Credit, debit card frauds and how you can avoid them

By *Riju Dave*, ET Bureau | Oct 31, 2016, 11.25 AM IST

Even as the RBI and banks are introducing several security features, customers need to take the initiative to prevent being conned.

On 19 October, the country woke up to a banking nightmare. The State Bank of India (SBI) blocked 6 lakh debit cards after a reported malware-related breach in a non-SBI ATM network. In what is possibly India's largest financial data breach, nearly 32 lakh debit cards across 19 banks, including HDFC Bank, ICICI Bank and Axis Bank, were compromised. As per the National Payments Corporation of India (NPCI), 90 ATMs were impacted and at least 641 customers lost Rs 1.3 crore in fraudulent transactions.

Even as the council of Payment Card Industry Data Security Standard (PCI-DSS), an international body that sets data security standards, has ordered a forensic audit, banks have advised their customers to change PINs and confine themselves to own bank ATMs. The customers, meanwhile, are worried about how secure their debit and credit cards really are.

It's a justified concern, considering that nearly 2.59 crore credit cards issued by 56 banks had a transaction worth Rs 24,341 crore via points of sale (POS) and Rs 202 crore through ATMs, while 69.72 crore debit cards registered transactions worth Rs 2.19 lakh crore through ATMs and Rs 17,100 crore via POS in July 2016. This is a fortune that fraudsters are waiting to tap into through several, ready loopholes. "Banks are definitely revisiting their network security by applying additional layers of security to prevent any compromise," says Rajiv Anand, Executive Director, Axis Bank.

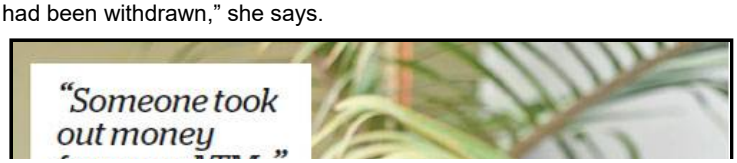
Even as the RBI and banks are trying to stay one step ahead by introducing several security features, including chip-based cards and two-factor authentication, customers need to take the initiative to prevent being conned. We list here the various ways that cards, credit and debit, can be used to commit fraud and steps you can take to steer clear of these.

HOW YOU CAN BE DUPED

Card fraud basically involves theft of identity or information on your cards. This information is then used to make ATM withdrawals or conduct online or offline transactions. The stealing can take place in one of the following ways:

Automated Teller Machines (ATMs)

The machines have become a favoured target of scamsters (see *5 traps set up by fraudsters at the ATM*). Ask Mumbai-based Rupali Pandagale (see below), who went for cash withdrawal to another bank's ATM. "I put the card in one of the machines, but it wasn't working. So I took out Rs 2,500 from the other machine and left. Five minutes later, I got an alert saying another Rs 10,000 had been withdrawn," she says.



Rupali Pandagale
29 years
Salaried, Mumbai
Fraud: ATM withdrawal from other bank machine.
"I inserted my card in one machine, but it wasn't working. I withdrew Rs 2,500 from the other machine and left. Five minutes later, I got an alert that Rs 10,000 had been withdrawn."
When: February 2016.
Amount: Rs 10,000.
What did she do?
"I contacted both the banks and asked for video footage, but they refused to share it with me. They insist I conducted the transaction and have failed to remit the amount."
Current status: Unresolved.

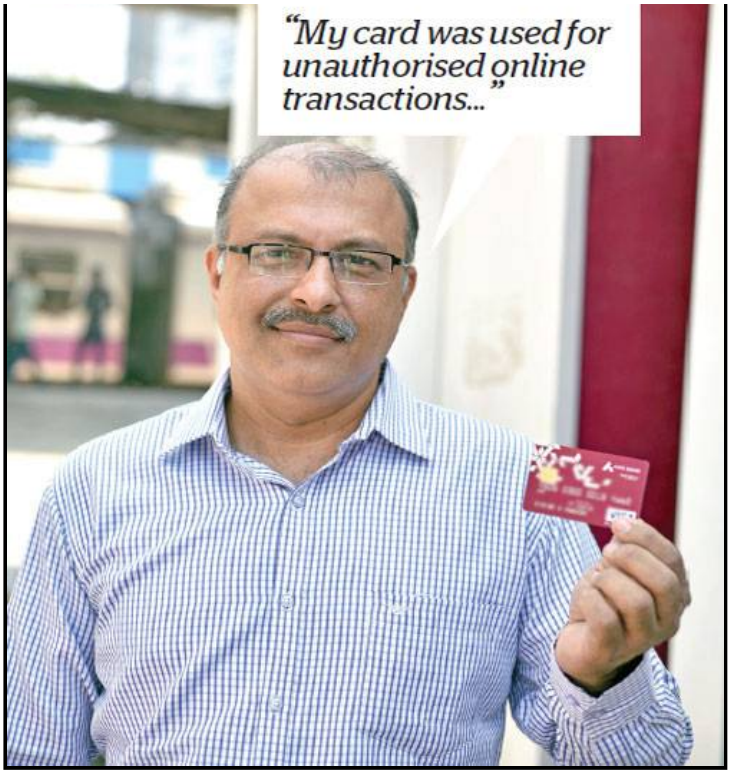
There are various techniques fraudsters use to steal your card information:
***Skimming:** "This technique involves attaching a data skimming device in the card reader slot to copy information from the magnetic strip when one swipes the card," says Mohan Jayaraman, Managing Director, Experian India. "They also set up cameras near the machine to get the PIN," he adds.

***Card trapping:** This is a barb that retains the card when you insert it in the machine and the card is retrieved later.

***Shoulder surfing:** If you find friendly bystanders in the room or outside who try to help you if your card gets stuck or peer over your shoulder, beware. They are there to get you to reveal your PIN.

***Leaving card/PIN:** If you write your PIN on the card and forget it in the ATM kiosk or the machine, it's a virtual invite to be scammed.

Online transactions
The ease of e-shopping or online bill payment is matched by the felicity with which identity theft can be carried out on computer or smartphone. This can then be used for unauthorised transactions. Mumbai-based Girish Peswani (see below) knows it well. "I was in my office when I got alerts about online transactions abroad made using my credit card," he says. There are various ways this credit card information could have been stolen from Peswani.



Girish Peswani
44 years
IT consultant, Mumbai
Fraud: Illegal online transactions.
"I was in my office when I got two alerts showing online transactions on my card in The Netherlands and Australia."
When: August 2014.
Amount: Rs 12,000.
What did he do?
"I blocked the card and contacted the bank. They asked me to get a new card. I asked them to resolve the issue first, but they continue to send me credit bills for the amount spent and a huge interest amount too."
Current status: Unresolved.

***Pharming:** In this technique, fraudsters reroute you to a fake website that seems similar to the original. So even as you conduct transactions and make payment via credit or debit card, the card details can be stolen.

***Keystroke logging:** Here, you unintentionally download a software, which allows the fraudster to trace your key strokes and steal passwords or credit card and Net banking details.

***Public Wi-Fi:** If you are used to carrying out transactions on your smartphone, public Wi-Fi makes for a good hacking opportunity for thieves to steal your card details.

***Malware:** This is a malicious software that can damage computer systems at ATMs or bank servers and allows fraudsters to access confidential card data.

Merchant or point-of-sale theft
This is perhaps the simplest and most effective form of stealth, wherein your card is taken by the salesperson for swiping and the information from the magnetic strip is copied to be used later for illegal transactions.

Phishing & vishing
While phishing involves identity theft through spam mails which seem to be from a genuine source, vishing is essentially the same through a mobile phone using messages or SMS. These trick you into revealing your password, PIN or

using messages or SMS. These trick you into revealing your password, PIN or account number.

SIM swipe fraud

Here the fraudster contacts your mobile operator with fake identity proof and gets a duplicate SIM card. The operator deactivates your original SIM and the thief generates one-time password (OTP) on the phone to conduct online transactions.

Unsafe apps

Mobile apps other than those from established stores can gain access to information on your phone like passwords, etc, and use it for unauthorised transactions.

Lost or stolen cards, interception

This is the oldest form of theft, wherein transactions are carried out using stolen cards, those intercepted from mail before they reach the owner from the card issuer, or by fishing out information like PINs and passwords from trash bins.

Cards using other documents

This is also an easy form of identity theft, where new cards are made by the fraudster using personal information that is stolen from application forms or other lost or discarded documents.

HOW TO PREVENT FRAUD

Some basic, preventive steps can ensure that you do not fall prey to credit or debit card fraud. Here's how:

ATM safeguards

"Stay away from ATMs that appear dirty or in disrepair. They may not work or, worse, may be fake machines set to capture your card information," warns Navroze Dastur, Managing Director, NCR India, a financial security solutions firm. Here are some other things you should keep in mind:

***Check machine:** "Do not use ATMs with unusual signage, such as a command to enter you PIN twice to complete the transaction," says Dastur. "Also watch out for machines that appear to have been altered , if the front looks crooked, loose or damaged. It could be a sign that someone has attached a skimming device," he adds.

***Cover keypad:** Make sure to cover the keypad with your hand while entering the PIN to escape any cameras attached nearby.

***Don't take help:** It is advisable to use only your own bank ATMs, particularly those attached to a bank branch and those that have security guards. Also, avoid taking the help of any person loitering outside the ATM or volunteering to assist you if you get stuck.

Online precautions

***Use safe sites:** Go only to well-known, established sites for e-shopping. "Remember to confirm the site's legitimacy before using it and shop only on those that are Secure Sockets Layer (SSL)-certified. These can be identified through the lock symbol next to the browser's URL box," says Porush Singh, Country Corporate Officer, Indian & Division President, South Asia, Mastercard.

Also make sure that the website uses the 'https' protocol instead of 'http', where 's' stands for 'secure'. Additionally, make sure not to click on the option that asks for saving your card details on any site.

"You should also look out for a site's payment verification tools, such as MasterCard's SecureCode, which verifies that you authorised the payment while protecting the privacy of you online transaction," says Singh.

***Anti-virus software:** While banks deploy ATM network security measures, an

***Anti-virus software:** While banks deploy ATM network security measures, on an individual level you can safeguard transactions by installing anti-virus software on your computer and smartphone to keep out malware. “You can also install identity theft detection apps on your phone from an official app store,” says Jayaraman of Experian. Besides, have software on your smartphone that enables you to wipe out the data remotely in case the mobile gets stolen.

***Debit card:** Make sure that you do not use your debit card for e-commerce transactions. This is because if your card is compromised, the entire cash in your bank account can be wiped out instantly. The credit card, on the other hand, offers a month’s grace period before the cash leaves your account, during which the investigation can possibly nail the fraud.

***Hide CVV:** When you enter the CVV on the site, it should be masked by asterisks. This is especially important while shopping on foreign websites where the CVV is the only point of verification. Also use a virtual keyboard to avoid keystroke logging.

***Public Wi-Fi:** “Customers must avoid using unsecured W-Fi networks or public Wi-Fi as these are easy targets for identity theft cases in online transactions” says Anand of Axis Bank.

***Register for alerts:** This is a very important step since the bank will alert you to any online card transaction or ATM withdrawals the moment these take place. Also remember to update your mobile contact number in case of a change.

***Log out:** “Always log out from social media sites and other online accounts to ensure data security and avoid storing confidential passwords on your mobile phones as these can be used by fraudsters,” says Jayaraman.

***Change passwords:** Keep changing your passwords from time to time to reduce the probability of identity theft.

***Virtual cards:** You can use this prepaid card if you are not a frequent shopper. It is a limited debit card that does not provide the primary card information to the merchant and expires after a day or 48 hours.

Offline preventive measures

Here are some additional precautions you can take to ensure your card is safe.
***Don’t disclose details:** Never reveal your PIN, CVV or password to anyone. Make sure not to respond to e-mails or SMSes that ask for crucial personal or card-related details. No bank or credit card firm is authorised to seek card details from customers on mail or through phone.

***Check statements:** Regularly go through your bank or credit card statements so that you can detect any unauthorised transaction through identity theft and alert the bank immediately.

***Merchants & POS:** At shops or petrol pumps, make sure that the card is not taken by the salesperson to a remote location where you cannot see it as the card information can be easily copied and stolen. Also, try shopping with retailers that use chip-enabled card readers. Though not every merchant has such readers, this provision can help bring down the risk of fraudulent card activity significantly.

***Don’t sign blank receipts:** Ensure that you never sign a blank receipt, and mark through any blank lines or spaces before signing so that nobody can add an additional amount to your transaction.

WHAT TO DO IF CHEATED

In case of card identity theft or a fraudulent offline or online transaction, report

In case of card identity theft or a fraudulent offline or online transaction, report the loss immediately to the bank or card provider and have the card blocked. For this, make sure that you have the customer care number of your bank handy. Follow it up with a letter or e-mail. It is also advisable to lodge an FIR at the earliest.

If the bank does not respond within a week, approach the nodal officer. If there is no response from the bank within 30 days, contact the banking ombudsman appointed by the RBI (*https://www.rbi.org.in/commonman/English/Scripts/Against-BankABO.aspx*). If this measure too fails, approach the court of law for redressal.

5 TRAPS SET BY FRAUDSTERS AT THE ATM

1. Hidden camera
Tiny, pinhole cameras may be placed on the machine or even the roof at strategic positions to capture your PIN.

2. Card skimmer
These devices are installed on the card reader slot to either copy the information from the magnetic strip of your card or steal the card itself.
***Bulky slot:** If the slot feels slightly bulky or misaligned, in all probability an additional card reader slot has been placed on top of the actual one.

***Loose slot:** If the slot is wobbly or loose, it indicates the presence of a 'Lebanese loop', which is a small plastic device with a barb that holds your card back in the machine. You may think the machine has swallowed your card or it has been stuck.

3. Shoulder surfers
These are people lurking in the ATM room or outside. They will either peer over your shoulder to read your PIN or offer help if your card is stuck.

4. False front
It may be a little difficult to detect as the fake front completely covers the original machine because it is installed on top of it. This allows fraudsters to take your PIN as well as money.

5. Fake keypad
This is placed on top of the actual keypad. If the keypad feels spongy to touch or loose, don't enter your PIN.

(With inputs from Hiral Thanawala and Yogita Khatri.)