

## GET DUPED Anytime, Anywhere

*Your friendly, neighbourhood ATM may not be as foolproof as you think. With ATM frauds on the rise, you need to be careful each time you withdraw instant cash, says Ashley Coutinho*

RAJ was an agnostic and never believed in miracles. This changed a few days ago, when a five-figure sum mysteriously vanished from his account. He promptly pinned the blame, first on God, and then on the bank, neither of which helped. Actually, he should have blamed his own carelessness as the PIN number of his debit card had somehow leaked out. But Raj can take heart from the fact that he is not alone.

With the increase in number of automated teller machines (ATMs) across the country over the past few years, the number of fraudsters thriving on ATMs has risen too. According to Frost & Sullivan (F&S), India is among the fastestgrowing ATM markets, with the number of ATMs doubling every year. ATMs have made life easier for customers, who can conduct cash withdrawals, cash or cheque deposits and balance enquiry any time of the day.

However, frauds continue to plague ATMs, warns F&S. Besides monetary loss, this can result in massive erosion of customer confidence. ATM frauds can also be referred to as identity thefts as the trickster assumes the e-identity of the user to gain access to his/her financial resources. Though these frauds are relatively new in India, they have gained widespread notoriety across the world.

Lebanese Loop is a popular method of ATM fraud overseas. A fake front, a plastic or metal sleeve, is custom-built to fit over the ATM. When a customer inserts his card and enters the PIN, a message instructing the user to re-enter the PIN is flashed across the screen as the machine cannot read the card's magnetic strip.

As the user re-enters the PIN several times, the fraudster slips up behind him and takes note of his PIN. The user is also unable to retrieve his debit card. After several unsuccessful attempts, he leaves, thinking the machine has swallowed his card.

Another method of ATM fraud is skimming, which uses electronic devices to read and store information located on the card's magnetic strip. There are also many organised gangs which specialise in ATM frauds. In some cases, crooks purchase ATM machines, place them at convenient locations, and withdraw cash from customers, especially high net worth individuals (HNIs).

In the US, a majority of the offpremise ATMs are subjected to RAM raids, while skimming is the most prevalent form of fraud in Canada.

Back home, the techniques employed are much simpler — fraudsters rely more on customers' foolhardiness to make a fortune. According to Loney Antony, MD of Euronet Services India, which provides ATM outsourcing services, 90% of the frauds at ATMs occur due to carelessness. For example, in the case of PIN frauds, someone may peer over the card-holder's shoulder to find out his PIN, before filching the card. According to S Nair, managing director, Intellvisions Software, which provides customer-service automation products, 30-40% of these frauds are done by people close to the victim.

There are also instances of duplicate card usage. This type of fraud can be tracked at the transaction level, since the card information goes to the back-end system where its usage is monitored. There are even reports of ATM cards reaching the wrong address, as well as thefts of ATM cards in transit and their subsequent misuse. Sometimes, customers may not be aware that money has been debited from their account.

If they regularly withdraw a fixed amount from their account, and withdrawals of the same amount are made in between, they are unlikely to notice the discrepancy in entries, says Mr Naik.

But ATM scams are rarely reported in India. There are two main reasons for this. Firstly, banks don't want to admit that a fraud has been committed as it can tarnish their reputation. And secondly, customers are reluctant to take the matter forward to consumer courts as they don't want to break their relationship with the bank.

Nevertheless, banks do warn customers to be careful while conducting transactions on ATMs. For example, HDFC Bank has a long list of dos and don'ts regarding ATM usage.

But customers are largely ill-informed about safety norms and the various ways they may get duped. According to Loney Antony, ATM manufacturers have come out with a technology that prevents the use of skimmers and most banks now prefer using dip card readers which can prevent Lebanese Loops.

Banks are also waking up to the need for sophisticated equipment and technology and inclusion of additional security features.



**✓ DO'S SWIPE IT RIGHT**

- ▶ Report loss of credit card immediately
- ▶ Keep your card in a safe place
- ▶ Conduct ATM transactions privately
- ▶ Stand close to the machine and use your hand to shield the keypad while typing the PIN
- ▶ Inform the concerned call centre/branch immediately if your card is swallowed
- ▶ Inspect the machine for signs of tampering
- ▶ Take your debit/credit card back after completing your transaction
- ▶ Go to another ATM if you find suspicious-looking people around you

**✗ DON'TS**

- ▶ Disclose your ATM PIN to anyone or write it down anywhere
- ▶ Hand over your card to anyone
- ▶ Accept help from strangers
- ▶ Count your cash at the ATM