ISSN:0975-9646

A Solutions Provided to Secured Your Online Banking Frauds

Komal Saxena[1] ,Dr. Anurag Awasthi[2]
[1]*Ph.D Scholar,*
[1,2]*Singhania university*

Abstract:-Growth of credit card and debit card usage along with online internet banking has led to a tremendous spurt in the amount of banking frauds. It is in the interests of institutions as well as individuals to become aware of the types of online banking frauds and take adequate measures to keep themselves protected. It is important for institutions to safeguard their interests, that of the customers and their reputation. For individuals it is important to safeguard their monies.

1. ONLINE FRAUD

The rise of the internet has meant that it is easy for cyber criminals to carry out their nefarious operations from anywhere in the world and target financial institutions. Their task becomes easy in so far as huge amounts can be moved electronically from one bank account in one country to another bank account in another country. That makes it difficult and sometimes impossible for law enforcement agents to trap and catch such perpetrators, much less recover amounts stolen.

From the legal perspective online fraud is a crime that involves the use of the internet as a medium. The fraud can be something like identity theft or financial fraud or using tactics such as email schemes and phishing attacks in order to obtain credit card and other personal details. This is not all. Cyber criminals use many different methods such as selling products through the internet in which they receive payments but do not deliver. Even reputed online shopping sites commit frauds of some kind of the other by offers that appear too good to be true and, in fact, are.

Individuals suffer loss of money at the most and the inconvenience of having to block credit or debit cards and having to obtain new ones. Financial institutions, on the other hand, suffer huge losses not only in monetary terms but also in terms of loss of confidence of customers and an adverse brand image. For them, it is more imperative to put in place measures that will keep them protected against any such attempts at online frauds. Even though it is expensive financial institutions must maintain anti-fraud teams and technologies to anticipate, detect and prevent any attempts at online frauds.

1.1Types of fraud committed online

There are dozens of different types of online frauds being committed all the time. Broadly speaking, online frauds can be classified into different categories such as:

- Online auction frauds
- Counterfeit money orders and cashier check fraud
- Advanced fee scams
- Charities fraud
- Investment fraud
- Nigerian 4-1-9 scam
- Ponzi schemes
- Debt elimination fraud
- Identity fraud in the form of hacking, phishing, spoofing, spam, spyware and identity theft
- Foreign lottery fraud
- Online advertising fraud, money laundering and pyramid schemes

1.2 Financial Frauds

1.2(a)**Cross border fraud** targets individuals more than institutions. Such frauds commonly involve promises of prizes and lottery winnings as well as low cost travel and credit card loss protection. Individuals are typically promised large sums of money if they make payment of minor fees.

1.2(b)Phishing is a common method employed by cyber criminals to lure unsuspecting people to reveal their credit card numbers, ID and password. The most common route is to send an email that requests recipients to click on a link that takes them to a fake website where they are required to disclose their details.

1.2(c) Identity theft is damaging in that criminals can make fraudulent use of credit cards or steal identity details in order to open false accounts or even obtain loans. Personal details can be obtained online, through spyware targeting mobiles and laptops and from papers disposed off carelessly.

1.2(d) Cyber criminals may launch viruses and Trojans that gather data from a target's computer and surreptitiously transmit these to the hacker.

1.2(e) Card skimming is another type of fraud in which data on the magnetic stripe and PIN data is captured illegally at any POS machine or at ATMs, encoding them into another card and using such cards to withdraw cash or make purchases.

1.2(f) **Fraudsters** may resort to the simple expedient of making phone calls, purporting to call from a bank and ask for details of credit or debit card for "verification" purposes. Similarly, SMS may be used as a route to target the unwary and obtain vital credit or debit card details.

1.2(g) **Wire Transfer fraud:-** of more relevance of institutions and of great concern is the growing amount of wire transfer fraud and automated clearing house transaction fraud. Large sums of monies can be transferred electronically in a matter of minutes. Businesses are targeted and, in majority of instances, it is not the customer but the bank that has to bear the brunt of the loss.

2) **EXPANSION OF CARD FRAUD YEAR-WISE[3]**

	1980	1990	2000	2010	2015
Fraudsters	Individuals	Teams	Local Crime Rings	Global crime Rings	Global Crime rings with decentralization Organisation
Target	Consumers	Small Retailers	Larger Retailers	Banks Processors	Payment Industry
Leading fraud types	Lost/stolen, Intercepted	Domestic, Counterfeiting/ Skimming	Identity theft, Phishing, Rudimentary data compromise	Cross-border data Compromise, CNP fraud, 3D- Secure Fraud, ATM fraud, ID Fraud	Cross- border data compromise, CNP fraud, ATM fraud, ID fraud, Pharming Hacking
Types of Cards targeted	Travel & Entertainment cards	Premium Credit Cards	Mass Market credit Cards	All types: Credit Cards, debit Cards, Pre-Paid Cards	All types: credit cards, debit cards, Prepaid cards, banking Accounts.
Necessary resources	Opportunism	Rudimentary Knowledge	Technical Know How	Audacity, Technical expertise, Insider information, Global connections	Audacity, Technical expertise, Insider information, Global Connections

3.1 **TOTAL CARD FRAUD LOSSES COUNTRY-WISE [3]**

	EU	FRANCE	NETHERLANDS	UK	CANADA	USA
Population(M)	508.1	65.7	16.8	64.1	35.1	313.9
Number of Cards(m)	759.7	85.5	30.4	157.3	105.0	827.4
Card Payments value(€bn)	2,204.4	438.4	100.3	653.6	417.2	3,438.4
ATM withdrawals value(€bn)	1,418.3	135.6	51.5	242.5	Na	534.7
EMV Implementation	Cards:81.6%	Complete	Complete	Complete	Debit cards:95%	--------
Total of card fraud Losses(€m)	1,330.0	405.8	41.9	530.3	361.5	4,148.5
Card fraud loss ratio	0.038%	0.071%	0.028%	0.0059%	0.087%	0.104%

Notes: 1. Number of cards covers both debit and credit and e-purses. Card fraud losses cover both domestic and international transactions. 2. EU card fraud figures and all USA figures are from 2012. Canadian and USA card fraud ratios are calculated in order to comply with European figures. 3. France: Statistics cover 68.4 million'CB' bank cards and Moneo e-purses and 17.1 million French "private" cards issued by third parties. 4. Netherlands: Number of cards comprises 24.5 million debit cards and 5.9 million credit/delayed debit cards. 5. UK: Number of cards includes 0.19 million ATM only, 95.7 million debit cards and 57.6 million credit/delayed debit cards. 6. Canada: Number of cards includes 23.9 million debit cards and 81.1 million credit/delayed debit cards. 7. USA: Number of cards includes 290.8 million debit cards and 905.6 million credit/delayed debit cards. Sources:" European Central Bank (ECB"), "Bank of International Settlement (BIS)"; for other sources see above. [3]

4 PREVENTIONS & PRECAUTIONS:

Prevention is always better than cure and before any crime to be committed. One has to take the precaution certain Points can be helped us to or prevent from online crime

4.1To protect yourself with phishing attacks

(a) Consider all email requests for personal information to be *apprehensive*

(b) Do not respond to such emails or enter information on questionable websites

(c) Check the legitimacy of the inquiry by contacting the number on the back of your credit card

(d) Report suspicious emails or websites to your financial institution

4.2 Other Ways to Prevent yourself from Online fraud:-

a) Update your software's and use current virus protection.

b) Create strong passwords by using at least one spl character

c) Don't except or received emails from unknown.(Restricted your email box)

d) Use your pop-up blocker

e) Download files only from well-Known sites

f) Sign up for email/text "transaction alerts" from your bank to keep track of your purchases

g) Remove history whenever use your id's credit card, Smart Card etc.

h) Remove Log list from the net.

i) Always log off from your internet managing an account session.

4.3 **Card Fraud Prevention**

Types of Misuse	Prevention Measures	Developments
Domestic/International transactions at EMV POS &ATMs	EMV with DDA/CDA, pin-only, SMS notification Cardholder awareness	DDA to CDA Dynamic authentication
International transaction in non-EMV POS & ATMs	Prevention of initial data capture. -Merchant(skimming protection, PCIDSS) -ATM security(skimming protection) .Issuer and acquirer monitoring: -card use, rule-based fraud prevention -major location of POS &ATM fraud .Cardholder awareness(pre-notation of International travel, SMS notification) Virus protection	Global EMV Rollout, including now USA . Dynamic authentication .Chip only cards(VPAY) .Geo-blocking .phase-out of magstripe processing of EMV card
Card-not-present, especially online transection	prevention of initial data capture: -Merchant(PCIDSS), -ATM security(skimming protection) .card security codes(eg CVC2,CW2,CID,CID2) 3D-secure combined with one time authentication code, Cardholder awareness(use of anti-virus software, secure websites, etc)	. Dynamic one time authentication codes .Geo-blocking(EG.:- Mastro-Cards) .MCC blocking . Tokenization .Digital wallet .Mobile phone location

5.) PROTECTION AGAINST ONLINE FRAUDS

Protection involves prevention and being careful about how one uses credit or debit cards. It also involves advanced security measures such as putting in place anti-virus and anti-spyware solutions, a stronger and more secure firewall and use of specialized tools to counteract and thwart attempts.

As far prevention of card fraud is concerned banking institutions have introduced measures such as PIN, SMS notification and EMV chips along with teaching card holders to be careful while using cards at ATMs, POS or online. Where ATM and POS transactions are concerned measures have been developed to prevent data capture and prevent skimming at the terminals. Other measures such as card security codes and 3D secure as well as one time passwords have helped to some degree.

Individuals are advised to make their computers secure by the use of anti-virus, anti-malware and anti-spyware software. It is a smart move not to store passwords and Pin details in the smartphone or computer and users must also keep a watch on the system performance. Awareness programs have helped people to be cautious about responding to fake mails and to check for “https” secure prefix while making card transactions. A good idea is to use a separate browser dedicated only for online banking, clear cache and history when done with and monitor all transactions. Institutions also issue smart cards and USB tokens for authentication purposes. Institutions have also implemented transaction monitoring software that keeps track of the transaction parameters and compares it with history in its data bank, thus being able to flag any suspicious activity.

5.1 F5 Web Fraud Protection[2]

There are as many suggestions and recommendations for individuals to guard themselves against attempts at fraud as there are smart methods developed by cyber criminals. In the end, it is for the individual to be informed and aware. However, for institutions, specific solutions are available to take care of issues related to banking online. Prevention is better than cure and with this in view F5 works perfectly as an advance warning system by detecting changes in HTML code, scripts, attempts at automated transfers and phishing attempts targeted at financial applications and at stealing user credentials.

Breaches that cause no monetary loss are not to be ignored because they can damage reputation of an institution and make it appear that it is vulnerable and not secure. F5 has inherent measures with a strong emphasis on prevention and detection as a way to ensure protection of the brand.

The beauty of this system is that end users do not need to install any component on their smartphones or computers. F5 works from the server side, residing at the applications delivery controller end from where it monitors the network and rides along with the applications delivered to users. To the end user the application appears transparent. Developing and deploying software is one thing whose efficacy reduces over time as cyber criminals try to find loopholes. F5 web fraud protection is tied to a malware analysis team that constantly keeps track of the security operations centre for real time detection and prevention of any attempts at online fraud.

As more banks go online and shift most operations online and as most users prefer online banking as well as payments, the threat of online fraud remains Omni present. The only way to counteract dangers is to be better informed and use the right tools such as F5 protection against online frauds.

Conclusion: We can prevent ourselves from Online frauds to take some precautions and used various types of solutions Like F5 Web Fraud solutions and other software’s.

REFERENCES

1. www.frederalreserve.gov
2. www.F5.com / web fraud Protection
3. Alaric Fraud report 2015,
4. www.paymentscardsandmobile.com
5. www.online.fraud Protection
6. www.cyberfraud.com
7. www.timesonline.co.uk/article/0,,2-2135422,00.html.
8. www.microsoft.com/technet/security
9 www.trendmicro.com

AUTHORS

Ms. Komal Saxena
Phd scholar,Singhania University (Raj)
Teaching experience-12 Years
Publication- 6 Paper Published in Reputed Journal

Dr. Anuraag Awasthi
Over 27+ years of rich overseas and indigenous experience (21 years in Corporate and 6+ years in Academics/Consulting) (Worked in India, Japan, France and Thailand. Visited SriLanka and Pakistan.)

- (Ex) Director and Professor (MCA) with Noida Institute of Engineering & Technology (NIET), Greater Noida.
- (Ex) Dean (Faculty of Engineering & Technology), JV Women's University, Jaipur (Taught M.Tech, MCA students)
- (Ex) Director and Professor in IIMT (MBA College), Dehradun.
- Received Shiksha Gaurav Puraskar for 'Excellence in Higher Education' (2014)
- Received Margdarshan Award for 'Innovation and Excellence in Mentorship' (2013)
- Received 'Bharat Gaurav' Sammaan for outstanding individual accomplishments (2012)
- Received 'Rajiv Gandhi Excellence Award-2012 from Shri Sriprakash Jaiswal, Hon'ble Minister, Govt. of India, New Delhi for excellence in Technical Education (2012)
- Conferred with Distinguished Toastmaster (DTM) award by Toastmasters International, USA for Leadership Skills
- Co-author of book '101 Great Ways to Compete in Today's Job Market'
- Co-author of ebook 'Public Speaking Tips from the Pros'
- Author of book 'Engage to Succeed' (to be released in Mar-15)
- Associated as Visiting Professor with institutions like Jamia Hamdard University, IP University (Bhai Parmanand Institute of Business Studies), Sikkim Manipal University, AIMA (Delhi), European Management Institute, WLC etc