Spring 2013

The importance of fraud detection techniques from the Enron case and the T.J. Maxx data breach

Luyao Peng
James Madison University

The Importance of Fraud Detection Techniques From the Enron Case and the T.J. Maxx Data Breach

Luyao Peng

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the degree of

Master of Science

Integrated Science and Technology

May 2013

Table of Contents

Lists of Tables

Lists of Figures

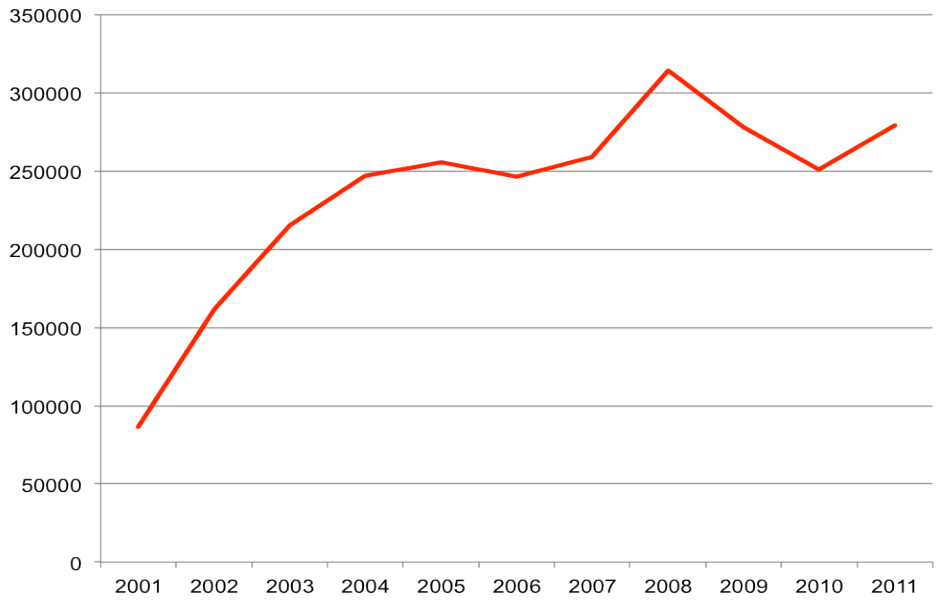
Abstract

This thesis examines the issue of fraud detection and its causes and solutions. After a description of two fraudulent cases Enron scandal (internal fraud), and T.J. Maxx Data Breach (external fraud), it discusses the causes of these two fraud cases using Cressey's "fraud triangle" theory and Albrecht's three-stage theory. It then describes various fraud detection techniques in internal and external fraud. Finally, the recommendations for the improvements of both internal and external fraud detection systems are explained.

I. Introduction

In October 2001, the Enron scandal caused the bankruptcy of the Enron Corporation eventually. At the same time, the scandal also led to the dissolution of Arthur Andersen, which was one of the five largest audit and accountancy partnerships in the world. Enron founder Ken Lay and CEO Jeff Skilling were responsible for most of the crime. They were sentenced for fraud, false statements, and insider trading. Because of these fraudulent activities, Enron lost $60 billion that led to thousands of job cuts and more than $2 billion in employee pension plan losses. Enron scandal, however, was only one instance of the internal fraud as there are thousands of external frauds reported in United States, such as consumer fraud including identity theft, check and credit card fraud, and computer internet fraud. In year 2000, 300,000 credit card numbers stolen from CD Universe. In year 2005, CardSystems Solutions, in violation of agreements with MasterCard and Visa, retained *40 million credit card numbers* for "research purposes" which were subsequently stolen by hackers. In year 2007, TJX Companies hacked and stole 90 million credit cards, debit cards. Fig. 1 clearly demonstrated that the number of identity thefts reported in America has been increasing each year.

Figure 1 Number of Identity Thefts Reported

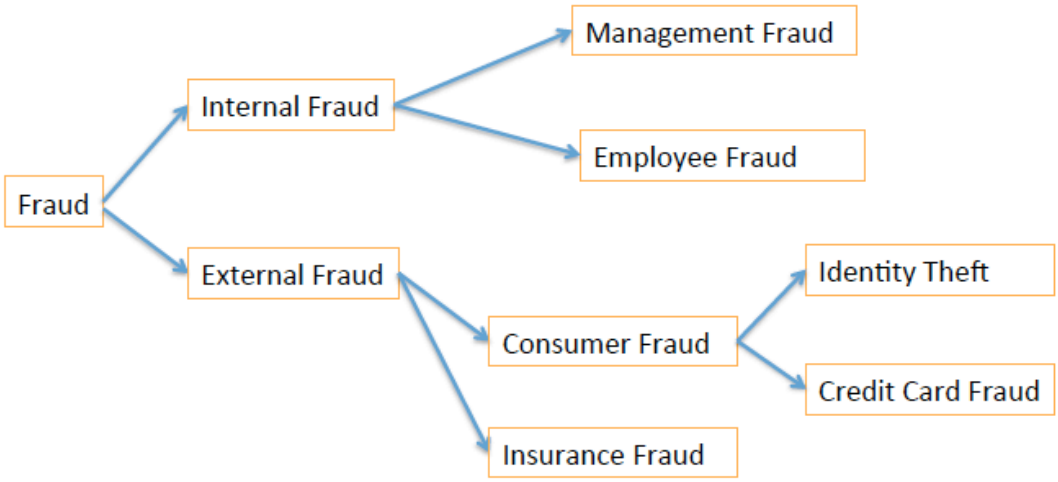


(Source: www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf)

These examples illustrate that suspected fraud, no matter internal or external fraud, will cause severe consequences both inside the company or to the society. Because of these consequences of the fraudulent activities, the technical skills learnt from the fraud cases and the techniques for fraud detection hence play an important role in fraud prevention and deterrence area. The objectives of my thesis are to describe different kinds of fraud, focus on the two major fraud categories: identity theft fraud, and the management fraud. I will analyze TJX data breach and Enron scandal to investigate how fraud occurred and what kinds of techniques are appropriate for these fraud detection and prevention. To solve this issue, my thesis will focus on three components: (1) to describe the fraud categories (2) to analyze the causes led to the Enron scandal and TJX data breach frauds to illustrate the fraudulent issues in this society; (3) to review the techniques for fraud detection and prevention. (4) to provide recommendation for the future about what should be improved for minimize the fraud risk.

II. The Categories of Fraud

Figure 2 The Categories of Fraud



The Classification of Fraud

According to three fraud examiners, Mary-Jo Kranacher, Richard A. Riley, JR, and Joseph T. Wells of a textbook named *Forensic Accounting and Fraud Examination,* fraud, often referred to as the fraudulent act, is an intentional deception, whether by omission or co-mission, that causes its victim to suffer an economic loss and/ or the perpetrator to realize a gain. (Kranacher et al, 2011). Fraud can be categorized by a number of different methods, but they are often categorized as internal and external frauds (Figure 2).

Introduction of Internal Fraud

Internal fraud refers to occupational fraud committed by one or more employees of an organization, which is the most costly and most common fraud (Kranacher et al, 2011). Internal fraud included two types of fraud: management fraud and employee fraud.

According to Elliott and Willingham, management fraud is “the deliberate fraud committed by management that injures investors and creditors through materially misleading financial statements”. Examples of management fraud include: WorldCom, Enron, PharMor, ZZZZ Best, et al. Enron scandal would be analyzed in this study to exemplify how to investigate management fraud. Besides management fraud, employee fraud is another type of internal fraud. Employee fraud is the use of fraudulent means to take money or other properties from an employer. For example, the cashier takes money from someone else’s cash register. For another example, the employee takes the companies’ printer to home as his own.

Introduction of External Fraud

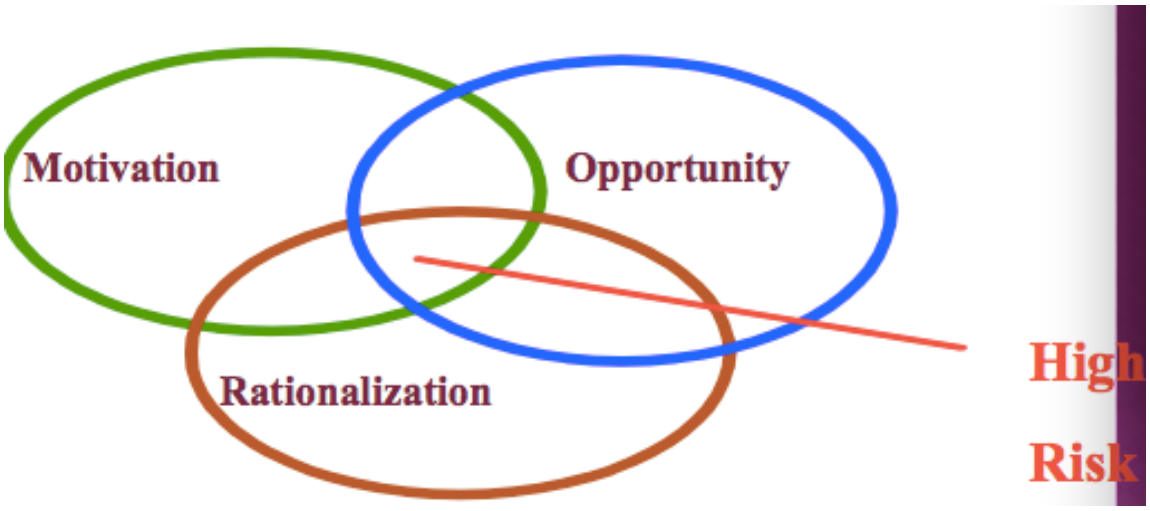
The other type of fraud is external fraud. External fraud refers to offenses committed by individuals against organizations (e.g., insurance fraud), or organizations against individuals (e.g., consumer frauds) (Kranacher et al, 2011). False insurance claims are insurance claims filed with intend to defraud an insurance provider, such as faking death to claim life insurance (Wikipedia, 2013). Consumer fraud includes identity theft, check and credit card fraud, and computer and Internet fraud. My paper will focus on two parts of frauds: management fraud (internal fraud) and identity theft (external fraud). I will investigate Enron scandal as an example to analyze management fraud and TJX data breach to analyze identity theft fraud.

III. Internal Fraud Analysis Method: Cressey's "Fraud Triangle" Theory

Background of Donald R. Cressey& "Fraud Triangle" Theory

Before the investigation, I will introduce the "fraud triangle" theory that helps analyze the management fraud. The theory is developed by Donald R. Cressey who is American criminologist and sociologist, famous for his extensive research into the minds of management and employee criminals (Wikipedia, 2013). The "Fraud Triangle" which attempts to explain the three elements those are generally present when fraud occurs. As Figure 3 shows, the three elements of fraud triangle are the motivation, opportunity, and rationalization. When these three elements are presented, a fraud must be occurred. I will explain each of the three elements as I investigate Enron scandal as follows.

Figure 3 Donald R. Cressey: The Fraud Triangle



(Source: W.Hillison, D. Sinason, and C. Pacini, "The Role of the Internal Auditor in Implementing SAS 82," Corporate Controller, July/August 1998, page 20.)

IV. The Enron Scandal as an Example of Internal Fraud

Introduction of Enron Scandal

In the year 1985, Kenneth Lay merged the company Houston Natural Gas and InterNorth to form Enron. During the period of 1990s, Enron became the seventh-largest company on the Fortune 500 and the sixth-largest energy company in the world. However, as more and more people chose Enron as a good investment, no one thought it could go into bankruptcy. By November 2001, the company's stock crashed from 90 USD a share to 0.02 USD a share. It was a nightmare for all the investors and creditors of Enron. Its founder Ken Lay and CEO Jeff Skilling were responsible for most of the crime which includes that they lie to the stockholders about the real financial situation of Enron, though they knew that Enron was not doing well, they used "off balance sheet entity" to get rid of the big debts of Enron, and they allowed external auditors to do some internal auditor's work which led to Enron's weak internal control. This huge fraud scandal cause thousands of jobs cuts and more than $2 billion in employee pension plan losses. At the same time, the scandal also led to the dissolution of Arthur Andersen that was one of the five largest audit and accountancy partnerships in the world at that time.

Analysis of Enron's Collapse

What caused Enron's collapse? Since Enron scandal is a very complicated case, many reasons contributed to Enron's collapse, however, there are three largest reasons. I will use the Donald R. Cressey's Fraud Triangle theory to analyze each of these reasons below.

1. Motivation

The first reason is that manager level people of Enron were greed motivated. Motivation is the perceived incentive that causes individuals to consider committing fraud. This motivation can arise from financial problems, such as living beyond one's means, poor credit, family medical bills, investment losses, or children's educational expenses (Kranacher et al, 2011). At the same time, the management fraud's motivation often lies in two categories. One is to "to get through a difficult period", such as cash shortage, increased competition and other financial difficulties. The other is "greed motivated", such as employee stock option plans, performance based compensation. As to Enron's scandal, the motivation for the management fraud lies into the "greed motivated". Enron's executives had the stock options on their hand, and they knew that they could become billionaire within a few years and made them did nothing but do the stock speculation. These people just treated the company as their own tool to earn money for themselves. Enron's executives knew they did the wrong thing and they lied to all of their employees and encouraged them to buy more and more Enron's stock, though they knew they were lying and the company was not doing well, and every one just cared for their own benefits. As a result, a large number of families had their life savings in Enron stock, but it's even sadder that the executives sold their stock just before the stock price crashed. The executives made billions collectively because they sold the stock when the value was high. After they sold their stock, the price crashed, and the families lost out. They could not have told the families that the company was going bankrupt, or the stock would have crashed sooner, and the executives would have lost their money. The price of the stock went from 90.00 USD a share, to about .02 cents a share. That means that if you had 90,000 USD in Enron

stocks before the crash, you would end up with just 20.00 USD after the crash. People who worked for Enron lost everything, including their homes. The Enron executives who knew the crash was coming and sold their stock quickly and quietly, stayed rich.

2. **Opportunity**

After perpetrators have the motivation to commit the fraud, the next thing is to seek the opportunities. In management fraud, there are many kinds of opportunities for perpetrators to conduct the fraudulent activities, such as weak internal control, absence of oversight by board of directors, unusual or complex transactions and significant estimates. Enron's "opportunities" are likely the weak internal control and the unusual or complex transactions. Firstly, certain parts of Enron's internal audit work were done by an external audit firm, Arthur Andersen (Locatelli, 2002). Every company should have an internal auditor, and there is a big difference between an internal and an external audit. But what Enron did was to give too much authorization to Arthur Andersen for Enron's internal bookkeeping, thus "blurring a fundamental division of responsibility that companies employ to assure the honesty and completeness of their financial figures" (Stevens & Schwartz, 2006). At the same time, a good internal control requires "senior managers must consider the design of an effective control structure to be a central part of their jobs" (Locatelli, 2002), whereas Enron's senior manager just "waived the company's conflict of interest policy to allow its CFO to invest in the corporation's special purpose entities, then failed to follow up to ensure the mandated compensation controls were being adhered to" (Locatelli, 2002).

Secondly, Enron is a complicatedly structured enterprise. Starting from the middle time of 1990s, Enron developed a complex company system with more than 3,000 entities in the forms of joint ventures, limited-liability companies, partnerships, or other unconsolidated entities (Jackson, 2006). The reason why Enron developed such a large number of entities was because they wanted to get rid of the massive amounts of debt on their books. Enron called these entities as "off-balance sheet entity" (OBSE). Enron used OBSE frequently through keeping these transactions off the company's balance sheet. OBSEs created for a specific purpose, which often referred to as "special or limited purpose entities, are contractually limited to narrow activities that facilitate a company's transfer of or access to assets" (Chandra, Etredge & Stone, 2006). Another key advantage to the sponsoring company for having these entities is that the company's share of the entities' earnings is accounted for in the company's income statement, and the company can also record profits on its transactions with these entities (Jackson, 2006). This means that these entity's earnings can appear on a company's income statement without its debt appearing on the balance sheet. Needless to say, Enron's executives' trick of getting rid of the debts was unfair to all the investors and shareholders. They posted profits or earnings based on how much a given business venture could make and hide the huge debts in the "off balance sheet company".

3. **Rationalization**

Rationalizations include an employee/manager's feeling of job dissatisfaction, lack of recognition for a job well dome, low compensation as well as an attitude of "they owe me". Any thoughts that convince the perpetrators to believe that their actions are

rational even though they know they did the wrong thing. In Enron's management fraud, the rationalization is the misguided loyalty meaning that the perpetrators think they do it for the benefit of the company. For example, according to the movie "*the smartest guys in the room*", the CFO of Enron Andrew Fastow once wanted to give the financial report that contains many fake numbers to the CEO Jeff Skilling to sign the documents, but Jeff Skillling just ignored those fake numbers and said it was good for Enron's future improvement.

Social Impact of Enron

Enron was the most disastrous business scandal in America history. Enron's collapse had a serious effect on the US economy: American investors lost the confidence to invest, the stock price in Wall Street fell continually, and stock price all over the world also fell. After the serious effect of Enron, this whole society reflected deeply about the problems of ethics, enterprise system, and the regulation system inside the enterprise that led to all the fraudulent activities of Enron.

First of all, American societies started to doubt whether enterprises should give stock options to the executives of the company. Stock options are a call option on the common stock of a company, granted by the company to an employee as part of the employee's remuneration package (Wikipedia, 2013). Giving stock options to the executives of a company has been regarded as a successful incentive system in American enterprises management. However, since Enron, the stock options have become the symbol of a company's bad habits and management. Many companies use employee stock option plans to retain and attract employees, the objective being to give employees an incentive to behave in ways that will boost the company's stock

price (Wikipedia, 2013). Some criticize stock options, because they can enhance some companies' executives become billionaire within a few years and make them did nothing but do the stock speculation; these executives just treat the company as their own tool to earn money for themselves. In order to earn money from the stock options, a large number of executives using financial fraud, ignore the long term development of the company, make the stock price higher in a short time, and hurt the investors. It was eventually determined by the Financial Accounting Standards Board, which sets accounting rules for the corporations in America, that the options should be expensed at their fair value to the employees as of the grant date instead of the set price.

Second, people start to consider what kinds of working environment is good for the employee and what kind of regulation system a company should comply with. Enron's working environment had so many ethics problems. In fact, Enron was a very harsh company that emphasized too much on competition and the financial achievement. For example, it had a rating system that required that 20 percent of all the employees had to be rated as "below requirements" every year and then was encouraged to leave Enron (Marianne, 2009). This rating system was the most important reason for the ethics problems in Enron's working environment. At the very first place, Enron's harsh working environments and the strict rating system led a culture of deception. All the employees just focused on how to improve their performance without comply with the ethical code, because they were afraid of losing their jobs. Once some employees began cheating on their work, there were more and more employees started to cheat also as they had no other choices. Gradually, a culture of deception had implemented into Enron's working environment. At the second place, the culture of Enron

concentrated the financial goals too much. The person who fraudulent can achieve the financial goal would become the hero of the company. Most of Enron's employees including the executives concerned about how to make the financial condition of Enron looks good instead of cared about the real financial situation of Enron. Finally, Enron required its employees not to say any information about Enron to the public. Employees had to hide the truth of Enron's financial condition though they knew the real financial condition of Enron. If an employee doubt about the financial condition, she or he will receive punishments from the executives. All in all, employees in Enron worked blindly, protected their own short-term interests if it was an obvious cheat, and hid all the fraudulent behavior in their heart without telling to anyone. This bad culture contributed to Enron's scandal. Enron's executives and most of the employees' unethically behaviors caused the bad working environment of Enron.

V. Management Fraud Detection Techniques

Traditional Management Detection Methods

The analysis of Enron scandal clearly showed that management fraud is a topic of critical interest to investors, analysts, regulators, auditors as well as the general public. Major financial frauds at Enron, WorldCom, Xerox, Qwest, Tyco, HealthSouth, Cendant, and other corporations caused the loss of confidence in the integrity of American business (Carson, 2003) and a severe decline in stock markets worldwide (Whiting et al, 2012). Due to the vicious effects of management fraud, it is necessary that better management fraud detection and prevention techniques need to be implemented into the company. A number of management fraud detection techniques are introduced hereby. A traditional management fraud detection method is the reactive fraud management method based on data mining, neural networks and/or other machine learning techniques to perform complex algorithmic analysis over stored transactional data towards identifying suspicious transactions (Michael & Pedro, 2012). There are three methods that have been used in this area, including regression, decision trees, neural networks (Wei & Gaurav, 2010).

1. Regression

Regression is the most widely used method to detect financial statement fraud (Wei & Gaurav, 2010). In regression method, there are many tools have been used for the transformations of variables in regression models, such as logit, stepwise-logistic, multi-criteria decision aid method and exponential generalized beta two (Wei & Gaurav, 2010). For instance, somebody used a collection data from 76 firms including 38 fraudsters and 38 non-fraudulent firms in Greece. Ten variables and the related

regression model have been used with this management fraud. The objective was to find out the relationship between these factors and the management fraud. It turns out that high debt to total assets, low net profit to total assets, and high financial stress are the best indicators for management fraud.

2. Neural Network

The modern usage of the term often refers to artificial neural networks, consisting artificial neurons or nodes. It is an information-processing paradigm that is made up of many highly interconnected processing elements working together to solve problems (Wei & Gaurav, 2010). The neural network is capable to capture patterns and trends that would be otherwise hard to detect for humans and other computer techniques. Back propagation neural network allows the network to adapt and thus has become one of the most popular techniques for prediction and classification problems.

3. Decision Tree

A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. As a way to display an algorithm, the decision trees aims to divide observations into mutually exclusive and exhaustive subgroups by properly selecting attributes that best separate the sample (Wikipedia, 2013). For example, Koh and Low successfully developed a decision tree to examine the hidden problems in management fraud by investigating six variables: quick assets to current liabilities, market value of equity to total assets, total liabilities to total assets, interest payments to earnings

before interest and tax, net income to total assets, and retained earnings to total assets (Wei & Gaurav, 2010).

Most of these management detection tools use machine-learning methodologies with two steps. The first step is to develop a model by training samples, and the second step is to put the objective's data into the model for analysis. Besides these data mining technologies used in the management fraud, there are other software and related products available that can help users gather, manage, analyze and search through a large volumes of transactions and information. These computer-assisted techniques not only help the fraud examiner get the digital evidence in an easier way, but also bring a convenient way for the fraud examiner to analyze their evidences, so they can find out who are involved in the fraudulent activities and who are responsible.

Computer-Assisted Management Detection Methods

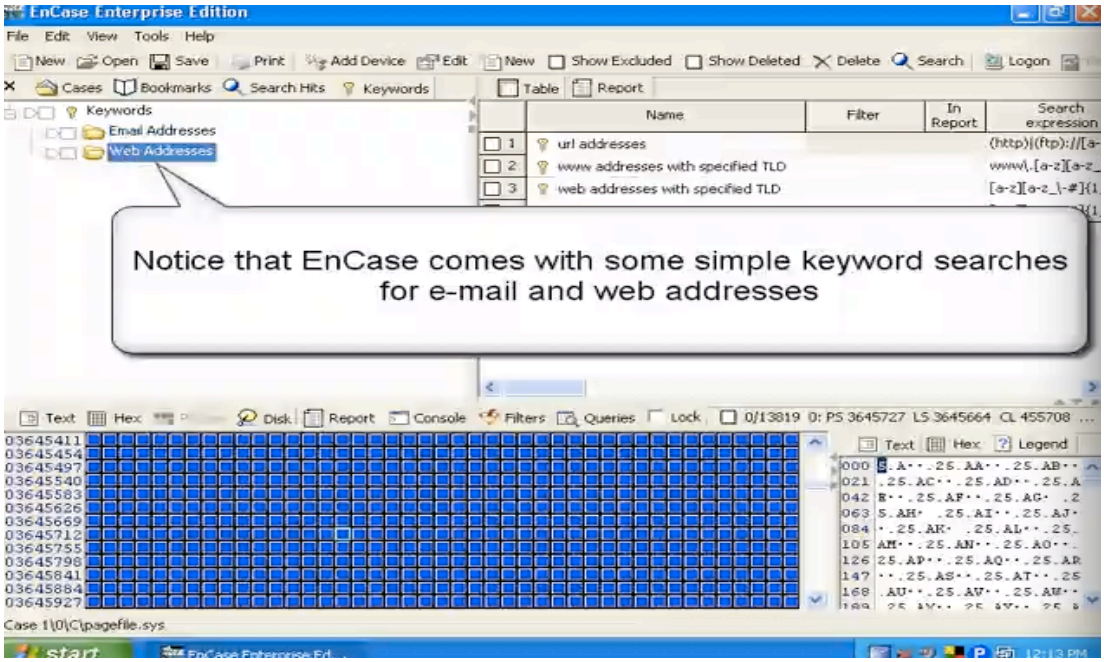
Firstly, I will introduce a few tools used to gather digital evidence. Digital evidence or electronic evidence is defined as any probative information stored or transmitted in digital form that a court case may use at trial (Casey, 2004). Police and prosecutors are fashioning a new weapon in their arsenal against criminals: digital evidence. The sight of hard drives, Internet files and e-mails as courtroom evidence is increasingly common (Coren, 2005). The use of the digital evidence contains a wide range of areas, such as e-mail, files saved from accounting program, digital video, audio files, Internet browser histories and the content of computer memory. In general, the electronic evidence refers to any evidence captured by computers and electronic devices (Kranacher et al. 2011). But how useful is the digital evidence? It provides great hints

for fraud examiner. For example, email is a rich source of digital evidence, because people often leave confidential materials and information they don't want others to know. A large number of tools have been developed in order to protect and gather digital evidence, a few of which are described as following.

1. EnCase

Encase is a software for digital imaging of hard drive and other storage media and is widely used as a computer forensics tool. More than 2000 legal operation departments use EnCase as an efficient tool to gather important evidence. EnCase can be used to investigate and analyze data on multiple platforms, including Windows, Linux, AIX, OS X, Solaris, and others. It also provides tools to identify information stored on hard drives despite efforts to hide, cloak or delete the data (Kranacher et al, 2011). In addition, it can also help examiners manage large amount of computer evidence and to view file types, including deleted files, and also it can view the file creation date and the file modified date. Moreover, it also supports many mail formats, such as Outlook, Outlook Express, Yahoo, Hotmail and Exchange. As Figure 4 shows, EnCase can help users to search through email addresses or web addresses they need to know in the target's computer or electronic devices.

Figure 4 EnCase Software Example



(Source: http://www.youtube.com/watch?v=O4ce74q2zqM)

2. Road MASSter

Figure 5 Road MASSter

(Source: http://www.officer.com/product/10043958/intelligent-computer-solutions-inc-road-masster-3)

Road MASSter is another useful computer forensic tool. As figure 5 shows, it is a "portable computer forensic lab" (Kranacher et al, 2011). This little briefcase contains a keyboard, a color LCD display and data copying devices. The main function of Road MASSter is to do the hard drive imaging and data analysis. "The device can be used to image hard drives of any kind, as well as capturing data from other media (e.g., CDs, stick drives, flash drives) and unopened computers" (Kranacher et al, 2011). In addition, this device can not only capture the data in the computer, but also image the data from the devices like cell phones.

3. Recovering Deleted E-mails

As mentioned above, email is a rich source of digital evidence as it is a tool often used by the perpetrator to receive or send fraudulent information. Most of the time, the perpetrator will delete the "secret" email in order to destroy the evidence. However, for the fraud examiners, the deleted email can provide solid references and evidences of what the perpetrators did and what their fraudulent activities were. Every email software system has recycle bin which is the first place to find after the emails have been deleted. However, if the examiner cannot find those emails in the recycle bin, the deleted email may still be recovered by some special email recovery software, such as Mail Recovery (for Outlook Express and Windows Mail) and Advanced Outlook Repair (for Microsoft Outlook PST files).

4. Recovering Deleted Files

Deleted files are very similar with the deleted emails. Provided that the fraud examiner cannot find the deleted files in the recycle bin, there are some useful software available for recovering the deleted files, such as DiskInternal's Uneraser, Office Recovery (Microsoft Office documents), Word Recovery(Word DOC, DOT, and RTF files), DOC Regenerator (Microsoft Word documents), Excel Recovery (Excel spreadsheets and worksheets), XLS Regenerator (Excel spreadsheets), Flash Recovery (digital image recovery, including photos, from hard drives and memory cards), Music Recovery (MP3, WMA, and other music files from hard drives, memory cards, and other music players) (Kranacher et al, 2011).

Once the fraud examiners mange to gather evidences using modern, the next step is to use some analytical tool to find out the perpetrators. Nowadays, an increasing number of computer companies have developed data analysis software to help fraud examiner and auditors detect red flags and potential fraud. The following section provides a few examples that are capable to do so.

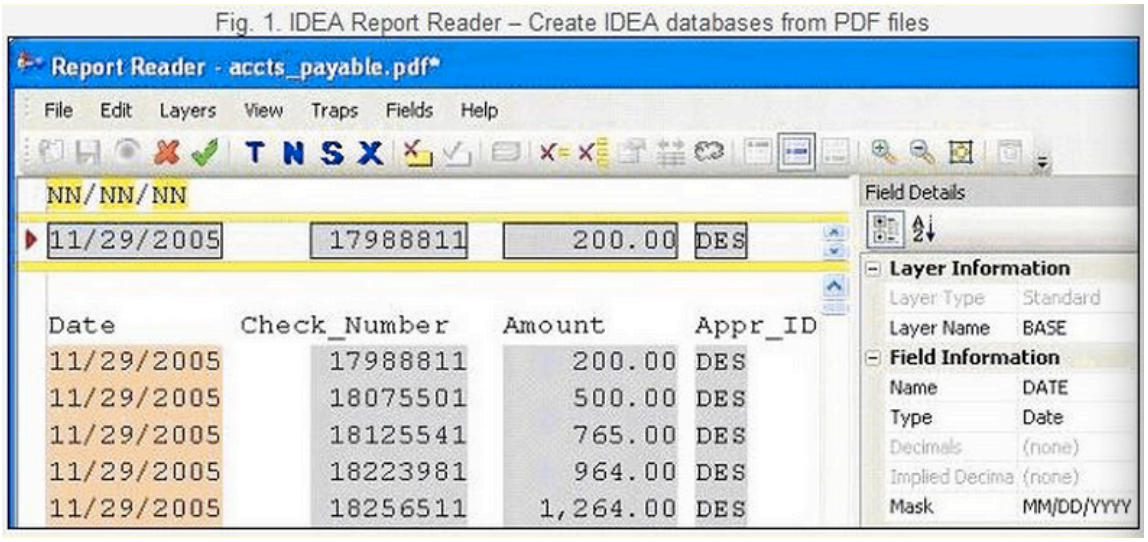
1. IDEA Data Analysis Software

IDEA stands for Interactive Data Extraction & Analysis. It helps the fraud examiners, accountants and financial managers to view, sample and analyze data from other computerized systems. IDEA also includes many data analysis features that are often provided by other software, such as Excel. The following is an example of how IDEA Data Analysis Software detects a fraud.

A company in east coast used IDEA and discovered a six-year fraud scam, totaling $860,000 in losses (Sparks, 2010). During six years of rumors and many employee

interviews, all the information pointed towards fraud in the accounts payable department till the company executives started to investigate the issue. The first step was to import the six-year data into the IDEA like Figure 3 shows.

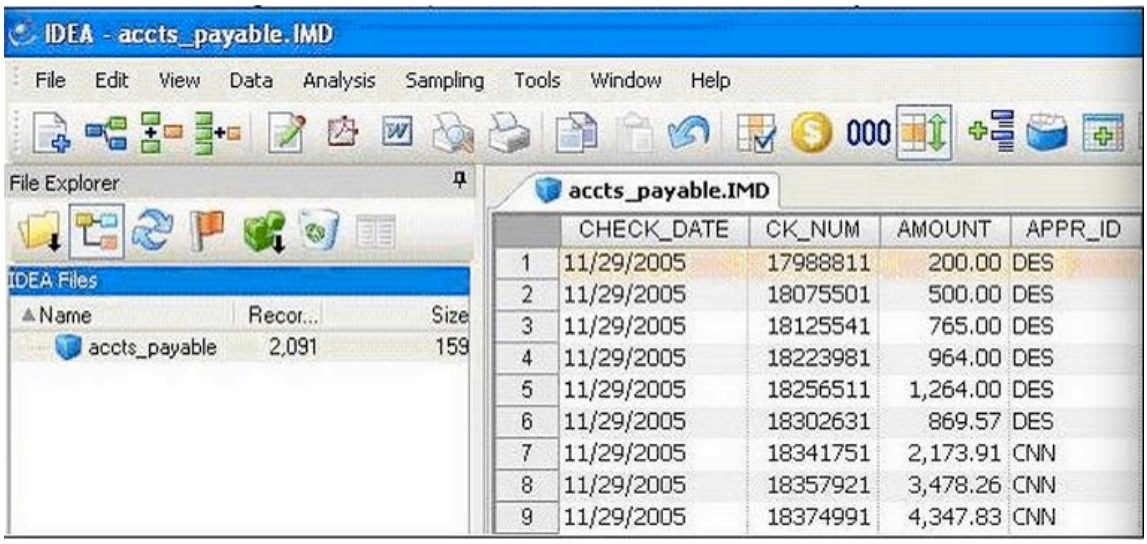
Figure 6 Create IDEA Databases from PDF Files



(Source: http://www.auditnet.org/articles/CAATTTalesV1I2.htm)

Figure 6 shows the PDF files has been imported into IDEA software and ready to analyze.

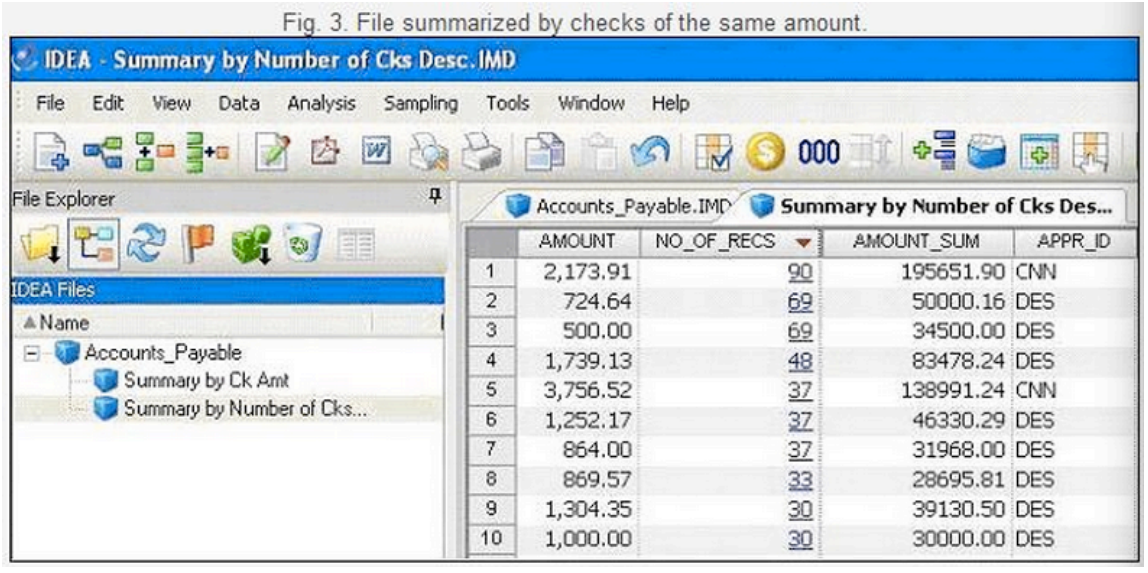
Figure 7 PDF File Imported into IDEA



Then the fraud examiners started to use the count function of IDEA to show the number of occurrences of each check amount in the six-year data file.

Figure 8 Data

Summary



After the fraud examiner and the company executives reviewed the result of the IDEA, they decided to ask the company's bank to re-image the checks appearing in the highest repeating check dollar amounts. Finally, the bank detected that many checks were made payable to, and were endorsed by the accounts payable employee who had worked for the company for six year.

VI. T. J. Maxx Data Breach as an Example of External Fraud

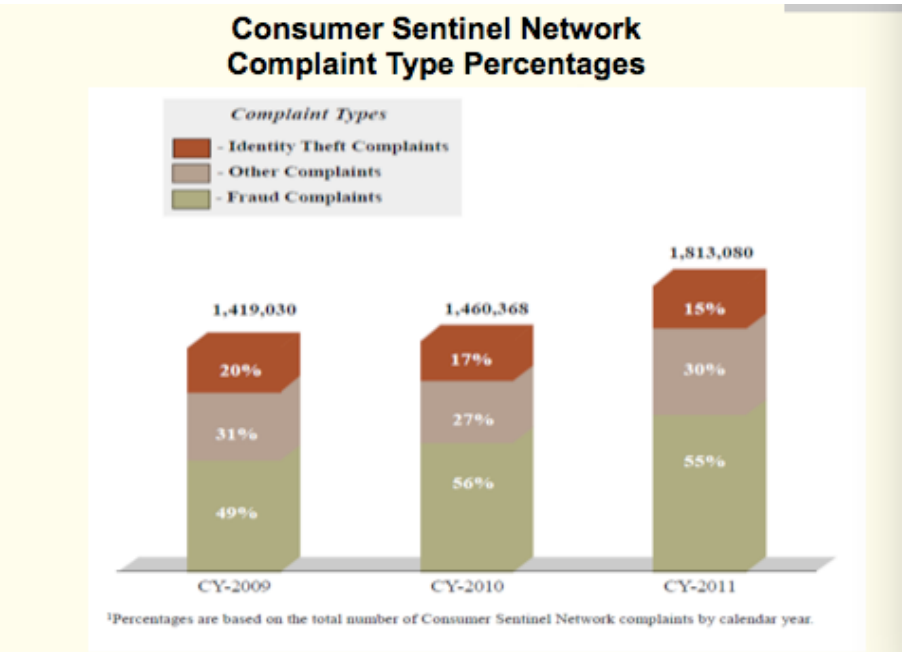
Introduction of Identity Theft

External fraud refers to offenses committed by individuals against organizations (e.g., insurance fraud), or organizations against individuals (e.g., consumer frauds) (Kranacher et al, 2011). False insurance claims are insurance claims filed with intend to defraud an insurance provider, such as faking death to claim life insurance (Wikipedia, 2013). Consumer fraud includes identity theft, check and credit card fraud, and computer and Internet fraud. This section I will focus on identity theft and credit card fraud to investigate this two fraud and to analyze the efficient ways to detecting these two kinds of external fraud.

What is identity theft? Identity theft occurs when someone

> "Knowingly transfer or uses without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.''
>
> (source: Identity Theft and Assumption Deterrence Act of 1998)

Figure 9 Consumer Complaint Type Percentages



(source: www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinelcy2011.pdf)

Figure 9 showed that the number of identity thefts complaints is the highest among the total complaints. At the same time, according to the Federal Trade Commission's estimation, the number of identity theft victims has already reached 9.9 million nationally. Government estimates $53 billion in damages related to identity theft in 2009. Table 1 summarized the number of identity theft that happened in past decade.

Table 1 Identity Theft Examples

Year 2000	300,000 credit card numbers stolen from CD Universe.
Year 2001	Credit card numbers, drivers' license numbers, Social Security numbers, dates of birth posted to chat room.
Year 2004	ChoicePoint (an information broker) sold the records of 145,000

	consumers to a fake company.
Year 2005	CardSystems Solutions, in violation of agreements with MasterCard and Visa, retained 40 million credit card numbers for "research purposes." They were subsequent stolen by hackers.
Year 2007	TJX Companies: Hackers stole 90 million credit cards, debit cards.
Year 2009	Albert Gonzales and two Russian accomplices indicted for theft of 130 million credit and debit card numbers.
Year 2012	Global Payments: 1.5 million account numbers, other data stolen by hackers.

Identity Theft Cycle

How identity theft occurred?

Perpetrators of identity theft follow a common pattern after they have stolen a victim's identity (Towle, 2004), and "identity theft cycle" has been developed by Towle who is an criminologist in America who had a deep investigation in identity theft to better understand how identity theft occurs. Needless to say, different identity theft perpetrators commit fraud in different ways, but most of them follow the three steps of the "identity theft cycle".

Step 1 Discovery: Perpetrators gain and verify information

It is obvious that discovering the chance to commit fraud is the first step for the perpetrators before they proceed to the identity theft. During the gaining discovery

state, perpetrators do all they can to gather a victim's information (Albrecht et al, 2004). The techniques used by perpetrators to gather information include stealing information from their employer, hacking into organizations' computers, bribing an employee who has access to confidential records, "dumpster diving" (go to somebody's trash), searching someone's mailbox, searching other's home or computer, scanning credit card information, and any other methods capable to gather the victim's information. After the perpetrators gathered the information, they will use a very short time to verify the information they gathered. Examples include telephone scams, where perpetrators call the victim and act as a representative of a business to verify the information gathered (Albrecht et al, 2011). Also, some perpetrators may not verify the information they gathered at the beginning, but they may process the verification during the scam.

Step 2 Action: Perpetrators "hack" to the victims' personal information and steal the documentation, then they cover-up or conceal actions.

T.J.Maxx Data Breach

I will use the TJX Companies happened in the year 2007 (Table 1) as an example to analyze how the perpetrators hacked into the TJX's information system and the reason why TJX data breach can happen.

In January 2007, TJX Inc., the parent company of retail chains of T.J. Maxx and Marshalls, issued an announcement that their computer systems had been breached and 100 million debit cards and credit cards had been stolen and exposed to potential fraud during the next few years. Actually on December 18, 2006, TJX had discovered an

unauthorized intrusion into their computer systems that process and store information related to customer transactions (Cereola & Cereola, 2011). Shortly after that, TJX hired two computer security and incident response companies—General Dynamics Corporation (GDC) and International Business Machines Corporation (IBM) to help with the investigation. The investigation shows that the scope of the intrusion spanned from July 2005 until December 18, 2006. Hackers stole 90 million credit cards, debit cards.

What went wrong with TJX? Through the investigation, TJX failed to comply with the Payment Card Industry (PCI) data security standards established in 2004 by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International (Berg, 2006). According to Berg who is an associate professor of accountancy at East Tennessee State University with PhD and CPA certification, his reports about analyzing the TJ Maxx Data Security Fiasco investigated that there are three major areas of reasons led to the data breach: inadequate wireless network security, improper storage of customer data, and failure to encrypt customer account data (Berg, 2006).

1. Inadequate wireless network security

The examination indicates that the intruder's first access occurred in the computer systems located in a Framingham, Massachusetts store (Cereola & Cereola, 2011). At that time, the transmitted wireless transaction in TJX systems used Wired Equivalent Privacy (WEP) technology. Wired Equivalent Privacy (WEP) is a security algorithm for wireless networks (Wikipedia, 2013). However, the intruder just used directional antennas and a laptop to intercepted electronic transmissions sent over TJX's wireless

network. The credit card and debit card payments, customers' personal information, and authorization requests were all included in the transmissions. Because of the inadequate wireless network in TJX, the intruder obtained access into TJX's information systems readily. In fact, the primary problem with WEP system is that it is easy to crack. Researchers from Darmstadt Technical University in Germany have demonstrated that a WEP key can be broken in less than a minute. In addition, WEP doesn't meet industry standards that require the use of much stronger WPA (Wi-Fi Protected Access) protocol (Berg, 2006). After the hacker broke into the store's systems, they broke the corporate headquarters' security easily and then stole all the customer account information there. Since the hacker's first access into the TJX information system, they stayed there for 18 months without being detected.

2. Improper storage of customer data

TJX Company stored the full-track contents including the card number, card validation code (CVC), and the personal identification numbers (PIN) scanned from each customer's card. This kind of storage customer's information had been violated Payment Card Industry (PCI) data security standards. The standards clearly state that after payment authorizations are received, a merchant is not to store sensitive data, such as the CVC, PIN, or full-track information (Berg, 2006). Table 2 summarized the data that had been stolen by the hackers and related PCI standards.

Figure 10 Suspected TJX Data Retention Practice Compared with PCI Standards

Suspected TJX Data Retention Practice Compared with PCI Standards

	Data Item	Data Retained by TJX	PCI Retention Standards
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name*	Yes	Yes
	Service Code*	Yes	Yes
	Expiration Date*	Yes	Yes
Sensitive Authentication Data†	Full Magnetic Stripe	Yes	No
	CVC2/CVV2/CID	Yes	No
	PIN/PIN Block	Yes	No

* Must be protected if stored in conjunction with PAN.
† Sensitive authentication data must not be stored after authorization (even if encrypted).

(Source: Berg, G. N. (2008). Analyzing the TJ Maxx Data Security Fiasco. CPA Journal, 78(8), 34.)

TJX Company did not take seriously of all the customers' personal information. The company used an out-of-date version of the point-of-sale (POS) software to store all the customer's card data that should not be reconfigured to comply with PCI standards.

3. Failed to encrypt customer data

Although the intruder could be able to break into the TJX corporate network and to access the customer's data, the data breach may still not have occurred if TJX securely encrypted the customer's data. According to the investigation, each in-store computer kiosk in TJX was equipped with a personal computer (PC)-style system that was directly connected to the corporate network. The intruder connected USB drives with

utility programs to these computers and then later used these terminals to access the corporate network (Cereola & Cereola, 2011). Other evidences showed that the intruders used key logging technology to obtain user identification and password information from the corporate network and then used this information to create fictitious accounts. These accounts were later used to collect transaction information remotely (Cereola & Cereola, 2011). That is how they did the cover up or concealment action to continue the identity theft for a longer period of time with out being noticed. PCI Data Security Standards 3.5 and 3.6 require merchants to protect the encryption keys used for protecting customer data from disclosure and misuse (Berg, 2006). Needless to say, the PCI Data Security Standard were again not complied with by TJX.

Step 3: Trial: how perpetrators get the financial benefits?

A perpetrator may go to a grocery store and use a stolen credit card to determine whether the cards works or not. If works, then the perpetrator may move on to bigger scams. If not working, the perpetrators can just quickly discard the card without any pressure to be noticed. Next, the perpetrator may use the stolen card to purchase some more expensive items, such as establishing wireless or phone service in victims' name, opening a new bank account, opening new credit card accounts, and even changing victim's mailing address.

VII. External Fraud Detection Techniques

The investigation on the data breach of TJX clearly indicates that the inadequate wireless network security system of the company was too vulnerable to detect the intrusion as it took nearly one year to detect the intrusion. It suggests that either the TJX has a very weak intrusion detection system or even it did not have an intrusion detection system. No matter how perfect the systems is, the intruder can find passwords, read and change files, alter source code, read e-mails and so on (Bolton, 2002). If the intruder can be detected early enough or prevented from penetrating the computer system, this kind of intrusion can be prevented efficiently. This kind of intrusion fraud has been taken seriously in recent years, and much more efforts are being put into developing intrusion detection technologies. I will introduce some intrusion detecting technologies and other identity theft detecting technologies as following.

1. Expert Systems

An expert system is defined as a computing system capable of representing and reasoning about certain knowledge-rich domains with a view to solving problems and giving advice (Sebring et al, 1988). The expert systems are the information systems that use the information about the attacks to detect intruder. The expert systems contain a set of rules that describe the attacks. Audit events are then translated in to facts carrying their semantic signification in the expert system, and the interference engine draws conclusions using these rules and facts (Nazer & Selvakumar, 2011).

2. Computer Immunology

Computer Immunology has ben described by Forrest et al (1997). It builds a model of normal behavior of the network services, rather than that of the users. It consists of short sequences of system calls made by the processes. Attacks that exploit flaws in the code are likely to take unusual execution paths. This tool collects a set of reference audits, which represent the appropriate behavior of the service and extracts a reference table containing all the known “good” sequences of system calls (Nazer & Selvakumar, 2011). In next step, these patterns are then used for live monitoring to check whether the sequences generated are listed in table. If not, the intrusion-detection system generates an alarm. The advantage of the computer immunology is that it has a very low error rate if the reference table is exhaustively enough.

3. Data Mining

Data mining (the analysis step of the "Knowledge Discovery in Databases" process, or KDD) is an interdisciplinary subfield of computer science. It is the computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. The overall goal of the data mining process is to extract information from a data set and transform it into an understandable structure for further use (Wikipedia, 2013). This technology can be used for intrusion detection. Classification model with association rules algorithm and frequent episodes can automatically generate accurate detection models from large amount of data. A team of researchers at Columbia University proposed detection models using cost-sensitive machine learning algorithms. Audit data was analyzed by association rules algorithm so as to determine static features of attack data (Stolfo et al, 2001).

4. Outlier Detection

Outlier detection is a credit card fraud detection technique. Because credit card fraud detection is a very confidential work, so there are not many techniques available in the public, including outlier detection. An outlier is an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism (Hung & Cheng, 1999). Outlier detection methods do not require prior knowledge of fraudulent and non-fraudulent transactions in historical database. However, what they do is to detect the changes in behavior or unusual transactions in the system. These methods model a baseline distribution that represents normal behavior and then detect observations that show the greatest departure from this norm. One advantage of outlier detection technique is that previously undiscovered types of fraud may be detected.

VIII. Recommendations for the Future

Recommendations for internal fraud:

Although we are now equipped with advanced technology like data mining, machine learning technology for detecting internal fraud, none of these techniques are perfect. Instead each of them has disadvantage and limits of usage, and the fraudsters can always find the ways to circumvent the detection programs. And thus it is very important that the mechanism should be able to update the detection software both effectively and efficiently. They should conduct researches all the time to realize the newest criminal methods the fraudsters used and update the detection program adaptive to these criminal methods.

However, taking advantage of modern technology is not sufficient to preven internal fraud, and the company owners' responsibilities are also very crucial. Owners of the companies need to have better education and put more concerns on how their firms are managed. A good management decision and control strategy and policy in business firm play a key role in the operation of the business. All these decisions and actions need to be more closely scrutinized. A good business environment is not only favorable for the employees, but also beneficial for the investors.

The owners need to take serious considerations on internal control. Executive fraud, like all frauds, is intended to misrepresent information to, and mislead those who rely on the correctness of this information. When this occurs, internal control is not as effective and inherently threatened (Mukweyi, 2010). A good internal control plays an important role in preventing and detecting fraud. In addition, it can also regulate both

employers and employees' behaviors and decisions. Taking Enron scandal as an example, bad internal control led a number of substandard actions by the employers and employees.

The owners should develop more effective regulations. Regulations need be not only about what may or may not be done only, but also about severe and dire consequences for those who willfully break laws, rules, and accepted trade practices (Mukweyi, 2010). Punishment rules can prevent the internal fraud effectively.

Recommendations for external fraud:

Most of the victims of identity theft fraud need a long time to be aware that their identity information have been stolen because fraudsters can use victim's personal information in any areas with a long period that cause a huge potential losses for the victims. There is a need to link the intermediary parties between the victims and identity fraudsters. These parties includes financial and credit institutions, law enforcement agencies, criminal record divisions of court houses, departments of motor vehicle, utility and telecommunication companies, and all other intermediary parties that may be affected by potential identity thieves (Perl, 2003). If the link has been developed, the victims can find out the fraud more quickly and therefore prevent further huge losses.

The other recommendation for external fraud is to use more biometric data (Perl, 2003). Using biometric data means "the techniques and methods used to identify individuals based on a physical characteristic or particular trait unique to that individual" (Lisa,

2000). Biometric data refers to fingerprints, hand imaging, voice recognition and other personal physical attributes. Although the biometric data have been used in many places, such as airport and grocery stores, more use of biometric data can prevent identity theft effectively. For example, voice recognition can be used in online purchases to prevent the fraudsters trying to use other people's credit card or debit card for online shipping.

IX. Conclusion

In my thesis, I have discussed all categories of frauds, using Enron scandal and T.J.Maxx Data breach as examples to investigate the internal and external fraud. Cressey's "fraud triangle" theory and Albrecht's three-stage theory were applied to analyze the causes of these frauds. In addition, the thesis also reviewed modern technologies and techniques that can be applied for both internal and external fraud detection and prevention. Finally, the recommendations were provided to how to improve the fraud detection system both in internal and external fraud. It is a shame that fraud is a growing problem in the modern world, and the best way to prevent them will require collective efforts from the entire society. The merchants need to be adaptive with the newest fraudsters' criminal action, and the customers need to be more vigilant and aware of how to protect themselves from the fraudsters, whereas the governments need to develop an efficient policy to keep down the number of fraudulent activities.

X. Reference

Albrecht, W.S. and Albrecht, C. (2004), Fraud Examination and Prevention, Thomson South-Western, Mason, OH.

Albrecht, C., Albrecht, C., & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. Journal Of Financial Crime, 18(4), 405-414. doi:10.1108/13590791111173722

Berg, G. N. (2008). Analyzing the TJ Maxx Data Security Fiasco. CPA Journal, 78(8), 34.

Bolton, Richard J. "STATISTICAL FRAUD DETECTION." Statistical Fraud Detection: A Review. Ed. David J. Hand. 3rd ed. Vol. 17. N.p.: Institute of Mathematical Statistics, 2002. 235-249. Print.

Carson, T. L. 2003. Self-interest and business ethics: Some lessons of the recent corporate scandals. Journal of Business Ethics, 43:389–394.

Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-163104-4

Cereola, S. J., & Cereola, R. J. (2011). Breach of Data at TJX: An Instructional Case Used to Study COSO and COBIT, with a Focus on Computer Controls, Data Security, and Privacy Legislation. Issues In Accounting Education, 26(3), 521-545. doi:10.2308/iace-50031

Chandra, U. & Ettredge, M.L. & Stone, M.S. (2006). Enron-Era Disclosure of Off-Balance-Sheet Entities. Accounting Horizons, 20. Retrieved February 16, 2008, from http://global.factiva.com/

Coren, Michael (2005). “Digital evidence: Today’s fingerprints” CNN Justice January 31, 2005. Web. 28 March.2013. http://articles.cnn.com/2005-01-

28/justice/digital.evidence_1_digital-evidence-computer-crime-law-enforcement?_s=PM:LAW

Cressey, Donald. (2013, March 15). In Wikipedia, The Free Encyclopedia. Retrieved 16:32, April 15, 2013, from http://en.wikipedia.org/w/index.php?title=Donald_Cressey&oldid=544452333

Data mining. (2013, March 25). In Wikipedia, The Free Encyclopedia. Retrieved 15:37, March 28, 2013, from http://en.wikipedia.org/w/index.php?title=Data_mining&oldid=546873904

Decision tree. (2013, February 18). In Wikipedia, The Free Encyclopedia. Retrieved 20:15, April 2, 2013, from http://en.wikipedia.org/w/index.php?title=Decision_tree&oldid=538846921

Employee stock option. (2013, April 4). In Wikipedia, The Free Encyclopedia. Retrieved 03:33, April 16, 2013, from http://en.wikipedia.org/w/index.php?title=Employee_stock_option&oldid=548676024

Hung. E. and Cheng. D. W. Parallel Algorithm for Mining Outliers in Large Database. http://citeseer.nj.nec.comihung99parallel.hbnl, 1999.

Insurance fraud. (2013, March 21). In Wikipedia, The Free Encyclopedia. Retrieved 15:44, March 21, 2013, from http://en.wikipedia.org/w/index.php?title=Insurance_fraud&oldid=545884439

Jackson. (2006). Grim Realities of Financial Reporting. Mason, OH: Thomson/South-Western.

Kranacher, Mary-Jo, Richard Riley, and Joseph T. Wells. Forensic. Accounting and Fraud Examination. Hoboken, NJ: John Wiley, 2011. Print.

Lisa Jane McGuire, Comment, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441,444 (2000)

Locatelli, M. (2002). Good internal controls and auditor independence. The CPA Journal, 72. Retrieved February 26, 2013, from http://global.factiva.com/

Marianne M. J. (2009). Business Ethic Case Study and Selected Readings (6th Ed.). Salt Lake City, UT, U.S.A.: South-Western Cengage Learning

Michael E., E., & Pedro R. Falcone, S. (n.d). The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams. Expert Systems With Applications, 399966-9985. doi:10.1016/j.eswa.2012.01.143

Mukweyi, A. I. (2010). MANAGERIAL FRAUD AND CORPORATE GOVERNANCE IN AMERICAN CORPORATIONS. International Journal Of Business & Public Administration, 7(1), 57-70.

Nazer, G., & Selvakumar, A. (2011). Current Intrusion Detection Techniques in Information Technology - A Detailed Analysis. European Journal Of Scientific Research, 65(4), 611-624.

Neural network. (2013, March 26). In Wikipedia, The Free Encyclopedia. Retrieved 19:48, April 2, 2013, from http://en.wikipedia.org/w/index.php?title=Neural_network&oldid=546999990

Perl, M. W. (2003). It's Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft. The Journal Of Criminal Law And Criminology (1973-), (1), 169. doi:10.2307/3491307

Sebring. M, Shellhouse. E, Hanna. M, and Whitehurst. R. Expert system in intrusion detection: A case study. In Proceedings of the 11th National Computer Security Conference, pages 85-91, October 1988

Sparks, Dons. "Applying Data Analysis to Uncover an Ongoing Fraud Scheme" AuditNet The Global Resource for Auditors February 28, 2010. Web. 28 March. 2013 http://www.auditnet.org/articles/CAATTTalesV1I2.htm

Stephens, L. & Schwartz, R.G. (2006). The chilling effect of Sarbanes-Oxley: Myth or reality? The CPA Journal, 76. Retrieved February 16, 2008, from http://global.factiva.com/

Stolfo. S.I., Lee. W, Chan. P, Fan. W, and Eskin. E.Data mining-based intrusion detectors: An overview of the Columbia ids project. In ACM Transactions on Information and System Security, TISSEC, volume 3, pages 5-14,2001.

Towle, H.K. (2004), "Identity theft: myths, methods, and new law", Rutgers Computer&Technology Law Journal, Vol. 30, pp. 237-326.

Wei, Z., & Gaurav, K. (n.d). Detecting evolutionary financial statement fraud. Decision Support Systems, 50(On quantitative methods for detection of financial fraud), 570-575. doi:10.1016/j.dss.2010.08.007

Whiting, D. G., Hansen, J. V., McDonald, J. B., Albrecht, C., & Albrecht, W. (2012). MACHINE LEARNING METHODS FOR DETECTING PATTERNS OF MANAGEMENT FRAUD. Computational Intelligence, 28(4), 505-527. doi:10.1111/j.1467-8640.2012.00425.x