## Customers Security Tips:

### Protecting your Cards

- Never allow anyone else to use your card.
- Keep your card in a safe place - don't allow it to be bent or scratched and keep away from magnetic objects and electronic devices.
- Always destroy cards when they expire by cutting them in half through the magnetic stripe.
- Carefully discard receipts from card transactions and ATMs once you have checked these against your account statement.
- Regularly check that you are still in possession of your card and inform us by calling 01/03-738800 immediately if it is lost or stolen.

### Protecting your Credit Card

- Regularly check your credit card account balance. If you suspect there are fraudulent transactions on your account, call us immediately.
- At work, keep your bag and other personal belongings locked in a cupboard or drawer.
- Give your credit card details when making a purchase only - do not provide them for any other reason.
- Don't give your card number or PIN number over the telephone to 'cold' callers. Only make the telephone transaction when you have initiated the call and you are familiar with the company.
- Never send your credit card number via e-mail.
- When you're overseas, always keep an eye on your card. Don't let your card out of your sight, and never leave cards unattended in a hotel room, at the beach or in a parked car.
- Keep your personal information, including mobile phone number, up-to-date so we can contact you if an unusual transaction is detected.
- To report fraud and other suspicious activity, call us or visit any branch.

### Protecting your Card Pin

- Memorize your PIN - never write it down anywhere.
- Never disclose your PIN to any other person, including any additional cardholders, family members, bank staff or Police. Remember bank staff or Police will never ask for this information.
- Don't let anyone else see your PIN when you enter it at an ATM or POS terminal.
- If you become aware of, or suspect your card or your PIN has been lost, stolen or disclosed, you should notify us by calling 01/03-738800 immediately or visit any Branch.

### Online Shopping:

- When using your card to purchase on-line, look for reputable Internet stores. If you are unsure, request more information from them about the company and the goods and services they are selling.
- Check that the on-line merchant or store has a return and refunds policy.
- Always use a secure browser connection when entering credit card details on-line. Check that a locked padlock or unbroken key symbol is shown in the bottom right of your browser window or the site has a URL that starts with "https".
- If you have to use a password to access a service, make sure this isn't easily identifiable and don't disclose it to anyone.
- If you make an on-line purchase, print out a copy of the transaction for your records. This will make it easier to check against your credit card statement
- Look for actual phone numbers or physical addresses for the company on the site if you're unsure whether a website is genuine or reputable.
- Turn off automatic connection feature for wireless services in mobile device such as Wi-Fi, Bluetooth, NFC, etc..
- Minimize the amount of data stored and avoid storing sensitive data on your mobile devices.
- Ensure all data have been completely erased before disposal or re-use of the mobile device.
- Set up a remote data wiping feature if available.
- Update your device's mobile operating system because it's likely that older versions are insecure.
- Protect your home WiFi (wireless) network if you are using one.
- Don’t use unsecured WiFi (wireless) networks either public or private.

**Using ATMs**

- Observe your surroundings before using an ATM. If the machine is obstructed from view or poorly lit, visit another ATM.
- Take a friend with you - especially at night.
- Have your card out and ready to use.
- Shield/ Hide the screen and keyboard so anyone waiting to use the ATM cannot see you enter your PIN or transaction amount.
- Put your cash, card and receipt away immediately. Count your money later, and always keep your receipt.
- If you see anyone or anything suspicious, cancel your transaction and leave immediately.
- If anyone follows you after making a transaction, go to a crowded well-lit area and call the Police.

- When using an enclosed ATM that requires your card to open the door, avoid letting strangers follow you inside.
- Do not leave your car unlocked or engine running when you get out using an ATM.
- While many ATM's are available 24 hours a day, some may be open only during local business hours. To be on the safe side, plan your withdrawals ahead of time.
- Look out for unfamiliar fixtures on ATMs. These fixtures will not appear to be part of the normal ATM, or are attached to the slot where you insert your card. If you notice something suspicious don't use it and report it to the Bank immediately.

**Phishing Attacks**

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. The recipient is tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. Attackers usually mimic electronic communications from a trustworthy or public organization in an automated fashion.

Protection Tips:

- Never give out confidential information or passwords by replying to an email or by visiting to a website through clicking a link included in an email. Even if you click on the link in an email but don’t actually provide confidential information, you could be exposing yourself to viruses, malware or other harmful pieces of software.
- Remember, Arab Finance House does not request confidential, personal or secure login information via email.
- If you do not recognize the sender of an email message, delete the email without opening it.
- Keep your passwords confidential. Change passwords regularly using a complex combination of letters, numbers and special characters. Avoid using obvious passwords that may be easily guessed or hacked.
- Always type in the browser the website you want to visit and do not click on the links embedded in the emails.
- Change your email account passwords immediately if you suspect that your passwords might have been compromised.
- Contact your bank immediately if you receive a transaction message from your bank that you do not recognize.

- Never send passwords, bank account numbers, or any other private information in an email.
- Be wary of any unexpected email attachments or links, even from people you know.
- Never enter private or personal information into a popup.
- Look for “https://” and a lock icon in the address bar before entering any private information.
- Update your devices regularly.
- Update your browser and the browser plug-ins regularly.
- Install the necessary software to protect your device such as firewall, spam filters anti-virus, and ensure they are up to date.
- Inform your bank immediately if you suspect that your email account has been hacked.
- Be cautious of anyone calling you to ask for bank account or personal information over the phone.

How to Spot a Phishing Message

- The message creates a sense of urgency meant to inspire a quick user response, generally by indicating the user needs to take action.
- The message lists a sender that differs from the email address it is sent from.
- The message claims to be from a legitimate company but come from an email address that is not linked to that company.
- Has no branding of any kind.
- Uses unusual words, syntax, or phrasing; contains simple spelling and grammar mistakes.
- Includes direct links to login pages.
- Includes an attachment with a generic name.