or that have been recommended to user or that carry the Trust logo.
- Avoid signing up for junk mail – this may result in pre-filled application forms being sent to an address long after user has moved out..
- If user has any doubts about giving user card details, find another method of payment.
- Keep passwords secret. Some online stores may require user to register with them via user name and password before buying. Online passwords, including, the one, verified by user issuer, should be kept secret from outside parties the same way user protect user Card PIN. Keep the login information safe and secret.
- Never send payment information via email. Information that travels over the Internet (such as email) is not fully protected from being read by outside parties. The most reputable merchant sites use encryption technologies that will protect user private data from being accessed by others as user conduct an online transaction.
- Never click on Hyperlinks within e-mails. If you are sure that the company is genuine then directly type in the URL in the internet browser address bar, or calls the company on a contact number previously verified or known to be genuine.
- Don`t let websites or merchants store the card information. The exchange of encrypted transactions will be better than to allow the storage of identity information on data bases.

For Mobile Banking Users:

DOs:

- Set up password of mobile phone and do not reveal password to anyone.
- Smart Phones with GPRS are vulnerable to virus, so install up-to-date antivirus software in user mobile phone.
- Download and run security updates and patches on user mobile browser. This helps in protection from known possible security problems.
- Install a firewall on mobile handset or enable the same if handset comes with a firewall.
- Remove the temporary files and the cache that were stored in the memory of the phone regularly, as that may contain any sensitive information such as account numbers.
- Clear the browsing history regularly.
- Type in the URL for mobile banking in the mobile browser, instead of clicking on any link. This will ensure access of the authentic website of the bank.
- Delete spam messages/mails.

- Be aware of the potential for fraudulent SMS messages. The Bank will never request or invite customers to logon to its mobile banking service via a SMS message.
- Check that the security padlock on internet browser is "locked" to ensure the connection is secure and protected by SSL. User should also check that the URL starts from `https` and not `http`.
- Avoid performing transactions or applications in public places. This helps in minimizing the risk of security threats such as "shoulder surfing" of mobile banking credentials.
- Keep mobile handset in an auto lock mode to provide additional protection.
- Monitor your account regularly and always keep a record of user transactions.
- While using Wi-Fi access, ensure that adequate security measures have been implemented on mobile handset to protect it against virus and attacks from other Wi-Fi users.
- Switch off the blue tooth function of handset when not in use. This protects from virus attacks .

DON`Ts:

- Do not share mobile banking credentials (user ID, passwords) with anyone.
- Do not share mobile handset with untrustworthy people, to restrict unauthorized access.
- Do not allow others to access your mobile phone before logging out from the sites (banking/financial/shopping) that you are accessing.
- Beware of online offers that require account details for `verification`. Do not reveal any information regarding account such passwords, account number etc.
- Do not leave Mobile banking application session unattended. Always sign off from a session.
- Do not follow any URL in messages that user is not sure about.
- Do not download any file from sites (e.g. applications, games, pictures, music etc.) or any e-mail attachments that you are not sure about.
- Do not download any software without verifying its security and privacy features from the website.
- Do not logon to the mobile banking application from a mobile handset that is shared with other people, as it may be difficult to ensure the handset is free of hacker or spyware.
- Do not save mobile banking credentials like user ID, passwords in the phone`s T9 dictionary. This helps to reduce the risk arising in case mobile phone is lost or stolen.

Helpline: 1800-180-7777(toll free)