SOUTH INDIAN Bank
Experience Next Generation Banking

## Consider this incident:

Albin was on his way to his office in Kuwait and suddenly remembered that he had to buy flowers for Susan, his co-worker, who was celebrating her birthday that day. Albin pulled up at the closest flower mart and used his Debit card to pay the bill, as he was falling short of cash. After 4 months, Albin was performing an online transaction and noticed a series of 8 ATM transactions amounting Rs.29,000/= in his account. Alarmed he informed the bank authorities and upon investigation it turned out that his ATM card had been duplicated. Those culprits had duplicated the card and withdrew the sum from his account, through ATMs of various banks installed in Thailand.

This is just one example of a POS machine fraud or in other words POS Skimming. Slight ignorance on your part will lead to heavy losses while performing ATM or credit card transactions.

**What is skimming?**
Skimming is the process where original data from your card's magnetic strip is electronically copied to create a duplicate card without your knowledge. Most of the cases of counterfeit fraud involve skimming.

**Types of skimming**
Here are the two most common ways, how fraudsters can duplicate ATM/Debit card and credit cards:

**Card skimming**
A scanning device (skimmer) is used here that copies the information present in the magnetic strip of your ATM card when you insert it in an ATM machine. When you perform your transaction, the skimmer copies all the details of your card on to the device and an overhead tiny camera records your PIN. The fraudsters can access the skimmer and camera using the laptop's wireless feature sitting nearby the ATM machine or pull the skimmer and camera from the ATM and then copy the skimmer data into a computer. Now they make a duplicate magnetic strip using a device called MSR (Magnetic Stripe Recorder) and withdraw large sums of money from your account using the PIN number.

**Card trapping**

A device attached inside the ATM machine traps your card as soon as you insert it. Well meaning people around you will request you to make a couple of attempts to perform transactions to observe and make a note of your PIN number. When you get frustrated, you give up, and move out of the ATM center to report the same to the bank. Miscreants would remove the trapping device, take your card from it, and as they are already aware of the PIN, they would have performed huge transactions within no time.

Now that you have learnt some information about ATM Skimming, its time you knew about Point of Sale (POS) skimming.

**Point of Sale (POS) Skimming**

ATM skimming is limited to ATMs and so you know you have to be careful when you are at an ATM, but Point of Sale scams /skimming can happen at the most unassuming and innocuous seeming places like bars, restaurants, supermarkets or gas stations. When you offer your card to make a payment, all that the corrupt employee has to do is to skim your card with a small, hand-held electronic device before handing your card back. This device captures all details about your card and the sales person observe and make a mental note of your pin number while you enter it, popularly known as shoulder surfing.

Once the corrupt employee has your card details and PIN number, he can create a duplicate card and with draw cash at an ATM or go on a shopping spree.

**Safety tips to protect yourself against card skimming frauds**

Here are few steps you can take to protect your ATM and credit cards:

- Keep your credit cards and ATM cards with you at all times.
- Never let these cards out of your sight or allow others to use on your behalf.
- If you see a shop assistant swipe the card through a second POS machine, then you need to question this action.
- If you notice something suspicious about the card slot on an ATM (like an attached device), do not use it and report it to the responsible authorities.
- Never trust your ATM card and credit card PIN numbers to strangers.
- Beware of your surroundings while withdrawing money at ATM centers.
- Do not crumple and throw away the transaction slips or credit card memos: read them, make a mental note of the details and then, either tear them or shred them to trash them.

- Periodically check your account balances on Internet or by requesting your bank or credit agency to send you statements to ensure that no transactions are happening behind your back.
- While entering any personal identification numbers (PIN), use your discretion to shield the keypad so that your hand movements are not very visible and you enter your passwords secretly.
- Change your ATM card PIN on a regular basis – once in a month at least. But change the PIN immediately, if you suspect some data disclosure.
- Bars, restaurants, supermarkets, fuel pumps etc are high risk areas and take adequate precautions while using the card as discussed above.
- Never write the PIN on the Card itself or on the card pouch.
- Subscribe to SMS alerts from your Bank, so that you get immediate alerts whenever a transaction takes place in your A/c.

Now, well armed with this knowledge about ATM skimming and POS skimming, we hope that you will be more careful, the next time you are at an ATM or while making transactions with your card. If you care for your friends and family members, please forward this document to enlighten and educate them about the perils of Credit / Debit card fraud, so that they are protected from latest scams.

---

Dated 1st December 2009