CUSTOMER AWARENESS & PROTECTION PROGRAM

Annexure A

Electronic Banking Customer Awareness Program

To ensure security in their e-banking transactions and personal information, customers should be oriented of their roles and responsibilities which, at a minimum, may include the following depending on the nature of instances that need to be prioritized:

1. Wireless Products and Services

a) Secure Password or PIN

- Do not disclose Password or PIN to anyone.
- Do not store Password or PIN on the mobile devise.
- Regularly change password or PIN and avoid using easy-to-guess passwords such as birthdays.

b) Keep personal information private.

- Do not disclose personal information such as address, mother's maiden name, telephone number, bank account number or e-mail address — unless the one collecting the information is reliable and trustworthy.

c) Keep records of wireless transactions.

- Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
- Review and reconcile periodical bank statements for any errors or unauthorized transactions promptly and thoroughly.
- Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
- Immediately notify the bank if there are unauthorized entries or transactions in the account.

d) Be vigilant while initiating or authorizing/ responding to transactions.

- Before doing any transactions or sending personal information, make sure that correct wireless banking number and message format is being used. Beware of bogus or "look alike" SMS messages which are designed to deceive consumers.
- Be particularly cautious while responding to a voice call that claims to be from a bank. Never give any personal information to such a caller.

e) Take special care of your mobile device.

- Do not leave your mobile device unattended. It may be used wrongfully by someone having access to your personal information and/or PIN.

f) Learn by heart and keep handy your account blocking procedures.

In case your mobile phone is snatched / stolen, please immediately proceed with account blocking/theft reporting procedures. For this, you need to familiarize yourself with the procedures to be followed, learn by heart the number provided by your bank for the purpose and either remember or keep handy the information (such as your mobile account number, CNIC number, secret question etc.) you may be required to complete account blocking procedures.

2. Other Electronic Products

a) Automated Teller Machine (ATM) and debit card

- Use ATMs that are familiar or that are in well-lit locations where one feels comfortable. If the machine is poorly lit or is in a hidden area, use another ATM.
- Have card ready before approaching the ATM. Avoid having to go through the wallet or purse to find the card.
- Do not use ATMs that appear to have been tampered with or otherwise altered. Report such condition to the bank.
- Memorize ATM personal identification number (PIN) and never disclose it with anyone. Do not keep those numbers or passwords in the wallet or purse. Never write them on the cards themselves. And avoid using easily available personal information like a birthday, nickname, mother's maiden name or consecutive numbers.
- Be mindful of "shoulder surfers" when using ATMs. Stand close to the ATM and shield the keypad with hand when keying in the PIN and transaction amount.
- If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report the problem to the bank.
- Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM.
- Do not leave the receipt behind. Compare ATM receipts to monthly statement. It is the best way to guard against fraud and it makes record-keeping easier.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.