

# Credit Card Frauds



*Sept.08, 2016*



# Definitions

- Credit Card – A card allowing the holder to purchasing goods or services on credit
- Debit Card – A card allowing transfer of money from a bank a/c electronically when making a purchase
- ATM Card – A card which allows transactions only on ATM

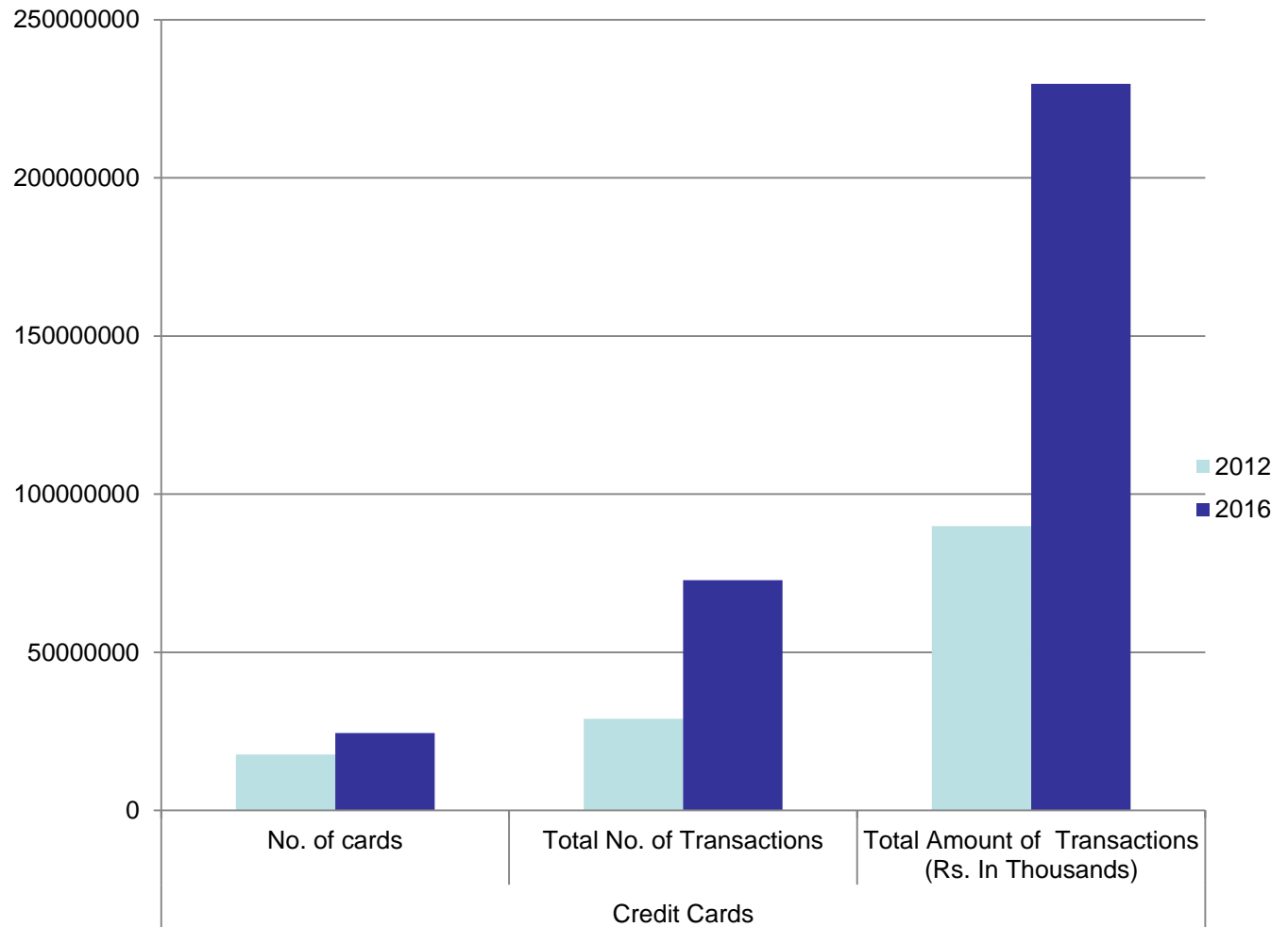


# Overview of Topics

- Recognizing types of Credit Card Fraud
- Protecting yourself from fraud
- Steps to take when fraud strikes

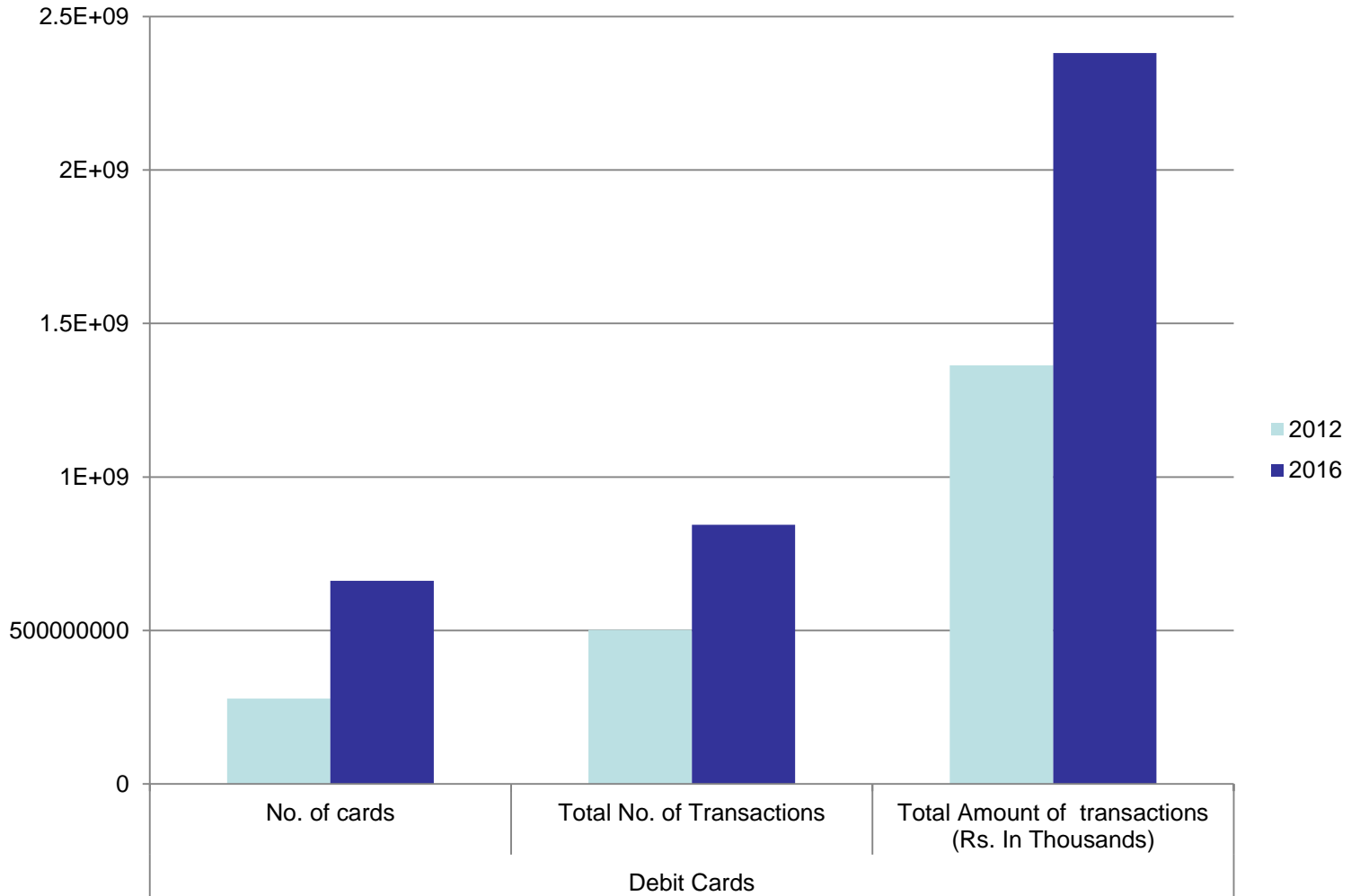


# Why this subject? Credit cards



# Why this subject?

## Debit cards





# Card Fraud

- Card information is stolen from garbage or mailbox
- Card information given to unfamiliar individuals
- Cards are lost or stolen
- Diversion of electronic mail
- Card information is copied
- Duplicate cards are got issued by impersonation
- SIM card swap



# What happens then?

- Counterfeit cards
- Unauthorized charges to card



# Card information is stolen from garbage or mailbox

- Dumpster Diving
  - Stealing credit card information from discarded receipts or account statements in people's garbage.
  - Shred unwanted documents that contain Aadhar numbers, bank and credit card information and other sensitive financial information





# Card information given to unfamiliar individuals

- Vishing
  - Act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.





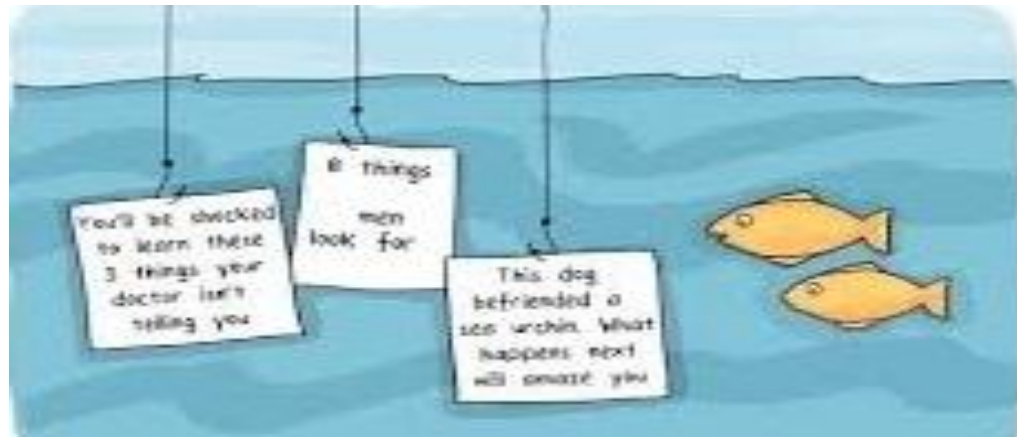
# Cards are lost or stolen





# Diversion of electronic mail

- “Phishing”
  - Email is received by many
  - Directed to fake websites which look like original websites on responding
  - Some people respond
  - Account numbers, passwords etc. asked
  - Information is used for theft



# Phishing



**Warning Notification : Your credit card has been suspended** Tue, Jan 29, 2013

From: Visa / MasterCard®  
To: len@lenpenzo.com

**Unprofessional Presentation**

**Broken English**

**Strange requests**

**Misleading link to scam website**

Dear (e) Customer (e)

Your bank offers you a new user Check level of security. Visa (Verified by Visa) and MasterCard SecureCode (MasterCard rescues Code) to serve our customers and ensure best banking service, against activities fraudulent. Protect Your Credit Card against the use not authorize is our primary concern. Grasse this latest update, we ask all our client update information and the coordinates of your bank account and your credit card or debit card by clicking on the link below.

[Click here to access your form security .](#)

Note: If this is not resolved within 72 hours we will be forced to **suspend** your credit card permanently as it may be used fraudulently. The purpose of this verification is to ensure that your credit card account has not been fraudulently used.

Best regards,  
Customer Support Service.  
Copyright © 1999-2013

**Misspelled or Non-existent words**

**Email address not from stated sender**

**Add to Contacts**

Visa / MasterCard®

Email: externalcommunications@ca-cib.com

Save Cancel

**annual-updates-security.empriseccs.com/redirect.php**

©2013 Len Penzo dot Com

# Card information is copied

- “Skimming”
  - Use of skimmers
  - Storing information parallel on swiping
  - Used for making duplicate cards
  - Using the card number and CVV

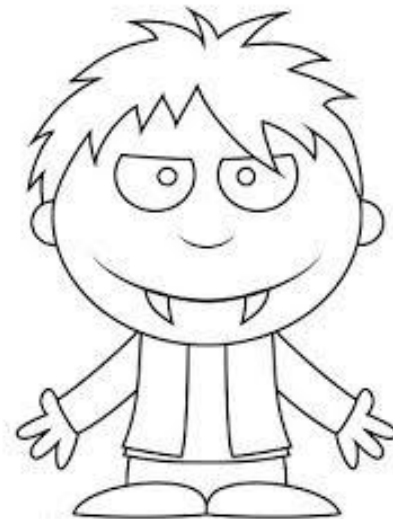


# Duplicate cards are got issued by impersonation

- “ID Theft” - Identity theft is the use of someone’s personal information, such as Aadhar number or PAN or date of birth etc. to commit fraud.



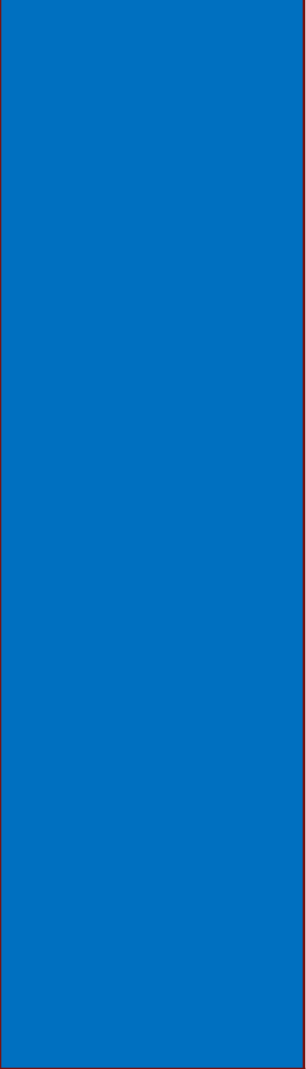
[How-to-draw-funny-cartoons.com](http://How-to-draw-funny-cartoons.com)



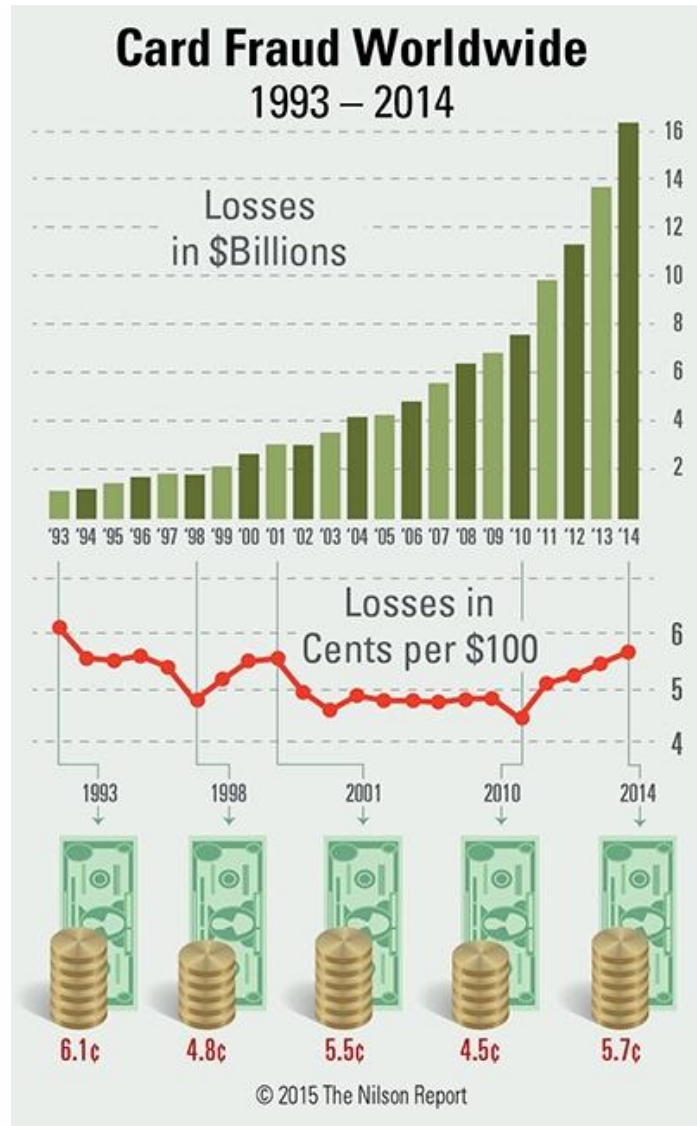
[How-to-draw-funny-cartoons.com](http://How-to-draw-funny-cartoons.com)

# Some other terms

- Shoulder Surfing - Practice of spying on the user of a cash-dispensing machine or other electronic device in order to obtain their personal identification number, password, etc.
- Shimming – For EMV cards (Europay, Mastercard, Visa)



# Why does credit card fraud matter?





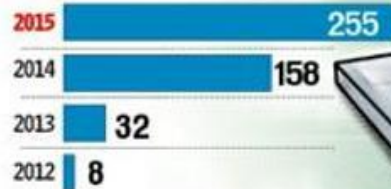
# Why does credit card fraud matter?

## EVERY POLICE STATION GETS 3-4 COMPLAINTS A DAY

Every police station, on an average, gets three to four complaints on cybercrime. Police stations in the city lack infrastructure and expertise to investigate cybercrime cases.



### CREDIT, DEBIT CARD FRAUDS ON THE RISE



### STATE'S CYBERCRIME CONTROL PROJECT

- The project was first drafted for Mumbai but was later extended to the state, with every district police having the infrastructure to deal with the menace
- Formation of four cyber cells equipped with latest hardware, software and tools
- Developing a force of 1,000 trained cyber cops
- Special fast-track courts dedicated to cyber crime cases
- Training prosecutors and judicial officers
- A Computer Emergency Response Team (CERT)

### POLICE CHIEF MEETS REPRESENTATIVE OF 19 BANKS

**Commissioner of police** Ahmed Javed met senior officials of as many as 19 banks, including MDs, CEOs, directors and senior risk managers to discuss measures taken for data security. The meeting was held at the police commissioner office. Possible measures on data security that banks can put in place internally and co-operation with police in investigating cyber crimes were discussed

### CITY POLICE YET TO GET FOUR CYBER CELLS, BUT GETS A DCP CYBER

**Though the cyber crime** cases are increasing manifold, city police are awaiting approvals for four CCICs which will look after cybercrimes of south, east-central and north regions. However, on Monday, city police got its first deputy commissioner of police (DCP)-cyber, M Rajkumar

### BKC CYBER CRIME POLICE STATION OVERBURDENED

**City's only cyber police station** has only 15 officers, including a senior inspector and two senior inspectors

**Since only an officer** of inspector rank can be official investigating officer of a crime

under the IT Act, the two PIs are overburdened with over 100 cases each

**Around 250 FIRs** have been filed at the BKC cybercrime police station this year

**In order to tackle** the manpower issue, the police sent a recommendation earlier this year asking for amendment to section 78 of the IT Act and allow officers of police sub-inspector (PSI) rank and above to probe cases



## The bottom line...

- All cardholders pay for credit card fraud losses
  - Victims spend time and money to repair the damage
  - Credit card issuers charge higher fees and interest rates to cover their losses
  - Victims of ID theft are not held liable for losses depending on terms, but it takes time and effort for victims to prove fraud.

# Security Codes

- Security codes for Visa, MasterCard and Discover cards are the 3 digits located on the back of the card in the signature box.
- 3D Secure code
- OTP





# New Cards

- For added protection, credit card issuers ask you to call from home to activate new credit cards
- As soon as you receive your new card, sign the back of it.
- Record all your account numbers and company contact information and keep the record in a secure place
- Never write down your personal identification number (PIN)
- Never give your PIN to anyone



# Protect your account numbers

- Never write your credit card number on post cards or on the outside of envelopes
- Never provide your card number on the phone, unless you know it's a legitimate, reputable business
- Never give your account number to anyone who calls you on the phone or sends you an e-mail
- If you let others use your card, you are responsible for charges



# Billing Statements

- Review credit card statements closely on the day they arrive
  - Report any questionable charges to your card issuer immediately
- A missing credit card statement may indicate stolen mail
  - Contact your card issuer right away if your bill doesn't arrive around the usual date



# Online account access

- If you have a computer, consider signing up for online account access
- This way you can track your account activity between statements



# Liability

- Fraud victims are not generally required to pay for unauthorized charges
- Victims may be liable for up to certain amount, depending on the circumstances





# Watch your credit card

- Watch closely when store or restaurant employees handle your card to make sure they are not copying or “Skimming” your credit card number
- After you make a purchase and your card is handed back to you, make sure the card is yours.



# Safeguard your mailbox

- Notify the post office and your credit card company immediately if you change your address
- Lock your mailbox. Never leave mail in an unlocked mail box or apartment building lobby
- Put your return address on out-going mail
- Shred unwanted credit card solicitations before discarding



# Internet Safeguards

- If you bank online, don't use “automatic sign on” for bank or credit card sites
- Avoid providing your credit card number to websites offering “free access”
- Install a firewall in your computer to prevent unauthorized access from hackers



# Reporting credit card fraud

- To report credit card fraud
  - Call your card company immediately about
    - Lost or stolen cards or PIN numbers
    - Unauthorized charges on your statement
  - Request a fraud affidavit
  - Get a police report if necessary



# Dispute Resolution

## IN CASE OF CREDIT CARD FRAUD

### THE JUSTICE HOOPS

- **BANK**  
What it costs? **Nil**  
Time it takes: **30-45 days**
- **BANKING OMBUDSMAN**  
What it costs? **Nil**  
Time it takes: **30 days**
- **APPELLATE AUTHORITY**  
What it costs? **Nil**  
Time it takes: **Reserve Bank of India says it replies as soon as complaint is received**
- **COURT**  
What it costs? **Depends on the lawyer's fee**  
Time it takes: **Can extend into many years**

### TIPS TO AVOID FRAUDS

- Use the virtual keyboard to key in the password
- Change your password frequently
- Use a combination of numbers, alphabets and special characters to make your password strong
- Go for credit cards that are chip-based as they are more secure as compared to those having magnetic strips
- Before logging in, check if the site has https and the lock sign in the address bar. In https, "s" stands for secured



# Legal issues

- IPC – Section 419,420
- IT Act – Section 66C,66D



Thank you