STATE BANK OF PAKISTAN

TELEGRAMS
BANK RATE

Post Box No. 4456, Karachi
(74000)

Payment System
Department

PSD/DIR/ Policy Guidelines/ 110 /102/81 **Dated: 05-12-2005**

The Presidents/Chief Executives,
All Commercial Banks

Dear Sir/Madam,

Subject: **Guidelines for Card Holders**

Electronic Payment Systems are rapidly replacing the conventional systems because of efficiency, convenience and cost effectiveness. However, security is one of the major challenges in the complete transformation of paper based systems to electronic. While the commercial banks are taking measures to strengthen security, they are also required to create awareness on the adoption of new practices by card holders to mitigate risks arising out of deployment of new technologies.

State Bank of Pakistan, in consultation with commercial banks, have developed "Guidelines for Account Holders using Debit/Credit/Smart Cards" which will facilitate the various stakeholders to disseminate basic information on e-banking practices to their customers. These guidelines are minimum set of information and may be customized by the banks to meet their specific requirements.

The banks are requested to update the guidelines on their web along with a section of FAQs. They should also take initiatives to create awareness among their customers who are using debit/credit/smart cards.

Banks are requested to comply with the instructions latest by 01-01-2006.

Encl: As above (01)

Yours faithfully,

(Muhammad Saleem Rehmani)
Director

Payment Systems Department

Guidelines For Account Holders Using Credit / Debit / Smart Cards

- **Note:** Please follow these guidelines for your safety as you enjoy the convenience of technology. However these guidelines are general; therefore, specific precautions may be taken as warranted by the situation and technology.

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 at a cash machine as soon as possible.
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.

Payment Systems Department

Guidelines For Account Holders Using Credit / Debit / Smart Cards

v 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.

v 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.
4) While paying the utility bills on ATM check the transactions details with the billed amount, customer ID on 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.
5) 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.

v 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.

v 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 credit card when returned to you after the purchase.

v Safe Internet Transactions / Shopping Virtually and with your Cards:

1) On the top of everything customers should make themselves familiar with the possible internet frauds. They should not be convinced by the persuasive and attractive traps of hackers.

2) Keep software updated (operating systems and browsers) because fraudsters and malicious hackers are very clever and have found vulnerabilities in software's (windows and browsers). Both institutions and customers should ensure that operating and browser softwares are kept upto date using legitimate upgrades and patches issued by the legitimate software vendors.

3) Make sure your computer has up-to-date anti-virus software and a firewall installed. Firewalls can monitor both incoming and outgoing internet traffic and anti-virus will protect your computer against Trojan and worm attacks.

4) Make sure your browser is set to the highest level of security notification and monitoring. The safety options are not always activated by default when you install your softwares on your computer.

5) Two of the most popular browsers are Microsoft Internet Explorer and Netscape Navigator. Check that you are using a recent version - you can usually download the latest version from these browsers' websites.

6) Only shop at secure websites - 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.

7) The beginning of the retailer's Internet address will change from 'http' to 'https' when a purchase is made using a secure connection.

8) Use sites you can trust, for example sites you know or that have been recommended to you or that carry the Trust logo.

9) Click on the security icon to ensure that the 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.

10) Keep your personal information safe – always be wary of e-mails asking you to click on a link or confirm your details. Reputable retailers, banks etc.

would never ask you to disclose or confirm sensitive personal or security information, including your PIN. If in doubt, phone the organization first.

11) Avoid signing up for junk mail – this may result in pre-filled application forms being sent to an address long after you've moved out.

12) 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 take up your case if you subsequently have any difficulties.

13) Ensure you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments.

14) In case you pay your utility bills using virtual banking facility, ensure that user name, customer ID, amount billed are exactly the same as in the bill sent to you by your company. The transaction receipt may be saved on the hard disk and may be 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 next billing cycle.

15) If you have any doubts about giving your card details, find another method of payment.

16) If you regularly make transactions over the Internet consider opening a separate credit card account specifically for these transactions.

17) 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 outside parties the same way you protect your Card PIN. Keep the login information safe and secret.

18) 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. The most reputable merchant sites use encryption technologies that will protect your private data from being accessed by others as you conduct an online transaction.

19) Never click on Hyperlinks within e-mails. 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.

20) 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 data bases.

Payment Systems Department

Guidelines For Account Holders Using Credit / Debit / Smart Cards

v 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).

v 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).

v Only Open and Respond to E-mails that Pass Some Basic Tests, such as:

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?

v 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) Avoid to submit 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.
3) 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.

4) Sign on the back of your new card as soon as you get it.

5) Carry fewer cards. It will reduce the risk of stealing.

6) In case of multiple cards make a list of all your cards and their numbers and keep it in a safe and secured place.

7) With credit and debit cards easily at hand, try not to keep large amounts of cash at home. Your financial institution is a lot safer.

8) Cancel any unwanted or expired cards by contacting the card-issuer and 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 give them your change of address.

10) Generally cardholders are not liable for losses resulting from circumstances beyond their control. Such circumstances include, but are not limited to:

a) Technical problems, card issuer errors, and other system malfunction.

b) 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.

v 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.

v 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 credit/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

Guidelines For Account Holders Using Credit / Debit / Smart Cards

make, contact your bank immediately. You may be asked to sign a disclaimer, confirming that you did not undertake the transaction.

v 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.

v Some 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.

v Problem Resolution Procedure:

1) Banks should strive to provide error-free services, so as to protect the increasing volume of transactions conducted everyday. 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.

END of Guidelines