Mobilink Microfinance Bank

Electronic Banking-Customer Awareness Program

MMBL is committed to protecting your personal and confidential information which you have entrusted in our care. We take the trust you have placed in us very seriously and have created this Awareness & Education Guide to inform you of important information to ensure security of performed E-Banking transactions & to assist you in keeping your information safe. On the same the roles & responsibilities of customers are as following:

1. Wireless Products and Services

a) Secure Password or PIN

- Do not disclose Password or PIN to anyone. Never reveal personal identifying information unless you are sure of how it will be used & why it is acquired?
- Never give out personal information on the phone, through the mail, or over the internet unless you have initiated the contact and you know who you are dealing with?
- Do not store Password or PIN on mobile device.
- Regularly change password or PIN and avoid using easy-to-guess passwords such as birthdays.
- The longer the password, the tougher it is to crack

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.

f) 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 or PIN.
- Delete all information stored on a device before the device changes ownership. Use a "hard factory reset" to permanently erase all content and settings stored on the device.

g) 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, customer needs to be familiar with the procedures to be followed, learn by heart the number provided by bank for the purpose and either remember or keep handy the information (such as your mobile account number, CNIC number, etc.) you may be required to complete account blocking procedures.

2. Other Electronic Products

a) Automated Teller Machine (ATM) & ATM/Debit cards

- 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.
- Be aware of your surroundings when using an ATM, especially at night. Consider having someone accompany you to the ATM when you make transactions after dark.
- 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 authorities.
- 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.
- Be mindful of "shoulder surfers" when using ATMs. Stand close to the ATM and shield the keypad with hand while entering 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.

Internet Banking Security

- Never give out any personal information including User Names, Passwords, CNIC Number or Date of Birth.
- Create difficult passwords which include letters, numbers, and symbols & should be changed frequently.
- Do not use personal information for your user names or passwords, like your CNIC Number, Mobile Number or Date of Birth.
- Avoid using public computers to access your Internet Banking accounts.
- Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate.
- Choose challenge questions carefully to avoid using information that could be obtained by identity thieves or readily guessed by a person with a basic knowledge about the target they are attempting to impersonate.
- Pay attention to the URL (web address) that you are visiting! Fraudulent websites often create misleading web address like https://www.somecompany.com.AnotherWebsite.com/ to trick users of a https://www.somecompany.com/ into believing they are visiting a legitimate site where they have an account when they are really at a password harvesting spoof of the legitimate website. This is a very common trick that scammers use to fool users into divulging passwords to fake copies of real websites!
- Avoid saving passwords to any computer.
- Never leave computers unattended when using online banking services.
- Shred/discard any documents you don't need any more that contain personal information, like bank statements, unused cheques, deposit slips, credit card statements and invoices.
- Do business only with companies that you know and trust, especially online.
- Always "sign out" or "log off" of password protected websites when finished to prevent unauthorized access. Simply closing the browser window may not actually end your session

Lottery / Prize Scheme Scam

- A typical lottery scam begins with a call from unknown number notifying that you have won a large sum of money in a lottery/ prize scheme. Scammers will often use the names of legitimate lottery organizations, thereby trying to make themselves look legitimate. You are usually told to keep the notice secret and to contact a claims agent to validate. After contacting the "agent" you are asked to pay a processing fee or transfer charge so the winnings can be distributed. Of course, you never hear from them again.

Best Practices

- Keep your personal information private and secure.
- Check your account balance regularly.
- Do not access your account from a public location.
- If you suspect suspicious activity, take swift action.
- Be skeptical of email messages, for example, from someone unlikely to send an email such as the IRS.
- Do not open the suspicious emails and do not click on the links.
- Do not use the password auto-save feature on your browser.
- Avoid storing sensitive information on mobile devices.
- Reconcile your bank account on a monthly basis to ensure all transactions that appear on your account are legitimate.
- Sign up for text message alerts to receive information about performed transactions automatically.

**Disclaimer: This is a customer awareness message. The customers of MMBL Bank Ltd. are requested to follow the above mentioned guidelines as the Bank will not be liable in case of any fraud arising from any such incident.