askari bank LIMITED

GUIDELINES
FOR SECURE USE OF ASKARI CREDIT/DEBIT/SMART CARDS

111-000-787 www.askaribank.com

askus

askari bank LIMITED

Askari Bank continues to provide innovative and safe electronic payment solutions to its customers. Facility of ATMs/Debit Cards, Internet Banking, Mobile Banking, Credit Cards, Call Centre IVR, Inter Bank Funds Transfers and facility for Utility Bill Payments are currently available. Using your cards is now quicker, safer and easier. With your Credit and Debit cards, experience your Bank account in your pocket.

When you get a new or renewed card, follow the procedure for activation as follows:

Activation of Askari Credit Card

Call Askari Bank 24/7 Help Line 111-000-787 to get your Askari Mastercard Credit Card activated.

Activation of Askari Debit Card

Activation of Debit cards can be done through ATMs, I-net banking services, Askari Bank Branches and Askari Bank call center.

I. Activation through Call Center

Just call on Askari Bank 24/7 call center at 111-000-787.

II. Activation through Branches

Visit your nearest Askari Bank Branch for activation.

III. Activation through I-Net Portal (for registered user)

- Log on to I-Net Banking, where ATM card management option shall be displayed.
- ATM Card management contains option for activation of Fresh/New cards.
- Select the card activation option by clicking on activate button.
- A One-time Password (OTP) shall be sent on your registered mobile number.
- You will be required to enter OTP into the I-Net system.
- You will also enter 16 digits of your debit card number in the system for validation.
- You will be required to enter desired PIN twice, to activate the card.
- A message regarding successful activation of card shall be displayed on the screen.

IV. Activation through ATM:

- Insert your new Debit Card in Askari Bank's ATM.
- After inserting Debit Card, system will ask for language selection.
- After language selection, system will ask for CNIC number.
- After providing CNIC, system will ask for date of birth (DD/MM/YYYY).
- After providing DOB, an OTP will be sent to customer on registered

mobile number.

- After receiving OTP, you will be required to enter the OTP.
- After entering OTP, you will be required to enter desired new Debit Card PIN twice, to activate the card.
- A message regarding successful PIN generation of card shall be displayed on the screen.

Guidelines for Using ATM/Debit/Credit Cards and Conducting Internet Transactions:

In order to enjoy the convenience of such payment solutions, you must exercise caution to minimize any risk of loss. Appended below are guidelines and few precautions that may be taken while using these services.

Choosing "Personal Identification Number" (Pin)/ Password:

1. ATM PIN, T-PIN and Credit Card PIN are normally four digit codes which enable you to access and conduct transactions at ATM & POS terminals and Call Centre IVR. Passwords are normally a minimum of 8 digit alpha numeric code which allows access to Internet Banking services.
2. DO NOT use PIN or PASSWORD numbers that are associated with you or are common, for instance, your telephone number, birthday, street number, driving license number or popular number sequences (such as 0786, 2014 or 1111).
3. Ideally, choose a random combination of numbers (alpha numeric in case of internet passwords) as these are the hardest for any lawbreaker to guess.
4. Change PIN and PASSWORD codes as frequently as possible.

Keeping your Pin/Password and Other Information a Secret:

1. Please do not share your Login ID/Password, ATM Card Number, ATM PIN, CVV Code, One Time Password (OTP) with anyone.
2. Always memorize your PIN/PASSWORD and other security information. If the PIN/PASSWORD you are provided with is difficult to remember, change it to something that you can remember easily. As a precaution, note your PIN/PASSWORD and keep it in a safe place not accessible to anyone but you.
3. Make sure to keep all your cards safe and your PIN a secret at all times. Neither your bank nor any agency is authorized to ask you to disclose your PIN/PASSWORD.
4. DO NOT write down or record your PIN or other security information on your card or at a place easily accessible by others.
5. DO NOT disclose your PIN on phone, mobile, internet messenger or any other mode of communication.

askari bank LIMITED

Precautions While Using ATMs (Automated Teller Machines):

Automated Teller Machines (ATMs) provide fast and convenient banking alternative and a wide array of services on a 24/7 basis. However, there is risk of loss at ATMs as stated below:

a) Unauthorized cash withdrawals or access to your accounts, if your ATM Card is left unguarded and its PIN is known to others.
b) Robbery while you are withdrawing cash.

If you follow the advice provided below, risk of loss will be minimized.

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.
2. If there is anything unusual about the ATM, or there are signs of tampering, DO NOT use the machine and report it to the bank immediately.
3. After dark, only use ATMs that have proper lighting arrangements, in and outside the location.
4. If possible, choose an ATM which is located in a busy area. A heavily trafficked location means additional security.
5. If you suspect that you are being 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 transaction, especially when you enter your PIN and take your cash.
2. If the ATM is in use, allow the person using the ATM the same privacy that you expect from others. After completion of the transaction, allow the first user to move away from the ATM before you approach the machine.
3. DO NOT accept help from strangers and never allow yourself to be distracted.
4. Most banks have established Call Centers to provide customer support. Inform these in case you have any problem or any suspicious activity and obtain a complaint number. Askari Bank Call Centre can be reached by dialing 111-000-787.
5. While paying the utility bills on ATMs, check the transaction details with the billed amount and customer ID on the 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.
6. Focus your attention on ATM screen and take due care in the selection of buttons to ensure the execution of desired transaction/ funds transfer. Enter the required information cautiously as pressing or touching a wrong button could lead to incorrect transaction being passed which cannot be reversed.

askari bank LIMITED

Leaving an ATM:

1. DO NOT forget to pick your card back from the ATM.
2. On completing a withdrawal, discreetly put your money and card in your pocket before leaving the ATM.
3. If the ATM does not return your card, report its loss immediately to your concerned branch, where your account is maintained and contact our Call Centre at 111-000-787 to block your card. You can collect your ATM Card from the acquiring branch (where your card was captured) within 2 working days by presenting your original CNIC.
4. You can request a receipt every time you make an ATM transaction. Don't discard your receipts, mini-statements or balance inquiry slips as these contain important information for reconciliation purposes.
5. Tear up or preferably shred your ATM receipt, mini-statement or balance enquiry when these are no longer needed.

Precautions While Using Point of Sales (POS):

1. Keep your card in your sight when it is being dipped and enter your PIN only by yourself on a POS (Point of Sale).
2. Banks usually monitor card transactions at a POS, to protect against any irregular transactions, for the safety of customers. In some circumstances, you may be contacted by your bank for authentication and confirmation of transactions. In any case, DO NOT disclose your PIN/PASSWORD to anyone.
3. Always check your card when it is returned to you after the purchase, to ensure that it is your own.

Precautions While Using or Making Transactions on Internet:

1. DO NOT use Internet facilities at Cafes or public places (at Airports, etc) to access your accounts to reduce the risk of compromising your log in information.
2. Use legitimate software (for operating systems, browsers and anti-viruses/ firewalls) and update these on a regular basis. Failure to do so may allow fraudsters and malicious hackers' access to your system and information.
3. Make sure your browser is set to the optimum level of security notification and monitoring. The safety/security options are not always activated by default when you install your software on your computer.
4. While shopping on the Internet, shop at secure and trustworthy websites only and ensure that the security icon, the locked padlock or unbroken key symbol, is appearing in the bottom right of your browser window before sending your card details. (HINT: The beginning of the retailer's Internet address will change from 'http' to

'https' when a purchase is made using a secure connection).

5. Click on the security icon to ensure that the internet 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.
6. Keep your personal information safe and always be wary of emails asking you to click on a link or confirm your details. Reputable retailers and banks would never ask you to disclose or confirm sensitive personal or security information including your PIN/PASSWORD. If you have any doubts, call the organization on their help line (111-000-787).
7. Avoid signing up for junk mail as this may result in prefilled application forms being sent to an address long after you've moved out, compromising your personal information.
8. Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to seek redress if problems arise, but having all the aforementioned information will help your card issuer to take up your case if you subsequently have any difficulties.
9. Ensure you are fully aware of any payment commitments you are entering into, whether you are instructing a single payment or a series of payments.
10. If you have any doubts about giving your card details over the Internet, find another method of payment.
11. If you regularly make transactions over the Internet consider opening a separate credit card account specifically for these transactions.
12. Keep your passwords secret. Some online stores may require you to register with them via user name and password before buying. Online passwords, including the one verified by your issuer, should be kept secret from others like you protect your card PIN. Keep the login information safe and secure.
13. 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. All reputable merchant sites use encryption technologies that will protect your private data from being accessed by others as you conduct an online transaction.
14. Never click on Hyperlinks within emails. If you are sure that the company is genuine, then directly type in the URL in the internet browser address bar, or call the company on a contact number previously verified or known to be genuine.

15. Don't let websites or merchants store your card information. The exchange of encrypted transactions will be better than to allow the storage of identity information on databases.
16. In case you pay your utility bills using internet banking facility, ensure that username, customer ID, amount billed are exactly the same as in the bill sent to you by the utility company. The transaction receipt may be saved on the hard disk and printed as well. It can be referred to in case of mismatch with the internet transaction history or the already paid bill may reappear in the next billing cycle.
17. In case you are making fund transfer, make sure that you have selected the correct beneficiary account from the predefined list or have correctly entered the beneficiary's entire account number, as per the facility offered by your bank. Also, make sure that you have entered the correct amount before confirming the transaction. The transaction receipt may be saved on the hard disk and printed as well.
18. Most importantly, make yourself familiar with the possible internet frauds. You should not be convinced by the persuasive and attractive traps of hackers.

Checking Your Statements:

1. Ensure receipt of statement regularly. In case you do not receive statement, contact your concerned branch for a copy of bank statement.
2. Reconcile your transactions regularly with statements (Bank Statement or Mini-Statement).

Recoginizing Fradulent E-mails

Please note and exercise caution:

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 website may not provide secure and authenticated communication (i.e. it does not show the closed padlock at the bottom of the web browser).

Protection of Cards and Personal Information:

1. Shield your card properly as important data may be stolen using cameras if left in plain view.
2. Store cards carefully as these are sensitive to mechanical, electromagnetic and heat exposure.
3. Avoid submitting personal details for lucky draws even if these are from reputed organizations. Normally organizations do not accept

responsibility in case of theft of personal information which may cause loss to the card holder.

4. 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 emails requesting information. If you have doubt, ask for proof of identity or undertake your own checks. Never disclose your PIN to anyone.
5. Sign on the back of your new card as soon as you get it.
6. Carry fewer cards. It will reduce the risk in case of theft.
7. In case you hold multiple cards, make a list of all your cards and their numbers and keep it in a safe and secured place.
8. Cancel any unwanted or expired cards by contacting the card issuer and vertically cutting up the unwanted or expired card in at least two pieces.
9. If you move house make sure you contact your bank and all other organizations to advise them of your new address.
10. Report loss of cards immediately to restrict the liability for transactions on stolen cards.

Precautions When Traveling Abroad with Cards:

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

Precautions When Making Transactions through Call Centers/ IVR:

1. Don't give your card number over the phone to anyone who cannot identify him/ herself to your satisfaction. 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.
2. Have the card in front of you. You may be asked for information including the card number, expiry date, the three-digit card security code on the signature strip (not your PIN code), issue date where applicable, and your name as it appears on your card etc.
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 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 such receipts and check them against your next statement.
6. If you find any transactions on your statement that you are certain you did not make, contact your concerned branch immediately. You

may be asked to sign a disclaimer, confirming that you did not undertake the transaction.

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 concerned branch immediately and contact our Call Centre at 111-000-787 to block your card. However, if the cardholder is shown to have acted fraudulently or without reasonable care, for example, by sharing their PIN or keeping their PIN written down with their card, they are liable for all the losses.

Warning Signs of ID Theft and Fraud:

1. Your regular bank or Credit Card statements fail to appear.
2. You notice that some of your mail is missing.
3. Your Credit 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:

Askari Bank Limited strives to provide error-free services to its customers. However, errors do occasionally occur. To assist our customers, we have procedures in place to resolve inquiries and complaints. Customers may contact the Bank as follows:

1. Call your Branch for assistance.
2. Call our 24/7 Call Centre on 111-000-787 for any assistance.
3. Register a complaint, suggestion or enter a query by emailing on customerservices@askaribank.com.pk or support@askaribank.com.pk.

Security Awareness:

This security awareness guide is intended to help you to recognize situations that give rise to possible frauds and to help you deal with them appropriately and effectively. The first step in protecting yourself from being scammed is to arm yourself with information. Learn more about the possibilities and other methods that fraudsters can use to obtain your personal information. Some of the common frauds are explained below, along with proactive measures that can save you from becoming the unfortunate victim of a hoax.

askari bank LIMITED

Cheque Fraud

Cheque Fraud is unlawful use of cheques (either by an account holder or an unauthorized individual) for the purpose of financial gain. There are a number of steps that you can take to protect yourself from cheque fraud.

- Whenever you receive your cheque book, please count the number of cheque leaves in it.
- Keep your cheques in a secure location.
- Review your monthly bank statement or regularly check your transactions through online banking. If you see transactions you didn't conduct, notify your bank immediatly and they will investigate.
- If you close your account, shred or destroy any unused cheques.
- Consider electronic payments as they are more secure than cheques.
- Beware of fake cheques.

Card Skimming

Skimming is a method used by fraudsters to capture your personal or account information from your plastic card for the purpose of stealing funds. To avoid skimming of your card, try to adopt the following safety measures:

- Use your hand, body or wallet to shield your PIN when you are conducting transactions at an ATM and never let your card out of sight when conducting a transaction at a point of sale location.
- Never disclose your PIN to anyone or write it down in a comprehensible manner.
- Regularly check your bank statements and account balances to verify all transactions.
- If your card is lost or stolen, or you suspect tampering, replace your card and report your suspicion to your bank immediately.
- Change your card's PIN frequently.

Pin/Password Safety

PIN/passwords are the first line of defense a gainst cybercrimes. It is crucial to pick strong alphanumeric passwords that are different for each of your important accounts and to change your passwords regularly.

askari bank LIMITED

CyberCrime

Cybercrime is a fast growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. Be cautious of suspcious looking websites when surfing and conducing transactions on the Internet. Always use a good anti-virus and malware detection application, and ensure that it is updated.

Social Networking

Social media enables networking but also offers a number of features that criminals may find attractive. Fraudsters can use social engineering in their efforts to appear legitimate, to hide behind anonymity, and to reach many people at low cost. Always be wary when engaging with strangers on social media.

Phishing

It is an attempt to fraudulently acquire sensitive information (usernames, passwords, card details and money etc.) by pretending to be a trusted identity in an electronic communication. It is a problem faced by banks worldwide. Usually account relatedinformation is requested for updating bank details or enrolling in lucrative reward schemes. You should never provide personal or confidential information through electronic communication unless you are sure that the inquirer or the website is genuine.

Spoofing

Website spoofing is the act of creating a fake website, with the intention of performing fraud. Online shopping sites with malware (malicious code aimed at compromising privacy) have increased significantly. You need to protect yourself when shopping online by practicing common sense and adhering to secure practices such as the following:

- Ensure the credibility of the seller.
- Protect personal information with strong passwords, etc.
- Ensure the shopping website is secure, i.e. it has "https:" in the address bar.
- Maintain a 'clean' and updated computing device.
- Type website/page addresses.
- Avoid clicking on links provided in emails.

Vishing

It is the act of using the telephone in an attempt to scam the user into surrendering private information. The caller pretends to be a legitimate business, and fools the victim into thinking he or she will profit. When approached by the person(s) claiming to belong to bank's staff, law enforcement agencies, SBP, Benazir Income Support Program (BISP) etc., never reveal the following details to a caller over the phone:

- The Login ID/Password, ATM Card Number, ATM PIN, CVV Code, One Time Password (OTP), passwords of your Internet Banking account and your Bank account number.
- Your Credit/Debit Card number etc.

Smishing

Smishing or "SMS Phishing" utilizes SMS services to send bogus text messages. The user is also tricked into downloading malware onto his cellular phone or other mobile device.

Email

Askari Bank will never send emails that ask for confidential information. If you receive an email requesting your Internet Banking details such as your PIN, password, or account number etc., you should never respond. In case of such fraud attempts and emails, please immediately contact the Call Centre at 111-000-787.

Disclaimer:

Violation & Non - Compliance after all these preventive measures would be Customer's liability

askaribank LIMITED

If you need any further information/ assistance, please contact your nearest Askari Bank branch, call Askari Help line at **111 000 787** or visit our website at **www.askaribank.com**

askus