Usage & Protection of your Card

Report the Loss, Theft or Damage of your Card immediately to Bank Alfalah Consumer Finance Center on the following contacts so that your card can be blocked. If you are traveling abroad, report the loss, theft or damage on +8802-8191751-8.

Please follow these guidelines for the safety of your Alfalah Debit Cards.

Choosing PIN

1. Do not use a number or numbers that can obviously be associated with you – for instance your telephone number, birthday, your street number, driving license number or popular number sequences (such as 786 or 2005 or 1111).
2. Ideally choose a random combination of numbers – this is the hardest for a criminal to guess. If this is difficult for you to remember then perhaps use a combination of double numbers e.g.99 along with two others that have some meaning for you.
3. Change PIN number at frequent intervals.

Keeping Your PIN a Secret

1. Do not allow anyone else to use your card, PIN or other security information.
2. Always memorize your PIN and other security information. If the PIN you are provided with is difficult to remember, change it to something more memorable as soon as possible by dialing +8802-8191751-8.
3. Always take reasonable steps to keep your card safe and your PIN secret at all times. Neither your bank nor any agency is authorized to ask you to disclose your PIN.
4. Never write down or record your PIN or other security information on card or at a place easily accessible by others.

Precautions While Using ATMs (Automated Teller Machines)

Automated Teller Machines (ATMs) provide a fast and convenient banking alternative for account holders. You can bank when you want and where ever you want because locations are so convenient. In order to mitigate risks of theft & frauds we're providing these ATM safety tips to help protect you and your account.

Remember, ATM theft can occur in two ways;

a) Unauthorized withdrawals from an account or

b) The physical theft of cash as a person completes a transaction. The following advice for cardholders using cash machines will help minimize the chances of becoming a victim of such incidences.

Choosing an ATM

1. Always observe your surroundings before conducting an ATM transaction. If you see anyone or anything that appears to be suspicious, cancel your transaction and leave the area at once. If there is anything unusual about the cash machine, or there are signs of tampering, do not use the machine and report it to the bank immediately.
2. After dark, only use ATMs that are well-lighted.
3. If possible, choose a machine in a busy area. A heavily trafficked location means additional security.
4. If you are followed after using an ATM, seek a place where people, activity and security can be found.

Using an ATM

1. Use your body to block the view of your transaction. Especially as you enter your PIN and take your cash. If necessary, ask a person to leave, even if that person is just curious. If the ATM is in use, give the person using the machine the same privacy you expect. Allow them to move away from the ATM before you approach the machine.
2. Do not accept help from strangers and never allow yourself to be distracted.
3. A number of banks have established call centers to provide customer support. Inform them in case you have any problem and obtain a complaint number.

Focus your attention on ATM screen and take due care in the selection of buttons (touch the parallel area in case the screen is sensor one) to ensure the execution of desired transaction / funds transfer. Before pressing / touching the keyboard button enter the required information cautiously. If you pressed / touched wrong button then transaction reversal is not possible.

Leaving an ATM

1. After completing transaction, remember to take your card back.
2. Once you have completed a transaction, discreetly put your money and card in your pocket before leaving the cash machine. Do not count cash at ATM machine.
3. If the cash machine does not return your card, report its loss immediately to your bank.
4. Don’t discard your receipts and mini-statements or balance inquiry slips which contain important information. You get a receipt every time you make an ATM transaction.
5. Tear up or preferably shred your cash machine receipt, mini-statement or balance enquiry when you dispose them of.

Same Precautions While Using Point of Sales (POS)

1. Banks usually watch the cards transactions at point of sale (POS), to sort out if there are any unusual transactions, for the safety of customers and risk aversion. In such circumstances you may be contacted by your bank for authentication and confirmation of transactions. You are required to confirm your genuine transactions but do not disclose your PIN, Password etc. Such vigilance at both ends will bring synergy in the security of e-banking.
2. Always check your debit card when returned to you after the purchase.
3. Retain your copy of the charge slip for future reference.

Checking Statements

1. Ensure receiving of statement from your bank regularly. In case you do not receive statement, contact your bank for a copy of bank statement.
2. It is recommended that mini-statements are regularly produced for reconciling transactions.
3. Reconcile your transactions regularly with statements (Bank Statement or Mini-Statement).

Fraudulent E-mails

1. Fraudulent email may bear the authentic trademarks, logos, graphics and URLs of the spoofed company.
2. The HTML tags behind the link will reveal that the underlying URL usually does not link to a page within the authentic domain.
3. The email requests confidential or personal information (such as PIN, four digit number, account number etc).
4. It may request immediate action to keep accounts or cards activated so as to use it for some fraudulent purposes.
5. The linked web site may not provide secure and authenticated communication (i.e. it does not show the closed padlock at the bottom of the web browser).

Only Open and Respond to E-mails that Pass Some Basic Tests

1. Is the email from somebody you know?
2. Have you received emails from this sender before?
3. Were you expecting email with an attachment from this sender?
4. Does email from this sender with the contents describe in the subject line and the name of the attachment makes sense?
5. Does this email contain a virus?

Protection of Cards and Personal Information

1. Shield your card properly and follow basic principles of card storage. Cards are sensitive to mechanical, electromagnetic, sun impacts and can be pictured using cameras if left in plain view.
2. Do not bend your card.
3. Do not leave your card near a television or any other electrical or electronic gadget which has a continuous magnetic field
4. Avoid damaging or scratching the magnetic stripe. This stripe is sensitively encoded and requires special care.
5. Do not place two cards with magnetic stripe face to face.
6. Avoid submitting personal details for lucky draws even if these are from reputed organizations. Normally the organizations do not accept responsibility in case of theft of personal information which may cause loss to the card holder.
7. Your bank would only ask for specific characters within your password, not the whole password. Ask them for their phone number, check it and call them back. Also, be wary of responding to e-mails requesting information. If in doubt, ask for proof of identity or undertake your own checks. Never disclose your PIN to anyone.

8. Sign on the back of your new card as soon as you get it. Always use the same signature on card as entered in application form.
9. Carry fewer cards. It will reduce the risk of stealing.
10. In case of multiple cards make a list of all your cards and their numbers and keep it in a safe and secured place.
11. With debit cards easily at hand, try not to keep large amounts of cash at home. Your financial institution is a lot safer.
12. Cancel any unwanted or expired cards by contacting the card-issuer and cutting up the unwanted or expired card in at least two pieces. Upon receiving a renewed Card, please destroy the old Card by cutting it in two pieces.
13. If you move house make sure you contact your bank and all other organizations to give them your change of address.
14. Generally cardholders are not liable for losses resulting from circumstances beyond their control. Such circumstances include, but are not limited to:

- Technical problems, card issuer errors, and other system malfunction.
- Unauthorized use of a card and PIN where the issuer is responsible for preventing such use, for example after the card has been reported lost or stolen, the card is cancelled or expired or the cardholder has reported that the PIN may be known to someone other than the cardholder.

Precautions When Going Abroad with Cards

1. Make a note of your card issuers' emergency contact numbers and keep the information somewhere other than your purse or wallet.
2. Be careful at airports and other terminals during checking times. Ensure the safety of your cards and other important documents.

When Making Transactions through Call Centers/IVRs

1. Don't give your card number over phone to cold callers. Only make telephone transactions when you have made the call and are familiar with the company. Be particularly cautious if you are cold-called by someone claiming to be from a bank or any authorized agency etc.
2. Have the card in front of you. You may be asked for information including the card number, expiry date, the four-digit card security code on the signature strip (not your PIN code), issue number where applicable, and your name as it appears on your card.
3. If you feel pressured by a telemarketing salesperson, be suspicious. Never give out your account number unless you've decided to make a purchase.
4. Do not volunteer any personal information when you use your debit card, other than your ID document, which may be requested.
5. If the retailer sends you written confirmation of the order, check the bill to ensure that it is correct. Keep any such receipts and check them off against your next statement.
6. If you find any transactions on your statement that you are certain you did not make, contact your bank immediately. You may be asked to sign a disclaimer, confirming that you did not undertake the transaction.

What to do if you are a Victim of Card Fraud in General

If you discover that your card has been lost or stolen or that you have been the victim of a fraud, you should inform your bank immediately. But if the cardholder is shown to have acted fraudulently or without reasonable care, for example, by keeping their PIN written down with their card, they would have to meet all the losses.

Some Warning Signs of ID Theft and Fraud

1. Your regular bank or card statements fail to appear.
2. You notice that some of your mail is missing.
3. Your card statement includes charges for items you have not purchased or ordered.
4. A debt collection agency contacts you about goods you have not ordered or an account you have never opened.
5. You receive a telephone call or letter saying you have been approved or denied credit for accounts you know nothing about.

Problem Resolution Procedure

1. Banks should strive to provide error-free services, so as to protect the increasing volume of transactions conducted every day. However, errors do occasionally occur which may be addressed properly. To mitigate risk and restore the confidence of customers, each bank has to keep procedures in place to resolve inquiries and complaints.
2. In case of problem do your homework first. Judge the nature of the problem, so as to refer it to the concerned quarter; possibly you may get your dispute resolved by phone.