ISSN:0975-9646

Survey on Frauds in Financial Transactions

Vaibhav Bhosale[#1], Megha Jonnalagedda[*2]

[#1]*Department of Information Technology, SGGSIE&T, Nanded, Maharashtra, India-413606*

[*2]*SGGSIE&T, Nanded Maharashtra, India-413606*

***Abstract*— The credit/debit card issuing banks are facing a critical problem of fraudulent transactions. Online purchases may be fraudulent if the credit card number, expiry date and CID number are copied from the card. Identifying fraudulent transactions typically takes hours or days, and many such transactions may slip through before a hold can be put on the card.**

This paper tries to summarize various categories of frauds as well as fraudsters. It also tries to explain various categories of data breach carried out by fraudsters for financial transactions.

A survey of various techniques is done to explore the possibility of proposing a new technique for developing a real-time fraud detection system.

***Keywords*— Fraud, fraudster, data breach, real time fraud detection, financial transactions**

I. INTRODUCTION

A critical problem faced by the issuing banks is that of fraudulent transactions. This problem has, of course, exploded with the high speed nature of electronic submission of credit and debit transactions. An ATM or POS transaction may be fraudulent, for instance, if the credit card is stolen. Online purchases may be fraudulent if the credit card number, expiry date and CID number are copied from the card. This copying can easily be done, for example, by a waiter taking a customer's credit card to pay for a meal or when a phone order is placed and paid for with a credit card. Identifying fraudulent transactions typically takes hours or days, and many such transactions may slip through before a hold can be put on the card. Worse, because the information can be quickly shared with thieves in multiple countries, they can rapidly attack via multiple avenues by submitting many different types of transactions simultaneously, anticipating that the lesser (slower, etc.) infrastructure that some of them may take will allow at least some of them to get through successfully.

II. BACKGROUND

Much of today's consumer activity depends upon plastic Credit and debit cards which are used to purchase products and services as well as to withdraw cash from Automated Teller Machines (ATMs). In order for a card transaction to be approved, the ATM, retailer, or food establishment must submit the request and the bank that issued the card must authorize the purchase or cash withdrawal. Furthermore, this approval must be provided in real-time since the customer is waiting for it. A key problem is quickly identifying suspicious or fraudulent user so that those transactions can be rejected and tracks the source of such transaction to protect users.

A major provider offers interbank transaction-switching services for just this purpose. It uses a redundant network of powerful HP Non Stop computers to implement an authorization and message switch that gathers the customer transactions from the servicing network, routes them to the appropriate issuing banks for authorization, and then returns the authorization or rejection responses back to the servicing network for delivery to the origination point.

A. Fraud statistics by 2013 Association for financial Professionals Payments fraud Survey:

- 61% of organizations experienced attempted or actual payments fraud in 2012
- 27% of respondents reported fraud incidents increased in 2012
- Affected organizations were hit more often (Once victim is always a favourite target)
- 64% of respondents discussed fraud prevention or security with their bank in 2012

Some reputed reports revealed that financial industry was hit the hardest, accounting for 56 per cent of all data records lost or stolen. However, it represented 14 per cent of the total breaches during the quarter worldwide.

III. CATEGORIES OF FRAUDS IN FINANCIAL TRANSACTION

Frauds in financial transactions are categorized as below:

A. Skimming

Skimming is attaching a device to the mouth of an ATM that secretly swipes credit and debit card information when customers slide their cards into the machines. This information is then used by fraudsters to produce counterfeit cards.

Though skimming is a popular form of traditional fraud, the upcoming rollout of EMV (Europay, MasterCard and Visa) in many countries will eliminate the issue of counterfeit cards due to the advance dynamic encrypted data that chip in the cards produce. But expect fraudsters to take advantage of the confusion just prior to the takeover of EMV cards.

Most of the banks are also deploying anti-skimming devices and data analytics to detect skimming patterns and isolate merchants whose terminals may have been compromised.

"Sophistication of fraud and the speed at which it is propagating has increased to alarming levels. Banks need a

more flexible and agile intelligent system to ensure that they can stay ahead of the fraudsters."

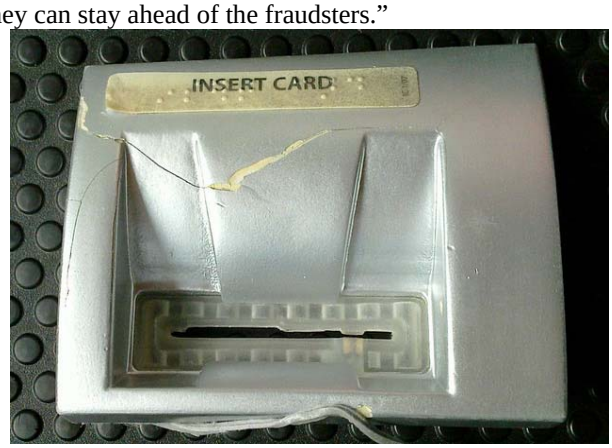

Fig. 1.Skimming

B. Card-Not-Present (CNP)

With the rapid improvements in lifestyle proliferation of online and mobile commerce, card-not present (CNP) fraud is a growing concern to banks. People aren't just using websites like Amazon.com to shop from their home computers; they are now using apps from various stores and businesses on their smart phones to make purchases. The growing popularity of mobile transactions has opened up a whole new avenue for criminals to defraud people. CNP fraud is more prevalent with general retailers, the telecom industry and service providers.

As financial institutes migrate from magnetic strips on cards to the increased security of EMV chips, more criminals will likely shift their focus to CNP fraud. Address verification, card security verification, and security programs from Visa and MasterCard are some of the ways to combat CNP fraud.

For example, attackers can easily steal user credentials with a well-executed spear phishing campaign. Such attacks are nearly impossible to thwart completely, even if an organization implements user training, URL reputation filtering, and other anomaly detection services for email. Once inside an organization, that is typically when attackers steal additional credentials and use them to move laterally throughout the corporate network, collecting more login details and sensitive data along the way.

IV. Categories of Fraudsters

A. Stolen Credentials Buyers

This category includes fraudsters with little bit or no professional computer skills (e.g. Computer Programming, Networking, etc.) who buy hacked (or stolen) credit-card information on an illegal "credit-card sales" website. They buy this credit-card information with the intention of making electronic payment for some good and services on the internet.

In January, Target spokeswoman Molly Snyder confirmed that the Fortune 500 retailer's ongoing forensic investigation of the incident showed that stolen credentials from a third-party vendor played a part in the breach, though Target has declined to name the vendor or the type of credentials used.

Stolen account credentials information have played a vital part in several massive data breaches, including the recent financials Corp. payment card data breach, leaving enterprises to question just how they can fend off attacks utilizing legitimate login details. One expert said user activity monitoring may be the only answer.

A growing number of web services on the Internet have commercial purposes and collect a huge quantity of information related to user's card data. Hackers are aware of this and have exploited numerous techniques to access the precious credential information. Unknowingly access to one of such databases that contains data for millions of card holders could open the doors of heaven for a criminal.

B. Professional Hackers/Crackers

Recent research on Hackers in terms of Computer Security defined a "black hat hacker" (also known as a cracker) as a hacker who violates computer security with malicious intent or for personal gain. They choose their targets using a two-pronged process known as the "pre-hacking stage"; Targeting, Research and Information Gathering, and Finishing the Attack. These types of hackers are highly skilled in Computer Programming and Computer Networking and with such skills can intrude a network of computers. The main purpose of their act of intrusion or hacking is to steal personal or private information (such as credit-card information, bank-account information, etc.) for their own personal gain (for instance creating a "credit-card sales" website where other cyber credit-card fraudsters with little or no computer skills can buy credit-card information).

This type of fraudsters will never stop working hard to come up with new ways to beat security systems with banks, ATMs, and other financial enterprises. This is why banks need to be proactive.

C. Physical plastic stealers

These types of fraudsters physically steal credit-cards and write out the information on them. They physically steal these plastic credit-cards (maybe by pick-pocketing in a crowded place) and write out the credit-card's information with the intention of using this credit-card information to make electronic payment for some goods purchased and/or services availed on the internet.

V. Category of Data Breach for Financial Transactions

In today's increasingly electronic society and with the rapid advances of electronic commerce on the Internet, to detect cyber credit-card fraud activities on the internet, a study conducted on how credit-card information is stolen is a good approach. Listed below are studied different techniques which are used for credit-card fraud information theft.

A. Credit-card fraudulent identity generators

Credit cards are produced in BIN ranges. In this method issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number using mathematical algorithm and generate valid card numbers by changing the last four numbers using a

generator. The expiry date of these cards would most likely be the same as the available cards. Fraudsters create dataset using existing card numbers and use it for generating card information.

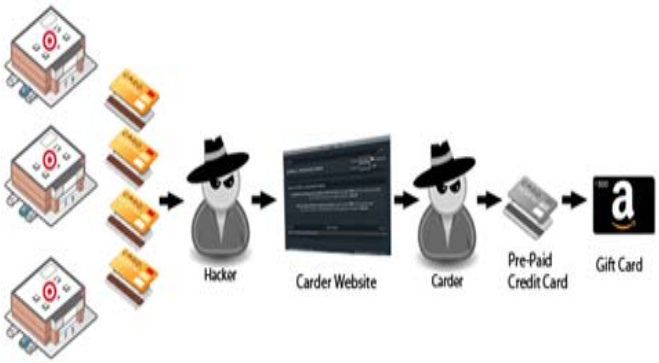

Fig. 2.Fraudulent identity generators

B. Key-logger and Sniffers

Fraudsters with professional Programming or computer skills are able to infect personal computers by installing and automatically running sniffers or key-logger computer programs to log all keyboard inputs made into the computer on a file with the intention of retrieving personal information (like credit-card information, etc.). These black-hat hackers or fraudsters are able to infect user's computers by sending spam emails to computer-users requesting them to download free software or games, or sometimes they create some porn-sites so that when these computer-users browse these porn sites or download those free software or games, the sniffers or key-loggers are automatically downloaded, installed and ran on the user's computers. While the sniffer or key-logger is running under the users' computer, they sniff and log all the keyboard-input made by the user over a connected network. Therefore, any computer-user can unknowingly share their private information (credit-card information, etc.) through viral-infecting software such as these. In some cases, no Programming or computer skill is required to sniff a computer-user's key-board input because this software are also being shared or sold to other cyber credit-card fraudsters with little or no computer skills.

C. Spyware, Site-cloning and False Merchant sites or Phishing

From knowing the website activities of the victimized computer-user on the internet using various spyware programs, electronic or banking websites regularly visited by the computer-user can be cloned and sent to the user for usage with the intention of retrieving personal or private information (like bank log-in's). In the case of false merchant sites, fake websites mostly created to advertise and sell cheap products to computer-users, and thereby asking for payment via credit-card. If a credit-card payment is made on any of these fake merchant sites, the user's credential information is therefore stolen.

D. Rise of Malwares in Point of Sales terminal (POS):

In recent years some very intelligent malwares are detected by various organizations.

At the end of 2012, the Israel-based company *Seculert* announced that it had detected a new malware called *Dexter*, used for parsing memory dumps of specific POS software-related processes looking for Track 1/Track 2 credit card data.

The Dexter targets mainly hotels, restaurants, and big retailers in 40 countries, most of them located in the U.S. and the U.K. One year later, Dexter is still active in Russia, the Middle East, and Southeast Asia, but it isn't the only malware designed to attack point-of-sales systems. In early 2013, Group-IB detected a new POS malware called "DUMP MEMORY GRABBER" just a few months after the detection of the popular malware vSkymmer and Project Hook.

Kaptoxa (pronounced kar-toe-sha) is a type of point-of-sale (POS) malware designed to compromise payment information systems.

This malware is memory-scraping malware, is believed to have been used in several retail data security breaches in 2013, including the attack that compromised the payment data of as many as 70 million customers who shopped at Target, the second-largest discount retailer in the United States. Kaptoxa, which is Russian slang for "potato," has also been nicknamed the "potato malware."

VI. CONCLUSION

This survey paper broadly categorizes, compares, and summarizes from available published technical and review articles in automated fraud detection in recent years. It also defines the professional fraudster, classifies the main types and subtypes of known fraud and presents the nature of data breach collected within affected industries.

This paper is focused on points that must be considered to detect fraud in a real-time transactions and it not prone to errors because of its classification of Transactions (legitimate, Suspicious Fraud and illegitimate).

This research will help to propose intelligent real-time fraud detection system using Neural networks in the business context of mining the data which proposes alternative data and solutions from related domains.

REFERENCES

[1] John Akhilomen "*Data Mining Application for Cyber Credit-card Fraud Detection System*" WCE 2013, July 3 - 5, 2013

[2] Philip K. Chan,Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo "*Distributed Data Mining inCredit Card Fraud Detection*", 1999 IEEE

[3] 2002.White Paper on "*Efficient Risk Management for Online Retail"*, ClearCommerce Product http://www.clearcommerce.com

[4] Management, ClearCommerce Corporation, September 2002. http://www.clearcommerce.com

[5] 2011. "*Global card fraud levels"* http://www.fraudwatchonline.com/news.htm

[6] 2014.*"Introduction to the Business of Stolen Card Data"* http://resources.infosecinstitute.com

[7] 2002. *Online Fruad Report – Online Credit Card Fraud Trends and Merchant's Response*, Mindware Research Group, CyberSource. http://www.cybersource.com

[8] Arvind Narayanan and Vitaly Shmatikov, Privacy and Security Myths and Fallacies of "Personally Identifiable Information" ACM 2010, vol. 53

[9] 2009. "*Global losses from credit card fraud and electronic crime"* www.atmmarketplace.com