

Tips for Fraud Prevention during Financial Transactions

Dear Customer,

By taking few basic precautions while conducting your financial transaction, you can go a long way in protecting yourself against financial frauds.

Listed below are a few tips that you could follow:

ATM transactions:

- ✓ Maintain an awareness of your surrounding throughout the entire transaction. Be wary of people trying to help you with ATM transactions.
- ✓ **Shield your PIN** – To guard against others observing you as you key in your PIN at a terminal, stand directly in front of the keyboard or PIN pad to block the view of anyone standing near you.
- ✓ **No one else ever needs to know your PIN** – Your ATM card will work only with a PIN (Personal Identification Number). Memorize your PIN. Never write your PIN on your card or store it with your card. Do not use your birth date as your PIN, especially if you carry your driver's license with your card. Never tell your PIN to anyone or let anyone else enter your code, keep your PIN a secret.
- ✓ Do not enter your PIN if the ATM eats your card - contacts your bank official.
- ✓ **Never count cash at the machine or in public** – Wait until you are in your car or another secure place.
- ✓ Maintain a supply of deposit envelopes at home or in your car. Prepare all transaction paperwork prior to your arrival at the ATM. This will minimize the amount of time spent at the machine
- ✓ **Report a lost or stolen card at once** – Even though your ATM card cannot be used without your PIN, report a lost or stolen card to your financial institution immediately.
- ✓ **Keep your receipts** – To guard against transaction frauds, check your receipts against your monthly statement.
- ✓ If you are involved in confrontation with an assailant who demands your money, COMPLY!!

Online Transaction (online shopping, movie tickets etc.:)

- ✓ Do not access Netbanking or make payment using your Credit / Debit from shared or unprotected computers in public places.
- ✓ Use secure websites for transaction and shopping. Shop with merchants you know and trusts. Make sure internet purchases are secured with encryption to protect your account information.
- ✓ Look for "secure transaction" symbols like the padlock icon at the bottom right of the browser window for secure webpage (you can double click on it to verify the website's security and authenticity) or "https:// in the address bar of the website." This "S" helps ensures that your information will be passed along in a secure manner.
- ✓ Always log off from any website after making purchase with your credit / debit card. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.

Avoid Phishing and Fishing Scams.

Scams like Phishing and Vishing are designed to steal your web identity and personal data. Phishing is carried out via fraudulent e-mails and Vishing is orchestrated via bogus voice messages and phone calls.

- ✓ Treat all e-mail messages with suspicion. What you see in the body of the message can be forged, the sender address and the return address can be forged, and the header can also be manipulated to disguise its true origin. Do not respond to forms and links in the e-mail.
- ✓ Do not open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.
- ✓ Never send any personal or financial information to anyone via e-mail. Do not share any confidential information such as password, customer id, Debit card number, Pin CVV2, DOB to any email requests, even if the request is from government authorities like Income tax department, RBI or any card association company like VISA or Master card.
- ✓ Set up either e-mail or SMS alerts on your net banking for all the transactions.
- ✓ Regularly log on to your Net banking account (At least once in a month)
- ✓ Do not address or refer to your bank account problems or your account details and password on social networking site or blogs.
- ✓ Do not transfer or share your account details with unknown / non validated source. Luring you with commission, attractive offers.
- ✓ Ensure that you have installed latest Anti-Virus / Anti-Spyware / personal firewall / Security patches on your computer or high end mobile phone/PAD's
- ✓ Do not access Net banking or make payments using your Debit cards from shared or unprotected computers in public places.
- ✓ Check for the padlock icon. Microsoft internet Explorer always displays the lock icon at the bottom of your browser window for secure WebPages. Double-click on it to verify the site security and authenticity.

Protecting Banking Information on Mobiles:

- ✓ Use the phone lock function on your mobile device when it is not in use, This function password protects your device so that nobody else can use it or view your information, Also be sure to store your device in a secure location.
- ✓ Frequently delete text messages from your financial institution especially before learning out, discarding or selling your mobile device.
- ✓ Do not store critical information like your ATM PIN number on your phone.
- ✓ Never disclose via text message any personal information (account numbers, passwords or any combination of sensitive information like your PAN number or birth date that could be used in ID theft)
- ✓ If you change your mobile number, contact your nearest Ratnakar Bank Branch immediately in order to update the new mobile number.