BARCLAYS

Fraud and Cybersecurity Awareness

Fraud

- Headline Figures
- Common Fraud Types
- Corporate Challenges

Headline Figures - India

According to the RBI, while the number of fraud cases declined from 24,791 in 2009-10 to 13,293 in 2012–13 i.e a 46% drop , the amount involved has increased substantially from 2,038 crore to 8,646 crore i.e. an increase of 324%"

Since 2011, 37,721cases of cyber frauds have been reported by RBI / CBI, involving Rs. 497 Cr.

According to RBI, in 2012, 8,322 cases of cyber frauds amounting to 527 million INR were reported. Although the number of cases reported decreased from 15,018 in 2010, the total amount involved increased from 405 in 2012, implying that the average value per cyber fraud case has increased significantly

National crime records bureau statistics :-

- Total number of cases of cybercrime registered in India in 2013: 4,356
- Total number of arrests made: 2,098

In India, frauds worth 11,022 crore INR were unearthed in public sector banks between April–December 2014; 2,100 cases of fraud were reported to the RBI

According to the 2013 Norton Report, India ranks among the top 5 countries in terms of Number of cybercrime incidents such as Ransomware, identity theft and phishing attacks

According to the PwC Global Economic Crime Survey 2014, cybercrime was one of the top Economic crimes reported by organisations across the world, including India.

Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through/ at an internet banking channel, ATMs and other payment channels like credit/ debit/ prepaid cards), whereas advance-related fraud accounted for a major proportion (64%) of the total amount involved in fraud.

Evovlving frauds trends over the years

1990–1999

- *Hawala transactions*
- *Ponzi schemes*
- *Fake currency*
- *Cheque forgery*
- *Advancing loans without adequate due diligence*
- *Siphoning of investors' money through fictitious companies*
- *Use of fictitious government securities*

2000–2015

- *Tax evasion and money laundering*
- *Black money stashed abroad*
- *Cybercrime*
- *Debit/credit card fraud*
- *Identity theft*
- *Fake demat accounts*
- *Benami accounts*
- *Collusive frauds emanating kickbacks to employee of financial institutions*
- *Use of forged instruments such as stamp papers and shares*
- *Violation of Know Your Customer (KYC) norms*

Common Fraud Types

Cyber Fraud
- Social engineering: manipulating situations and people
- Malware: software used to obtain personal information
- Hacking

Invoice Fraud
- Organisation is tricked into changing bank account payee details for a payment, where the computers are infected by Trojans / Malwares.

Cheque Fraud
- Intercepted, amended, counterfeit
- Over-payments, requests for refunds

Lending Fraud
- Facilities granted on fraudulent basis
- Clients turning to deception during trading difficulties

Internal Fraud
- Where controls are not operated or controls have not been reviewed - can lead to abuse
- Employment screening
- Payment processes - sole authorisation, password and card sharing
- Reconciliation of accounts and reviews of spending, segregation of duties
- Control thresholds

Corporate challenges

- The ability to deliver new products for new markets
- Need to balance reduction in fraud losses with maintaining customer experience
- An increase in the use of email
- SMS channels being attacked
- A consistent Cyber attack threat

Cybersecurity

BARCLAYS

Social Engineering - threat

The use of social media or social engineering to facilitate fraud:

"The clever manipulation of the natural human tendency to trust",

Kevin Mitnick – former hacker

This is a method some attackers use to deceive people by getting them to open malicious webpages and run unwanted file attachments.

Uses

- Gathering data and passwords
- Stealing cash and data
- Infecting machines

Protection

- Ensure browsers navigate to correct web addresses
- Authentication on systems.
- Don't click on link or emails.

Ransomware

Ransomware is software that denies you access to your files or computer until you pay a person a ransom –

Uses:

- Access personal files.
- Holds your data hostage.
- Makes copies of files and deletes originals.
- Offers bribes / blackmail to retrieve files.

Protection

- Update computer software
- Avoid clicking on links or opening unexpected emails.
- Have a pop-up blocker running.
- Always back-up valuable information.

Spyware

Spyware is a piece of software that can allow advertisers or potentially hackers to gather information from a persons PC without permission –

Uses:

- Can report activity to unauthorised 3rd parties.
- Can slow down and make pc's crash.
- It can consume the processing speed of a pc and consume memory.
- It can track users activities.

Protection

- Use a firewall
- Ensure latest updates are installed.
- Run anti spyware software.
- Run virus scans on a regular basis.
- Delete any unknown sourced emails.

Adware

Adware is software that displays advertisements on your computer. It is often only there for legitimate reasons, but can be used to gather information that you do not want to share with others.

Uses:

- Tracking people online.
- Spying
- Increases Ad revenue
- Driving more traffic to other websites.

Protection

- Authorise adware programme to remove during scans.
- Install dedicated programmes for detecting adware.

Malware

Malware is malicious software that is used to disrupt a computers operation and gather sensitive information. This software can also be used to gain access to a private computer network –

Uses:

- Spam emails
- Track users keystrokes
- Access Personal information.
- It can modify, delete and upload files and data.

Protection

- Use a firewall
- Ensure latest updates are installed.
- Run anti virus software.
- Run anti spam software.

Spear phishing

Spear phishing is a fraudulent email that targets organisations or customers and it is looking for access to confidential data.

Uses:

- Will be looking for usernames and passwords.
- Tricks users with fake emails.

Protection

- Change passwords on a regular basis.
- Ensure latest updates are installed.
- Always check email source.
- Check the links you click on in an email and the actual URL that is the landing page.
- Secure passwords

Virus - threat

A computer programme usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into others. This virus will usually perform a malicious action (such as destroying data)

Uses:

- Spam emails
- Steel Data
- Give hackers control
- Take over computer

Protection

- Use a firewall
- Ensure latest updates are installed.
- Run anti virus software.
- Don't open unexpected email attachments.
- User the browser privacy settings
- Use a pop up blocker with the browser.

Social Media

Publicly available information can be used to gather information on a potential attack victim. Then a virus can be published on a reputable social media platform that could look like a genuine securely on a PC.

Protect against

- New and emerging threats.
- 0 day exploits that are difficult to defend against.

How it works

- Social media platforms are vulnerable to hackers.
- Information may need to be verified from other reputable sources.

Privacy Settings – Social media

Privacy settings protect the personal information of users to social media platforms.

Protect against

- Hackers being able to build a profile of individuals and write phising emails.
- Hackers can potentially trick users into clicking on tagged media of their friends with hidden malware.
- Hide sensitive information from being viewed by anyone on social media networks.

How it works

- A change can be made on how people view you profiles on websites.
- Information may need to be verified from other reputable sources.

Password Manager – protection tool

There is now password management software that can store and manage passwords. When you choose unique passwords it will encypt them and store them securely on a PC.

Uses

- All accounts being compromised.
- Separate passwords for account.
- Passwords can be more unique adding a layer of security.

How it works

- In using some of this software it can create random passwords.
- A person would never have to remember multiple passwords again.
- They will store all passwords for all accounts.

Email

- Email is an excellent communication tool. However email is frequently used to deliver unwanted material which can cause considerable harm to the business and potentially to the email infrastructure
- Do not forward emails which don't make sense
- Do not open attachments from unknown sources
- Do not readily click on links in emails from unknown sources
- Do not respond to emails received unexpectedly even if the email looks like it has come from a legitimate source

- **Report all cases of emails received from unknown sources to internetsecurity@barclays.com prior to opening and clicking on any links / attachments embedded in it**

Client Breach – Target

40 million – credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

70 million – records stolen that included the name, address, email address and phone number of Target shoppers.

46% – drop in profits at Target in the fourth quarter of 2013, compared with the year before.

$200m – estimated cost to credit unions and community banks for reissuing 21.8 million cards - about half of the total stolen in the Target breach.

$100m – amount Target says it will spend upgrading their payment terminals to support Chip-and-PIN enabled cards.

0 – The number of customer cards that Chip-and-PIN-enabled terminals would have been able to stop the fraudsters from stealing had Target put the technology in place prior to the breach (without end-to-end encryption of card data, the card numbers and expiration dates can still be stolen and used in online transactions).

1 million – 3 million – The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud before issuing banks cancelled the remainder(based on interviews with three different banks, which found that between 3-7 percent of all cards they were told by Visa/MasterCard were compromised actually ended up experiencing fraud).

$53.7 million – The income that hackers likely generated from the sale of 2 million cards stolen from Target and sold at the mid-range price of $26.85 (the median price between $18.00 and $35.70).

Additional Information Sources and Assistance

Cyber Crime, Assistant Commissioner of Police, CCPS,BKC Police Station Complex, Mumbai
Ph:022-26504008

Contact Details
Head Office Tel: +91 - 022 - 22653714

Email: cybercell.mumbai@mahapolice.gov.in

http://cybercellmumbai.gov.in/html/contact-us.html

For cases of victims of Invoice Frauds please reach out to

Reportascam@barclayscorp.com
cc Paresh.Tamhankar@barclays.com

Please do visit Barclays.in for additional information on various fraud types & How to protect yourself

http://www.barclays.in/secrity-scam-alerts.html

Disclaimer

Barclays offers corporate banking products and services to its clients through Barclays Bank PLC. This presentation has been prepared by Barclays Bank PLC ("Barclays"). This presentation is for discussion purposes only, and shall not constitute any offer to sell or the solicitation of any offer to buy any security, provide any underwriting commitment, or make any offer of financing on the part of Barclays, nor is it intended to give rise to any legal relationship between Barclays and you or any other person, nor is it a recommendation to buy any securities or enter into any transaction or financing. Customers must consult their own regulatory, legal, tax, accounting and other advisers prior to making a determination as to whether to purchase any product, enter into any transaction of financing or invest in any securities to which this presentation relates. Any pricing in this presentation is indicative. Although the statements of fact in this presentation have been obtained from and are based upon sources that Barclays believes to be reliable, Barclays does not guarantee their accuracy or completeness. All opinions and estimates included in this presentation constitute the Barclays' judgment as of the date of this presentation and are subject to change without notice. Any modeling or back testing data contained in this presentation is not intended to be a statement as to future performance. Past performance is no guarantee of future returns. No representation is made by Barclays as to the reasonableness of the assumptions made within or the accuracy or completeness of any models contained herein.
Neither Barclays, nor any officer or employee thereof, accepts any liability whatsoever for any direct or consequential losses arising from any use of this presentation or the information contained herein, or out of the use of or reliance on any information or data set out herein.

Barclays and its respective officers, directors, partners and employees, including persons involved in the preparation or issuance of this presentation, may from time to time act as manager, co-manager or underwriter of a public offering or otherwise deal in, hold or act as market-makers or advisers, brokers or commercial and/or investment bankers in relation to any securities or related derivatives which are identical or similar to any securities or derivatives referred to in this presentation.

Barclays Bank PLC is a member of the London Stock Exchange.

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register No. 122702). Registered in England. Registered number is 1026167 with registered office at 1 Churchill Place, London E14 5HP.