ATM Fraud

Financial fraud of all types is a huge problem throughout the world. With the advent of automated teller machines, or ATMs, came another opportunity for would-be thieves to steal money, account information, and identities. The term "ATM fraud" can refer to an illegal transaction that is committed by using an ATM, including fraudulent deposits or skimming card information.

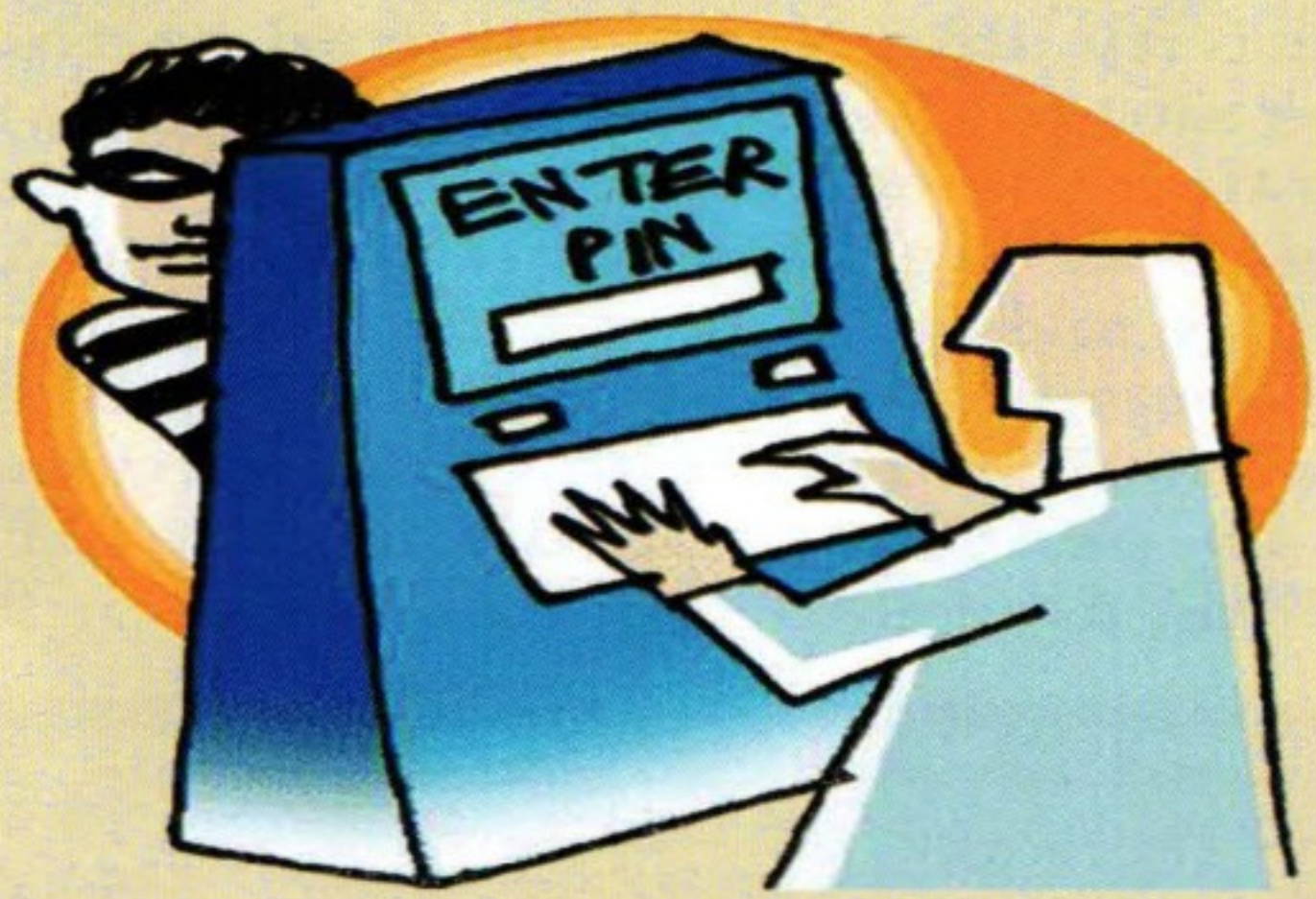
Tips to take while using ATM machines

- Always check the premises and the machine, if you find anything unusual DO NOT do a transaction. Eg: Additional gadgets on the ATM machine
- Cover while entering your PIN be careful of small camera that can be installed
- Do not leave your statements that are printed after a transaction behind. Take it home and shred them.
- Always check your balance and keep a record of all transactions.
- Do not get into conversations or be on a call.
- DO NOT forget to take your Card after the transaction.

Remember:

- Not everything you read on the Internet is true. Think twice before signing up for anything online. Don't give out your credit card number (or anyone else's). Remember, when you are online, what you do is up to you. Don't do anything you don't want to do.
- Don't open files or e-mail from someone you don't know. You don't know what might be inside—the files could contain a computer virus or offensive material.

- Always pay close attention to the ATM and your surroundings. Don't select an ATM at the corner of a building — corners create a blind spot. Use an ATM located near the center of a building. Do your automated banking in a public, well-lighted location that is free of shrubbery and decorative partitions or dividers.
- Maintain an awareness of your surroundings throughout the entire transaction. Be wary of people trying to help you with ATM transactions. Be aware of anyone sitting in a parked car nearby. When leaving an ATM make sure you are not being followed. If you are, drive immediately to a police or fire station, or to a crowded, well-lighted location or business.
- Do not use an ATM that appears unusual looking or offers options with which you are not familiar or comfortable.
- Do not allow people to look over your shoulder as you enter your PIN. Memorize your PIN; never write it on the back of your card. Do not re-enter your PIN if the ATM eats your card — contact a bank official.
- Do not wear expensive jewelry or take other valuables to the ATM. This is an added incentive to the assailant.



- Never count cash at the machine or in public. Wait until you are in your car or another secure place.
- When using a drive-up ATM, keep your engine running, your doors locked and leave enough room to maneuver between your car and the one ahead of you in the drive-up line.
- Maintain a supply of deposit envelopes at home or in your car. Prepare all transaction paper work prior to your arrival at the ATM. This will minimize the amount of time spent at the machine.
- Closely monitor your bank statements, as well as your balances, and immediately report any problems to your bank.
- If you are involved in a confrontation with an assailant who demands your money, COMPLY.

A CARD SKIMMER

- A card skimmer is a device which is designed to steal information from a card with a magnetic strip, classically a credit card, when the card is used in a legitimate financial transaction. Once collected on the device, the skimmer can be used to make a clone of the card which can be used for fraudulent purposes, or the collected

information can be utilized for online and over the phone transactions which do not require a physical credit card, only the information on the card. The annual losses caused by card skimmers are difficult to estimate, but appear to be upwards of $1 billion US Dollars (USD).

- There are several ways in which a card skimmer can be used. Some skimmers are designed as standalone units through which a card must be swiped. For example, an unscrupulous restaurant employee might carry a skimmer so that he or she can run a customer's credit card to pay for a tab, and then run the card through the skimmer to collect the information. This type of skimmer can usually store numerous credit card numbers.
- The second type of skimmer is a small electronic device which attaches to a credit card terminal or automated teller machine (ATM). In this case, every time a card is swiped or inserted, the skimmer gathers the user's information, and it may be attached to a device which logs keystrokes to collect the personal identity numbers (PINs) of people who use the terminal.

Remember

- People can protect themselves from credit card skimmers in a number of ways. If a credit card is taken by someone to be run, the card holder can ask to watch the process. Most credit card terminals are kept in plain view, making it easy for people to see if their cards are run twice, or if there is anything unusual about the way in which the card is handled. When asked to enter

a PIN, people should also get into the habit of covering their hands while they enter the number, to make it harder to collect the number with the use of a camera or observation.

- Standalone credit card terminals with card skimmers may look or behave in a slightly unusual way. For example, the area to insert the card may be loose or crooked, indicating that it has been moved, or that a card skimmer has been attached over the actual area of insertion. People who regularly use the same terminal may also want to note changes in the configuration, which could indicate that a skimmer is being used. Card skimmers are also often accompanied by cameras to log PINs.

- If someone believes that he or she has identified a card skimmer, the skimmer should be reported to the fraud department in the company which operates the terminal, and to the police. If, for example, someone notices what looks like a card skimmer on Bank A's ATM, he or she should call Bank A's fraud department with information and notify the police. If someone suspects that a card skimmer is being used by an employee of a business, they should report it to the police and the manager.

- Victims of card skimmers will notice unusual activity on their credit cards or bank accounts. This activity should be reported to the credit bureaus and to the bank which administers the card so that the card can be closed and a fraud investigation can be initiated. Card skimmers can also be used to collect information from key cards, government identification cards, and any other sort of card with an embedded magnetic strip, so people should be careful about controlling access to such cards.