

IS TRANSPARENCY A SIGN OF FRAUD RISK?

A THESIS SUBMITTED TO
THE GRADUTE SCHOOL OF SOCIAL SCIENCES
OF
THE IZMIR UNIVERSITY OF ECONOMICS

BY

SELİN DURMUŞ

AUGUST
2008

ABSTRACT

IS TRANSPARENCY A SIGN OF FRAUD RISK?

Selin Durmuş

MA in Financial Economics, Department of Social Sciences

Supervisor: Assoc. Prof. Dr. Ayla Ođuş Binatlı

August, 2008

Fraud risk which has been observed as a separate department within the private and public institutions in many countries and which has been a controversial issue for Federal Bureau of Investigation (FBI), has spread very commonly in Turkey. Generally, the companies deny that they are subject to fraud risk, when they are asked whether their company/ institution confronts fraud cases. Turkey is a not a transparent country, hence is this country vulnerable to fraud cases. As an auditor, I am going to prove that fraud risk is a function of transparency, Turkey is not a transparent country and that it is vulnerable to many fraud risks, because the required conditions for a fraud crime can be easily prepared in this country. My whole thesis will analyze different definitions of fraud risk, under which circumstances it occurs, relationship with transparency index and the transparency of Turkey. I will also point out some samples as a PwC worker. At last, I will emphasize some important auditing strategies that can be applied in order to prevent fraud risk.

Key Words: Fraud, transparency, preventing

ÖZET

ŞEFFAFLIK SUİSTİMAL RİSKİNİN BİR GÖSTERGESİ Mİ?

Selin Durmuş

Finans Ekonomisi Yüksek Lisans Programı, Sosyal Bilimler Enstitüsü

Tez Yöneticisi: Doç. Dr. Ayla Oğuş Binatlı

Ağustos, 2008

Şu sıralar Amerikan Federal Soruşturma Bürosu (FBI)'nda dahi önemle üzerinde durulan, özellikle gelişmiş ülkelerde birçok özel kuruluşlarda ve kamu kuruluşlarında ayrı birer bölüm olarak incelenmeye başlanan suistimal/ usulsüzlük, Türkiye'de de yaygın bir şekilde kendini göstermektedir. Ancak “şirketinizde/ kurumunuzda suistimal var mı?” diye sorulduğunda genellikle olduğu inkâr edilmesine rağmen, Türkiye çok şeffaf olmayan bir ülke olarak bu riski yoğun olarak barındırmaktadır. Bir denetçi olarak gözlemlerime de dayanarak, bu tezde şeffaflıkla suistimal riski arasında bir ilişki olduğunu, Türkiye'nin şeffaf bir ülke olmadığını, suistimal riskinin ortaya çıkmasına neden olan unsurların zemininin çok rahat yaratıldığını ve yaygın bir uygulama alanı bulduğunu kanıtlamaya çalışacağım. Tez boyunca öncelikle suistimalin tam olarak ne olduğu, hangi koşullar sonucunda ortaya çıktığı, şeffaflık endeksiyle ilişkisi ve Türkiye'nin şeffaflık derecesi incelenecek; ayrıca bir PricewaterhouseCoopers (PwC) çalışanı olarak yaptığım anketlerle örnekler sunulacaktır. Son olarak da bir firmada en etkin iç denetimin nasıl yapılacağına ve suistimali önlemeye dair politikalar önerilecektir.

Anahtar Kelimeler: Suistimal, şeffaflık, önleme

ACKNOWLEDGMENTS

I am very grateful to Assist. Prof. Dr. Ayla Oğuş Binatlı for her supervision, constructive comments and motivating encouragement throughout this study.

I would also like to thank to the other members of examining committee for their contribution.

I am also thankful to Mehmet Karakurt, Wayne Anthony and Serdar İnanç from PricewaterhouseCoopers who have helped me very much with their valuable comments, supporting attitudes, patience and provided the data I have needed for my thesis.

Consequently, I would like to state my pleasure to my parents who continuously motivated me through my studies and supported me by patience to accomplish my graduate study.

TABLE OF CONTENTS

ABSTRACT	i
ÖZET	ii
ACKNOWLEDGMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vi
LIST OF FIGURES	vii

CHAPTERS

1. INTRODUCTION	1
2. DEFINITION AND INDICATIONS OF FRAUD	4
2.1 Characteristics of Fraud	4
2.1.1. Types of Fraud	5
2.2 Cost of Fraud	8
2.2.1 The Duration of Fraud.	15
3. THE POTENTIAL VICTIMS AND PERPETRATORS OF FRAUD	18
3.1 The Victims of Fraud	18
3.2 The Perpetrators of Fraud	20
3.3 Economic Crimes, the Number of the Victims and the Number of the Perpetrators	24
3.3.1 One Perpetrator –One Victim	24
3.3.2 One Perpetrator – Multiple Victims	25
3.3.3 Multiple Perpetrator – One Victim	26
3.3.4 Multiple Perpetrator – Multiple Victims	27
3.4 The Susceptibility of Fraud Incidents	27
3.4.1 The Organizational Characteristics	29
3.4.2 The Type of the Organization	30
3.4.3 Industrial Sector	30
3.4.4 Management Controls	31
3.4.5 Assets	32
4 - RELATED LITERATURE	33
4.1. The White – Collar Crime	33
4.2 The Blue – Collar Crime	35
4.3 Occupational Crime	36
4.3.1 Skimming	37
4.3.2 Billing	38
4.3.3 Cash Larceny	38
4.3.4 Check Frauds	39
4.3.5 Expense Reimbursement	39
4.3.6 Payroll Fraud	40

5 - INTERNET FRAUDS.....	41
5.1 Auction Fraud.....	43
5.2 Counterfeiting the Cashier’s Check	47
5.3 Credit Card Frauds.....	48
5.4 Debt Elimination	49
5.5 Employment/ Business Fraud Incidents	50
5.6 Escrow Services Fraud.....	51
5.7 Identity Theft.....	52
5.8 Investment Fraud.....	56
5.9 Lottery Frauds	57
5.10 Nigerian Letter or “419”	58
6 – TRANSPARENCY AND FRAUD INCIDENTS	61
7 – A GOOD DETECTION SYSTEM.....	87
7.1 Internal Controls.....	87
7.2 Supervision	91
7.3 Audit	94
7.4 Whistle – Blowing System	100
CONCLUSION.....	103
REFERENCES	105
APPENDIX	120

LIST OF TABLES

Table 1:	Comparison of Major Occupational Fraud Categories by 1996 and 2002 Data.	14
Table 2:	Loss by Number of Employees	19
Table 3:	Loss by Type of Organizations	19
Table 4:	Frequency and Loss Comparison of 1996 and 2002 Data	36
Table 5:	The Bribery Index of the Countries in 2006 Published by the Transparency International	65
Table 6:	The Corruption Perception Index 2006	66
Table 7:	The CPI Rates	71
Table 8:	Descriptive Statistics for CPI vs GDP per Capita	77
Table 9:	Correlations for CPI vs GDP per Capita	77
Table 10:	Variables Entered/Removed(b) for Regression 1	77
Table 11:	Anova for Regression 1	78
Table 12:	Residuals Statistics(a) for Regression	78
Table 13:	Descriptive Statistics for FPI vs GoodGov	83
Table 14:	Correlations of FPI vs GoodGov	83
Table 15:	Variables Entered/Removed(b) for Regression 2	83
Table 16:	Model Summary for Regression 2	83
Table 17:	Anova for Regression 2	84
Table 18:	Coefficients for Regression 2	84
Table 19:	Coefficient Correlations for Regression 2	84
Table 20:	Model Summary for Regression 1	85
Table 21:	Impact of Audits	95

LIST OF FIGURES

Figure 1: The Reasons Why People Commit Fraud According to a Survey of Pwc 2005 ...	3
Figure 2: The Distribution and The Costs of Different Fraud Types for Companies from Different Countries	10
Figure 3: Cost of Economic Crimes, Pwc 2007	11
Figure 4: Price Movement of Tukaş Stocks Between The Years 1999-2008	12
Figure 5: Price Movement of Tukaş Stocks During July 2008.....	13
Figure 6: %43 of Fraud Committed in Turkey was Perpetrated by Employees with One in Four Being Committed by Management (Pwc 2005).....	20
Figure 7: Profiling the Fraudster (Pwc 2005)	20
Figure 8: How Close is the Fraud Perpetrator to You?	23
Figure 9: Who Was the Person Who Misused Your Personal Information?.....	23
Figure 10: Shill Bid Identification Algorithm Decision Tree.....	46
Figure 11: Different Types of Accounting Fraud Related to Identity Theft	53
Figure 12: New Accounts Opened by the Perpetrator in the Name of the Victims	54
Figure 13: The Cycle of the Nigerian Letter or “419”	60
Figure 14: Percentage of Companies Asked to Pay Bribe.....	63
Figure 15: Reported Fraud Percentages versus CPI Rates of E7 Countries	75
Figure 16: CPI Rates versus GDP Per Capita Power Rates	76
Figure 17: Histogram 1	79
Figure 18: Normal P-P Plot of Regression 1.....	80
Figure 19: Point Graph of GDP Per Capita versus CPI.....	81
Figure 20: Fraud Perception Index of 2002 by the International Transparency Organization	82
Figure 21: Histogram 2	85
Figure 22: Normal P-P Plot of Regression 2.....	86
Figure 23: Respondent’s Perceptions of the Prevalence of Fraud in Their Industry, in Their Country (2003 – 2007).....	93
Figure 24: The Percentage of the Companies, Which Think That the Whistle – Blowing System is Beneficial.....	102

1 – INTRODUCTION

The modern world and globalization offers a depressingly predictable cycle of events. New markets lead to new opportunities which lead to new business rules which lead to new opportunities for crime. Fraud which has been felt over the last decades with scandals like Enron, Global Crossing, Worldcom, Parmalat and Adelphia, has been an increasing problem for public and business world.

Actually, at first we have to make it clear what fraud is in order to narrow the fraud risk down in a logical way. As a simple definition, we may say that fraud is a deliberate misrepresentation, which causes damage – especially monetary damage - to some people around. Other kinds of damages that can occur as a result of a fraud case are related to the effective usage of the management time, the brand value, the staff morale...etc. “Fraud” refers to an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.¹

¹ The PwC Audit Guide, Fraud Appendix 1

In the broadest sense, a fraud is a deception made for personal gain, although it has a more specific legal meaning, the exact details varying between jurisdictions. Many hoaxes are fraudulent, although those not made for personal gain are not best described in this way. Not all frauds are hoaxes – electoral fraud, for example. Fraud permeates many areas of life, including art, archaeology and science. In the broad legal sense a fraud is any crime or civil wrong for gain that utilizes some deception practiced on the victim as its principal method.² From these definitions we can understand that fraud has been a significant and growing threat for the companies or institutions around the world.

As a second step, we may investigate why people commit fraud (see figure 1). According to a study carried out by PwC (Global Economic Crime Survey, 2005) most fraud cases are committed because of a lack of internal controls, the need to maintain an expensive lifestyle and the lack of the perpetrator's awareness that their actions are wrong and unethical. If there is a lack of internal controls and supervisions, employee may believe that he will not be caught. In this case he may have achieved the required opportunity to commit a fraud. If the employee has a high personal debt, if he consumes drug or alcohol and if his family or friends put pressure on him in order to succeed, the employee may get the required incitement and motivation in order to commit a fraud.

² <http://en.wikipedia.org/wiki/Fraud>



Figure 1 – The Reasons Why People Commit Fraud According to a Survey of PwC 2005.

Fraud can not be analyzed just with the definitions of the term. Subsequently, all the relevant issues and the related problems will be thoroughly examined and discussed within this study. Finally, the risk of fraud in the future will be discussed.

2 – DEFINITION AND INDICATIONS OF FRAUD

In this section, fraud will be defined with its characteristics and types. Cost of the fraud and duration of fraud will also be examined to have a deeper knowledge for fraud risk.

2.1 Characteristics of Fraud

Not all issues that can cause damage are defined as fraud cases. There are some features, which certify that the case is related with a fraud commitment. The Antifraud & Corporate Responsibility Center has defined the characteristics of fraud. These are;

1) Some issues may be related to an error, which is made unintentionally. The difference between fraud and error is that fraud is committed intentionally. At this stage a professional auditing process is strictly important in order to determine the intent, although it is very difficult.

2) Fraud is a broad legal concept, but the auditor's interest is related to the decision making process about the existence of a misstatement. This case may not include legal determinations of whether fraud has taken place.

3) Two types of misstatements due to fraud are those which are the results of:

a) Fraudulent financial reporting: This includes the intentional misstatements, omissions of amounts or disclosures.

b) Misappropriation of assets: This includes the theft of an entity's assets. It refers also to defalcations.

4) There are three main conditions related to a fraud crime. These are:

- a) Incentive / Pressure – This condition is a reason to commit fraud.
- b) Opportunity – Ineffective controls, override controls, the lack of supervision and auditing some of the main conditions that cause fraud risks.
- c) Attitude / rationalization – This is related to the ability to justify the fraud to oneself.

5) The management has directly or indirectly the authority to manipulate accounting records and present fraudulent financial information by overriding controls or they direct employees to carry out the fraud. As a consequence, we can state that the management has a unique potential so as to perpetrate fraud.

6) Fraud is ordinarily concealed, but there are some certain conditions (such as missing documents and the strange behaviors of the perpetrators) may suggest the possibility of fraud.

7) Audits provide reasonable and not absolute assurance of detecting material fraud.³

2.1.1 Types of Fraud

The categorization of the fraud types may help us in order to clarify this issue. When categorizing the fraud cases we have to take the industry in which the fraud has occurred

³<http://antifraud.aicpa.org/Resources/Educators%20and%20Students/Regulatory%20Considerations/SAS%20No.%2099%20Guidance/Outline%20of%20Statement%20On%20Auditing%20Standards%20No.%2099%20Consideration%20of%20Fraud%20In%20a%20Financial%20Statement%20Au.htm>

into consideration. The types of fraud can differ according to the sector in which they are applied. Australian Institute of Criminology (AIC) pointed out that there are enormously ranges of circumstances in which fraud can exist. These include:

a) Fraud by industry ex. Private sector:

- Financial services fraud: There are many financial services that are provided for the consumers and the fraud perpetrators may benefit from these services. Within this framework we can point out fraud types such as credit card fraud, cheque fraud and other identity frauds.

In terms of financial services sector fraud, the most common types include: transaction fraud such as credit card (and other card) fraud, obtaining finance by deception and cheque related fraud; and identity-related fraud.⁴

- Insurance fraud
- Telecommunications fraud
- Superannuation fraud
- Securities fraud
- Computer fraud

b) Fraud exists also within the public sector. In this case, fraud is committed against the government and the public sector agencies. Some of these fraud types are stated below:

⁴<http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146>

- Migration fraud
- Health care/ benefits fraud
- Taxation fraud
- Welfare fraud

The study of PwC (2007) emphasized also mentioned about different types of fraud that cause serious problems within the companies. These types are:

- Asset Misappropriation: The fraud incidents concerning the company assets such as monetary assets, supplies and equipments. Generally, the company directors or employees are involved in such cases and these cases are related to the interests of the perpetrators.
- Accounting Fraud: Generally, those who are responsible to write and sign the companies accounting book are involved in such cases. They may be able to change the data within the accounting book according to their own benefits. This is an intentional action carried out by the perpetrator.
- Corruption and Bribery: The perpetrator use his situation for unlawful gains. This can include the promise of an economic benefit.
- Money Laundering: This case includes the fraud incidents that intend to legitimize the proceeds of crime by disguising their true origin.
- Intellectual Property (IP) Infringement
- Other

At the beginning of the industrial age, people were unaware of the fraud risk and how to prevent it, but when we search the documents from that time, we may see that the awareness of people have changed since that time. According to a study carried out by Johann Graf v. Lambsdorff (2007), the awareness of people has increased due to the activities of the governmental and trans-national organizations in order to combat fraud.

They especially focused on the prevention of corruption and money laundering. Being aware of the risk is not enough in order to prevent fraud incidents. The companies have to evaluate the fraud incidents and they have to focus on the cost of the fraud incidents so as to estimate the dimension of the incident and this will be wider discussed in the following section.

2.2 Cost of Fraud

When we talk about the cost of fraud incidents, we have to think about two important points. The first is material damage and the second is collateral damage. The material damage is directly related to the amount of the money that is stolen and the collateral damage is related to the image and brand of the company. It is a daunting task to estimate the damages due to fraud incidents, because not all fraud incidents have been detected or reported.

PwC has conducted two studies about fraud and the one focuses on the fraud crimes of companies from different countries and the second focuses on the fraud crimes of the companies within Turkey. In these studies, they focused on asset misappropriation, accounting fraud, corruption and bribery, money laundering IP infringement and some

other kinds of economic crimes. When estimating the cost of economic crime one needs to look at the immediate financial cost of the incident along with the intangible cost of “collateral damage” to the company’s brand and reputation. In respect of financial losses the survey asked companies to estimate the direct financial loss as a result of economic crime.

As a conclusion of these studies, they have found out that the companies experienced difficulties when determining the cost of fraud incidents. We may get a closed opinion about the material damage when we examine figure 2. We can see that asset misappropriation was seen as the most harmful type of fraud according to the global study of PwC in 2007. (The 4th biennial Global Economic Crime Survey, Pwc 2007)

A similar study was conducted also in 2005 and when we compare the results of these two studies we see that the financial loss because of fraud incidents has increased within these two years and it still increases. The average loss from fraud for every company was revealed as US\$ 1,732, 253 in 2005, but this amount increased to US\$ 2,420,700 in 2007.

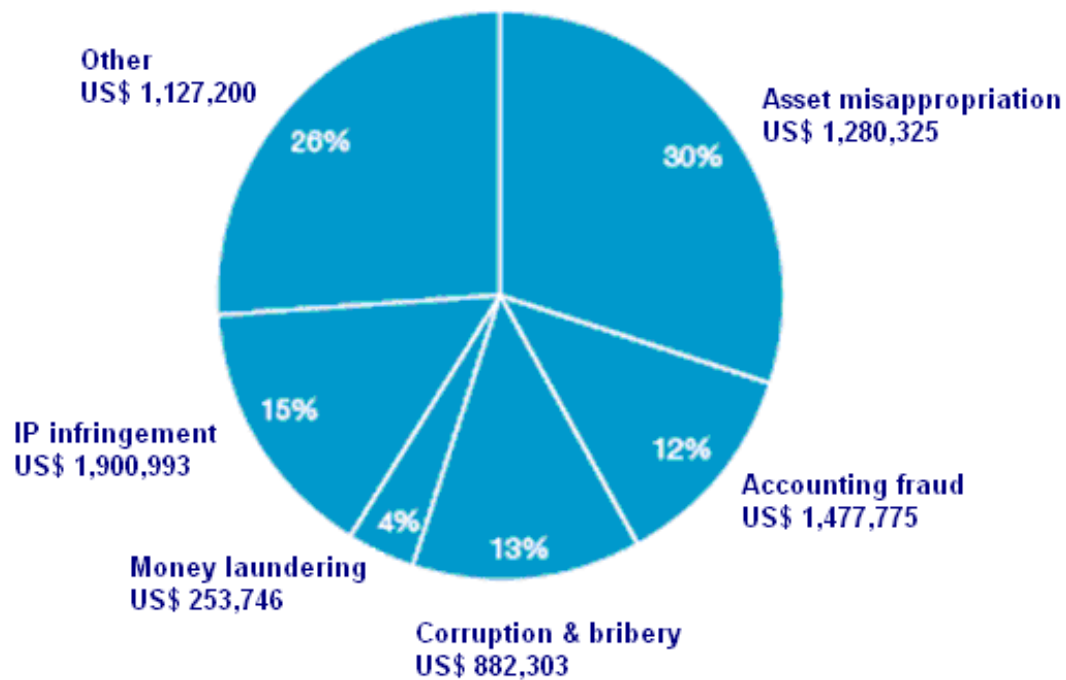


Figure 2 – The Distribution and The Costs of Different Fraud Types for Companies from Different Countries

The same method of research has also been applied to Turkey and as a result of this study it was found that the fraud incidents were not so high in Turkey. Although the incidents were not so many in Turkey, we can see that Turkey's loss is much higher than the other countries when we compare the financial loss of global companies and Turkish companies (see figure 3). This is related to the transparency of Turkey. The authorities reported and examined just the largest incidents of fraud. Namely, we can say that the reports and the records of fraud incidents within the Turkish companies do not reflect reality, because they just include the large and important incidents. According to my own opinion, this type of strategy during the fraud registration is wrong. I think that the Turkish companies have to be aware of the risks of all kind of fraud incidents, no matter how large or small they are.

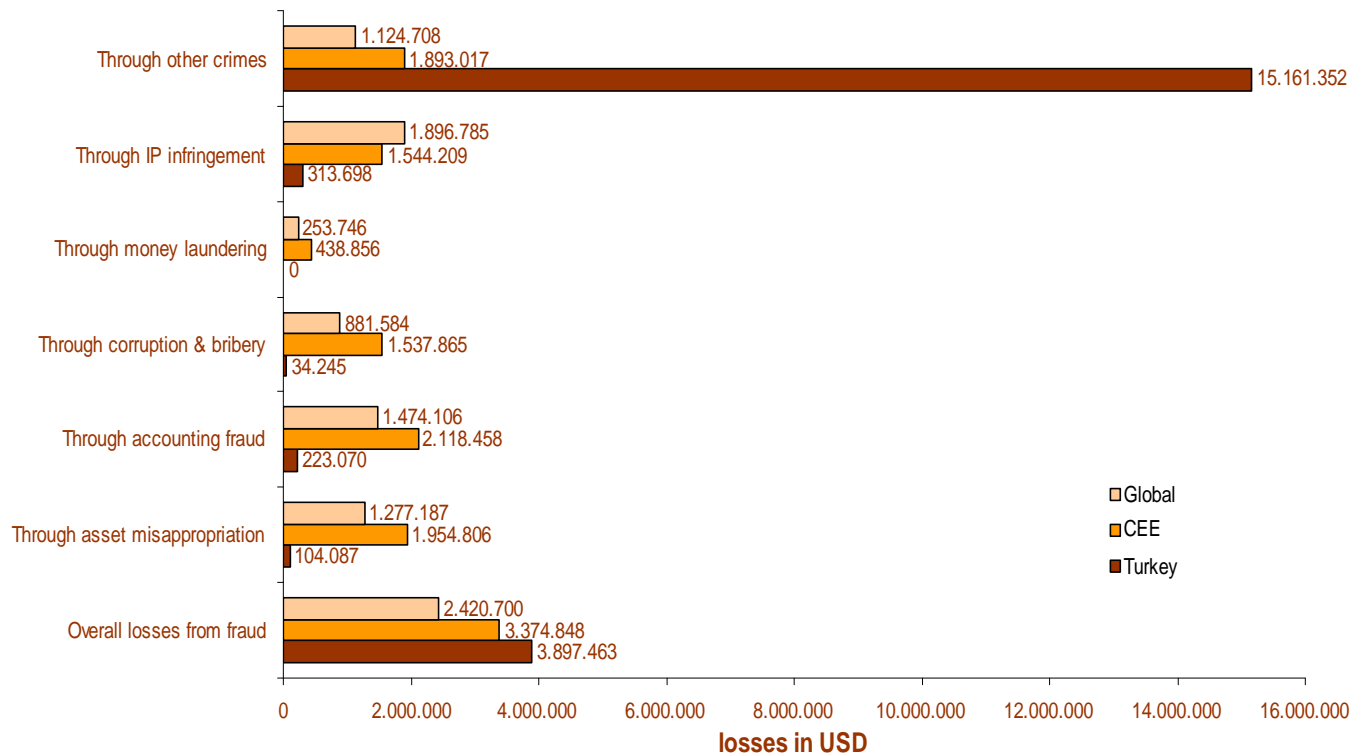


Figure 3 - Cost of Economic Crimes, PwC 2007

Collateral damage is another effect of fraud incidents. Collateral damage is highly related with the company's brand and the customer's trust; the share prices and the shareholder's trust; the company's relationship with its suppliers and the staff morale. As a conclusion we can add that collateral damage can indirectly affect the financial loss of the company via clients and shareholders. The global study of PwC in 2007 pointed out that %80 of the respondents stated that fraud incidents damaged their business. When we compare with the financial loss, we can see that determining the collateral damage is much more difficult. In Turkey it has been found that the fraud incidents of corruption and bribery, and money laundering caused the highest collateral damage up to year 2007.

I want to give a current example from Turkey in order to express both material and collateral damage. On July 2008, Capital Markets Board of Turkey (CMB) declared crime report for the general manager of Tukaş Company which is the group company of OYAK A.Ş. The reason of the crime report was about the loss of the shareholders because of the fraudulent reported financial statements belong to 2005 and 2006.

When we examine the stock market trend of Tukaş shares, we see that there is a decrease in prices.



Figure 4 - Price Movement of Tukaş Stocks Between The Years 1999-2008

Source: Istanbul Stock Exchange Matriks Data Server



Figure 5 - Price Movement of Tukaş Stocks During July 2008

Source: Istanbul Stock Exchange Matriks Data Server

In this way, there is both material and collateral damage. First of all, after the crime report of CMB, reliance to company decreased and the image of the company was disparaged. Then the share prices decreased and both company and the stockholders met with a loss.

Another study that focused on the methods of fraud incidents was carried out by Association of Certified Fraud Examiners (ACFE) and it was published in 1996⁵. According to this study asset misappropriations, corruption and fraudulent statements were among the most important occupational fraud methods.

When we evaluate the results of this study (see table 1), we may see that asset misappropriation has long been a vital problem for the companies around the world. We

⁵ Report to the Nation on Occupational Fraud and Abuse, ACFE (1996)

can go back and compare the results of PwC studies in 2007 with these results and as a conclusion we may add that the strategies, which have been developed in order to combat with fraud, have been inadequate.

Table 1 : Comparison of Major Occupational Fraud Categories by 1996 and 2002 Data				
	2002		1996	
Scheme type	Fraud incidents	Cost of fraud incidents	Fraud incidents	Cost of fraud incidents
Asset misappropriations	85.7	\$80,000	81.1	\$65,000
Corruption schemes	12.8	\$530,000	14.8	\$440,000
Fraudulent statements	5.1	\$4,250,000	4.1	\$4,000,000

*Readers will note that the sum of percentages in this column exceeds 100%. A number of the schemes that were reported in this survey involved more than one type of fraud; thus, they were classified in more than one category. In the 1996 survey we classified schemes based on the principal method of fraud only.

Source: www.cfenet.com

A study by an internal auditor called Jonny Frank (2004), revealed also some important points about the risk assessment and cost of fraud incidents. According to this study, risk assessment and the cost of fraud is the cornerstone of fraud incidents.

There are different kinds of risk assessments and we may say that the risk assessment of a fraudulent incident and the traditional risk assessments differ from each other. The traditional risk assessment focuses on the main objectives of a company. The main point of such a risk assessment is to determine to what extent the aims are fulfilled.

Fraud risk assessments focus on the control problems and the main point of such assessment is to detect, to report and to prevent fraud incidents. To a wider extent we may say that fraud risk assessments deal with the circumvention of the control programs and as a result of this investigation it has been determined how vulnerable the company to fraud risk is.

Scenarios and fraud schemes are the foundation stone of a fraud risk assessment period. The assessment team has to investigate the geographic situation of the company and its place within the emerging market in order to identify the potential fraud schemes and scenarios. The team has to pay attention at three points during this process. These are:

- a. The impact of a fraud incident upon the reputation of the company or organization
- b. The criminal and civil liability of the company as a result of a fraud incident
- c. The material / financial loss due to a fraud incident.

2.2.1 The Duration of Fraud

The duration of a fraud incident is one of the most important details, because the longer a fraud goes undetected, the larger should be the amount of material and collateral losses. The duration may be effected by the size and type of the organization, the lack of controls in the management systems, the perpetrators situation within the company or

organization...etc. A questionnaire study was carried out by BDE GLOBAL (Business Defense Europe) related with the duration of fraud incidents and the academicians asked some questions to the respondents. Respondents were asked to indicate the duration of the fraud as falling into one of the following categories, less than 6 months, 1 year, 18 months, 2 to 5 years and over 5 years. These data were expressed as a continuous variable by converting the category into a fraction of years and, where appropriate, taking the category mid-point. An assumption was made that the maximum fraud duration is ten years and, therefore, the over five years' category was defined for these purposes as 7.5 years. Usually, the longer an occupational fraud goes undetected, the larger should be the amount lost or stolen. The mean duration statistics tend to support this. According to Pearson correlation coefficient, which is .244, the monetary size and the duration of the fraud incidents are interrelated. As a conclusion of this study categorizations were made about the duration of fraud incidents. These categories were:

a. Duration of fraud for less than 6 months

b. Duration of fraud for 1 year

c. Duration of fraud for 18 months

d. Duration of fraud for 2 to 5 years

e. Duration of fraud for over 5 years

Some assumptions were made according to the categorizations above. One of them is that the maximum fraud duration is ten years. The questionnaire study of BDE GLOBAL found

out that it is a bit easier for the auditors to detect the fraud incident whilst ongoing, because the fraud perpetrator, who carried out a successful fraud incident in the past, may have terminated all the evidence so that no one can find a trace concerning the fraud incident. Conversely, if the fraud is undetected the perpetrator may have been unable to hide the evidence and related accounting documents.

3 – THE POTENTIAL VICTIMS AND THE PERPETRATORS OF FRAUD

In this section, victims and the perpetrators of fraud will be examined in detail. How these two factors affect each other and what kind of correspondences they have. The susceptibility of fraud incidents also will be defined.

3.1 The Victims of Fraud

Joseph T. Wells, the founder and the chairman of the Association of Certified Fraud Examiners, Austin, Texas, and the professor of fraud examination at the University of Texas, focused on different types of fraud victims in his study, which was carried out in 2002. According to this study there were two key points when determining the victims of fraud incidents. These key points were related with the type and the size of the companies. The largest losses appear in public companies, because they have more assets than nonprofits and governmental companies. Conversely, we can say that the nonprofits and the governmental companies appear to have the smallest losses because of fraud incidents. (See table 3)

The number of the employees is also another issue, which determines the loss and victims of fraud incidents. The smallest companies are more vulnerable to per – employee losses (see table 2). This is because of three factors:

1 – The lack of basic accountings: Since the numbers of employees are not high in small companies, there may not be more than one individual who are writing and signing the checks and to control the company's accounting book.

2 – Trust: Since the number of employees is not high in small companies, we can say that there is a high possibility that all the employees know each other well. The possibility of a fraud incident may decrease in an atmosphere, where nearly all employees know each other.

3 – Auditing: Small companies are not so often audited. The same study was also carried out in 1996 and these results were similar to this study.

Number	Fraud cases	Average loss
1–99	39.0	\$127,500
100–999	20.1	\$135,000
1,000–9,999	23.4	\$53,000
10,000+	17.5	\$97,000

Victim	Fraud cases	Average loss
Government agency	24.7	\$48,000
Publicly traded company	30.0	\$150,000
Privately held company	31.9	\$127,000
Not-for-profit organization	13.4	\$40,000

Source: www.cfenet.com

3.2 The Perpetrators of Fraud

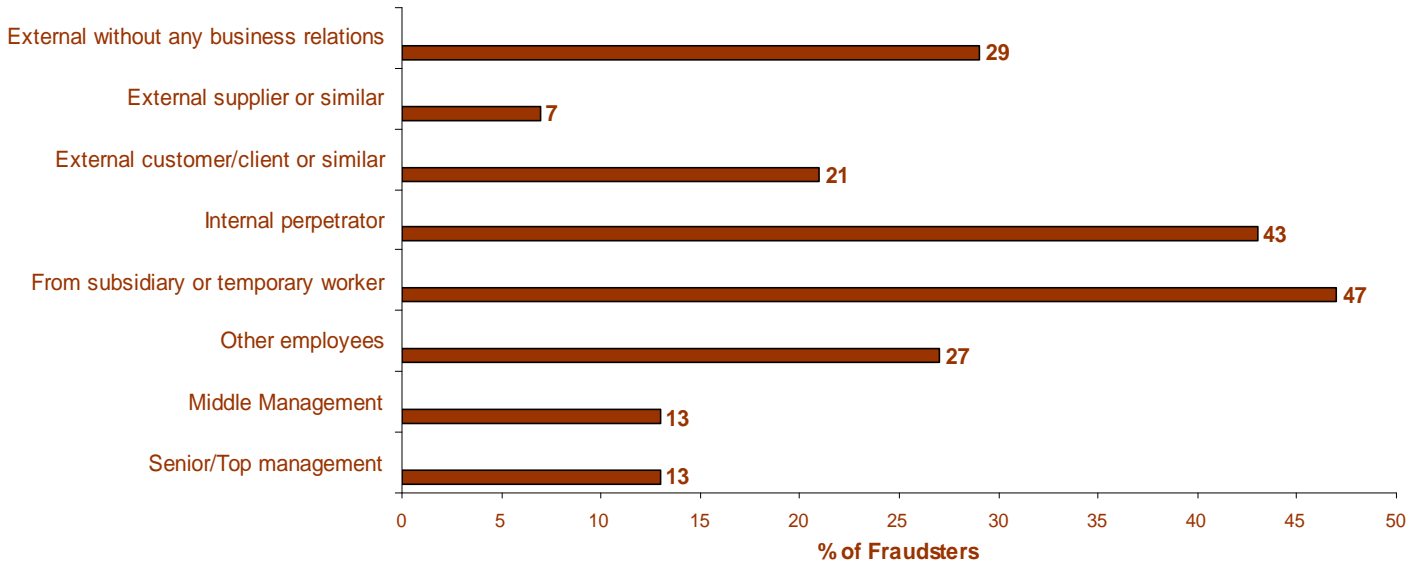


Figure 6 - %43 of Fraud Committed in Turkey was Perpetrated by Employees with One in Four Being Committed by Management (PwC 2005)

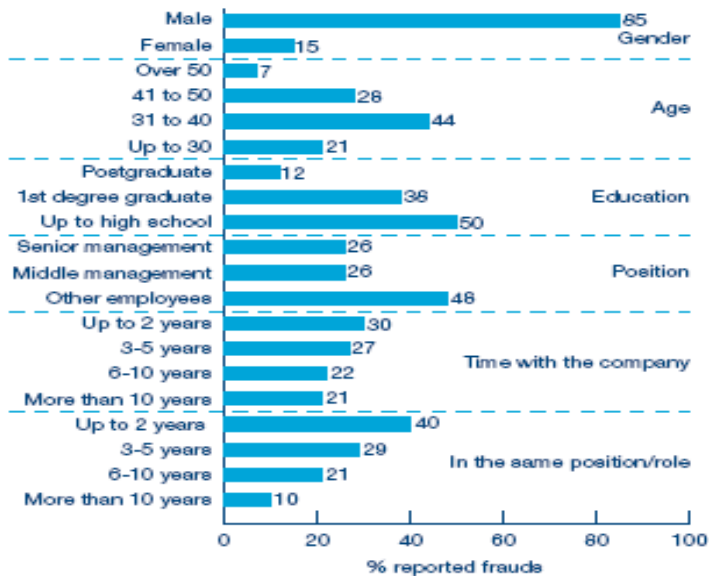


Figure 7 – Profiling the Fraudster (PwC 2005)

The study of PwC demonstrates some basic characteristics of the perpetrators. According to this study, the perpetrators of fraud are in most cases male and they are between the age of 31 and 40. One of the most interesting points of this study is that the perpetrators are generally educated to degree level or higher. Another interesting point is that half of the perpetrators are employed by the defrauded company and almost one quarter of them works as a senior manager (see figure 6 and 7). The Association of Certified Fraud Examiners (ACFE) revealed a report in 2004, which included some information about the characteristics of fraud perpetrators. Different from the study of PwC, this report revealed that the time on job has also been an important factor for fraud perpetrators. This is defined as:

“The longer an employee works for organization, more likely he or she is to advance to higher level of authority.

Longer an employee works for an organization, the greater degree of trust he or she will tend to engender from supervisors and co – workers.”

This report explains also some red flags about a fraud crime. These are:

- Not taking vacations
- Not allowing someone else access to the area of responsibility
- Prefer to be unsupervised by working after hours or taking work home
- Financial reports sometimes disappearing
- Unexplained debts
- Unexpected change in behavior

These indications are called as “red flags” within the framework of this report. From these points you may understand that someone has the potential to commit a fraud crime. Red flags have been used within the academic literature as signs of fraud in the accountancy practitioner guidance and the internal auditors may examine these red flags to prevent the fraud incidents. (For example, Albrecht et al 1995, Bologna, 1993, Bologna and Linqvist, 1995, and Wells, 1997, AICPA, 2003).

Moreover, Practitioner Surveys by Ernst & Young (2001) and KPMG (1999) show how important the red flags are in the identification of fraud incidents.

Another study carried out by Javelin Strategy & Research in the year 2004 focused on the identity fraud, which is related to misuse of personal information. This study revealed that the perpetrators of identity fraud may also be a family member, a friend, a neighbor or a relative of the victim (see figure 8 and figure 9). From these studies we may understand that it is not so important whether you are the head of a company or a man on the street, but you have to pay attention even to your close friends and relatives in case of a fraud risk.



Figure 8 – How Close is the Fraud Perpetrator to You?, Javelin Strategy & Research (2004)

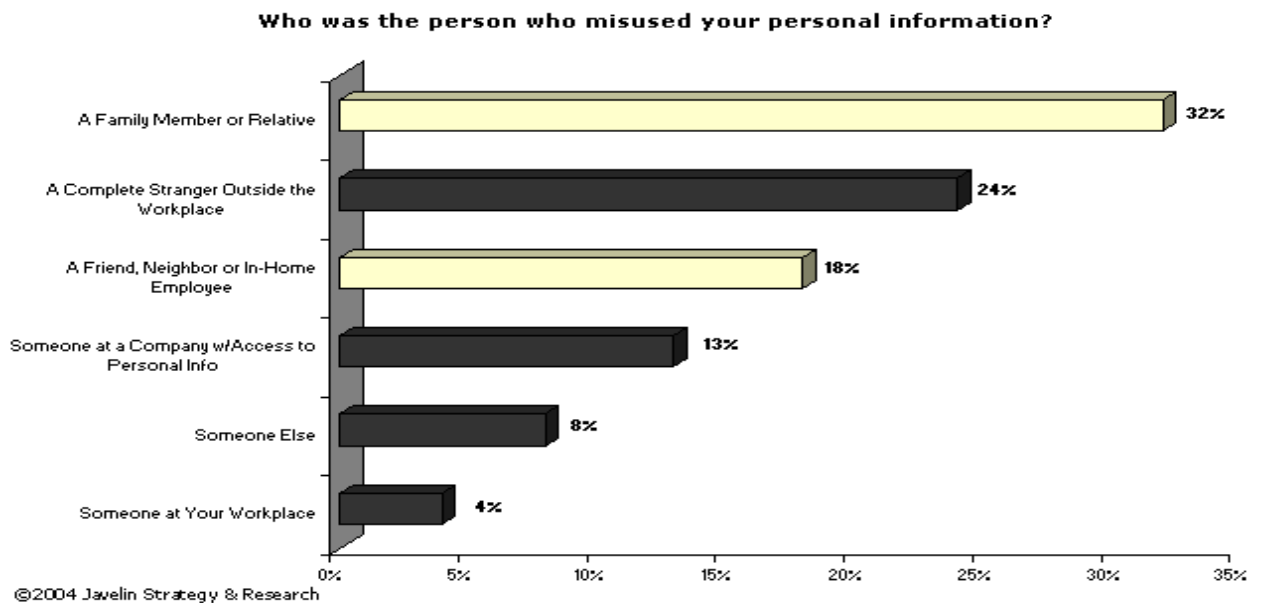


Figure 9 - Who was the Person Who Misused Your Personal Information?

Also a study carried out by Joseph T. Wells (2002) pointed out that approximately 33% of fraud incidents reported involved two or more perpetrators. These kinds of fraud incidents cause more loss to the company and they are better organized while each individual fulfills his own task.

3.3 Economic Crimes, the Number of the Victims and the Number of the Perpetrators

Dr. Russel G. Smith from the Australian Institute of Criminology presented a paper related to the controlling of economic crimes (2001). In his study he categorized the economic crimes according to the number of the victims and the perpetrators of the crimes. The categories that are mentioned within this study are:

- One perpetrator – one victim
- One perpetrator – multiple victims
- Multiple perpetrators – one victim
- Multiple perpetrators – multiple victims

3.3.1 One Perpetrator –One Victim

Within the framework of the first category, we may confront with a perpetrator who commits an economic crime in one country to a victim who lives in another country. Dr. Russel G. Smith dealt with an English case of *R. v Thompson* ([1984] 1 WLR 962). At this case the defendant was a computer programmer working for the Commercial Bank of Kuwait. At first he opened saving accounts at five local branches of the bank in Kuwait. Then he programmed the computer of the bank so as to debit the accounts of the victim and credited the five accounts he had opened. He later left Kuwait and went to England. He

opened there five more new accounts within the English bank and wanted the Kuwait bank to transfer all these amounts to the English bank. Namely, he withdrew an amount of £45,000 from the bank in Kuwait. Thompson was charged in England because of his economic crimes. The English Court of Appeal gained control over his funds in England.

3.3.2 One Perpetrator – Multiple Victims

Within the framework of the second category, we may be confronted with a perpetrator, who gives damage to multiple victims. One of the recent issues about this category is related to a 24 year – old man who lived in Melbourne. He manipulated the share prices of an American company by sending E – mails on the internet. These mails included false information about the company. On 08.05.1999 and 09.05.1999 he sent messages and e - mails on Internet Bulletin Boards in the United States to the recipients from the United States, Australia and in other parts around the world. During those days the share value of the company was US\$0.33 and this 24 year old man informed his victims that this share value would increase to US\$3.00. Moreover, he added that the value may increase up to 900 per cent within the next few months. As a result of this misinformation the company's share prices on the NASDAQ doubled and the trade volume was also affected by this incident.

The perpetrator had purchased 65,500 shares from the company just several days before he had transmitted the wrong information. Subsequently, the Australian Security and Investment Commission found the perpetrator guilty due to the transmission of intentional, false and misleading information. The Court ordered that 21 months of the sentence be suspended and he was bound with a surety of \$500 (*Australian Securities and Investments Commission v Steven George Hourmouzis*, County Court of Victoria, 30 October 2000, Stott J).

3.3.3 Multiple Perpetrator – One Victim

We can explain this category directly via the example of the Citibank case in 1994. A group of Russian computer hackers tried to steal about US\$10.7 million from various customers of Citibank. During this process they benefited from the computerized funds transfer system of the bank.

Vladimir L. Levin was one of the perpetrators and he worked in a Russian firm. He used a personal computer, stolen passwords and identification numbers in order to benefit from the funds of Citibank. He was able to confirm the transfer process of Citibank's funds via a computer terminal in his office in St. Petersburg. Namely, he and his friends were able to transfer the funds of Citibank to the accounts held in California, Finland, Germany, the Netherlands, Switzerland, and Israel.

On March 3rd, 1995 he was arrested at the Stansted Airport in England. After the legal procedures he was sentenced to 3 years imprisonment and he had to pay an amount of US\$240,015 to Citibank.

The last current example is Tesco Kipa Kitle Pazarlama A.Ş. ("Tesco Kipa") case in Turkey. 5 people (2 of them worked at Tesco Kipa, İzmir) tried to defraud Tesco Kipa. S.B. is the accounting clerk who is responsible of the investments and fixed assets process of the company. She used another coworker's password who has the access of invoice recording and payment order giving. Other members have imaginary companies that sell goods to Tesco Kipa. She recorded the imaginary invoices to the system and gave payment order to those companies. However it is noticed by the employee who is responsible for the

preparation of “one purchase one sale” form* that the tax number of those imaginary companies did not pair off the numbers at Tax Office. Then the situation was declared to Ministry of Finance and at the result of the investigation, S.B. and her friends were arrested for 1 months. The cost of their fraudulent activity to Tesco Kipa is YTL4,500,000. Now they are released pending trial.

As you see, in the first case Citibank is the victim, and Levin and his friends are the perpetrators. Again, in the second case Tesco Kipa is the victim and S.B. and her friends are the perpetrators. Therefore, we can say that this case belongs to multiple perpetrator – one victim category.

3.3.4 Multiple Perpetrator – Multiple Victims

In this category, we may see that a group of perpetrators aim to benefit from a group of victims, who can also be from various countries. The fee frauds since the 1980s can be seen as an example for this category. The United States Secret Service estimated that about US\$5 billion had been stolen from victims around the world via this kind of economic crimes since the 1980s. In this category, we may say that the E – mails have been very useful in order to define the identity and personal information related to the perpetrators, because each of them may send fee letters.

3.4 The Susceptibility to Fraud Incidents

According to a global economic crime 2005 survey of PwC, it has been found that 45% of the companies have fallen victim to fraud incidents since 2003. The survey pointed out that this number has increased during the recent years. Many companies have taken measures in

order to combat fraud incidents, but why are they still confronting fraud risks? This is the question that we will try to explain under this topic.

The factors that contribute to the occurrence of fraud incidents vary and so as to understand the susceptibility of the companies within the market to fraud incidents we have to explain these factors. According to the study of PwC in 2005, it has been found that larger companies are more vulnerable to fraud incidents. As a result of this conclusion we may say that Well's perception of fraud in 2002 (see table 2) has changed with this study. The survey of PwC in 2005 demonstrated that the only 36% of small companies suffer from fraud incidents. At the same time 62% of the large companies reported fraud incidents within this study. ⁶

According to PwC, the greater opportunities for fraud incidents are:

- a) The complex structure of a company: The structure of a company is more complex, if the company is large, because the staff is loaded with more complex responsibilities and there are many objectives, which they have to fulfill.
- b) According to the fraud perpetrators in large companies, a fraud incident is much more accepted as a "victimless crime." They may think that their damage would not cause so much damage to the organization.

⁶ In this study, small companies are the ones which have less than 200 employees nationally and the large companies are the ones which have 5000 employees nationally. (PwC)

c) Larger companies may have closer relationships with international companies. As a result of this relationship, they may have to stay in contact with new and unfamiliar markets and employees, and this increases the opportunity for fraud incidents.

The study of BDE also reveals some factors that are important when determining the vulnerability of a company to fraud incidents. These factors are: The organizational characteristics, the organizational type, the industrial sector, the management controls and the assets.

3.4.1 The Organizational Characteristics

The characteristics of the organization may both influence the amount of the losses and the type of fraud that is committed. One of the most important characteristics of an organization is related to its size. The size of a company may affect the structural controls, the opportunities for fraud and the motivation of employees. We may think that if a company's size is larger, it may suffer more from fraud incidents. Actually, I do not agree with the idea that smaller companies suffer less from fraud incidents, but they may not be able to report and detect all fraud incidents because of a lack of a sustainable control system. Larger companies have more opportunities to implement professional control programs, but it has been found that larger companies lose more money because they have more funds in order to renovate themselves and this creates an opportunity for the perpetrators (Akerlof and Romer, 1993).

As a conclusion we may add that the susceptibility of an organization may increase with the size of an organization.

3.4.2 The Type of the Organization

According to Leatherwood and Spector (1991), the type of the organization has also been an important factor, which affects the vulnerability of an organization to fraud incidents. Jensen and Meckling also prepared a seminar paper (1975) and they supported that the organizational type may create an opportunity for fraud incidents through the agency problems, which can cause from the separateness of the ownerships and the controls of large corporations. The type of organization determines the performance of the staff and it may be effective on the incentive factors on fraud.

According to the study by BDE GLOBAL the following hypothesis concerning the fraud issue can be conducted as a conclusion of the effects of the characteristics and type of the organization.

Hypothesis 1: The characteristics and type of the organization has a function when determining the susceptibility of an organization. The possibility of a fraud incident may increase with an enlargement within an organization.

Hypothesis 2: The level of the collateral and material damage depends on the size, characteristics and type of the organization.

3.4.3 Industrial Sector

The fraud incidents are not only affected by the internal factors such as the type of the organization, the characteristics of an organization and the management control, but they are also affected by external factors such as the cultural features of an industrial sector. The

situation of the organization within the emerging market and the changes within the market may also affect the possibilities of fraud incidents. For example, fraud incidents and fraud perpetrators within an insurance company may differ from those within a telecommunication company. Clinard and Yeager (1980) support that this difference is because of the different norms, which have been manipulated within the industrial sectors.

3.4.4 Management Controls

Management controls have been vital for organizations to combat fraud perpetrators, because the susceptibility of an organization may vary due to the effectiveness of the management controls. The capacity of an organization in order to implement fraud policies and procedures (prevention, detection, investigation and prosecution) against the fraud incidents depend on its funds (NCFRR, 1987; ACFE, 2000). There is an “acceptable amount” for each organization. Namely, this amount refers to the loss, which the organization is able to bear. The policies, procedures and the control programs have to be based upon so – called acceptable amount of the organization.

Schnatterly (2003) demonstrates that the management controls have to be supported by governance measures, but she also reveals that these measures are not deterrent enough because of their limits. An operational mechanism, which goes beyond the accounting system, notably clarity of policies and procedures, formal cross – company communication, and performance – related pay should significantly reduce the likelihood of reported fraud incidents.⁷

⁷ Report of BDE in 2005

When determining the required policies and procedures of a management control system, the basic needs of a professional system and the different cases should be taken into consideration. Wells (1997) examined hundreds of cases and as a conclusion he decided that the nature of the management system should be helpful for the organization. For example he proved with the Vasiloff case (Wells, 1997, pp. 499-503) that the lack of separation of duties, proper authorization procedures within the public sector may create an opportunity for fraud perpetrators.

To establish a well – operating management control system is not enough to combat with fraud incidents. The procedures and the policies, upon which the management control system depends, should be in harmony.

3.4.5 Assets

The nature and the amount of the assets are also another factors, which affect the vulnerability to a fraud incident. If the amount of the assets is high, the risk of fraud may also be higher. Certain asset categories may provide scope for greater gains to the fraudster than others. For example, the size of a fraud involving theft of stock may be limited by physical constraints whereas there are no such limits on the transfer of money.⁸

⁸ Report of BDE in 2005

4 - RELATED LITERATURE

In this section, the white – collar crime, the blue collar crime, occupational crime and the state – corporate crime has been discussed in order to support this study with a theoretical view.

4.1. The White – Collar Crime

White – collar crime has been defined by Edwin Sutherland (1949) as “a crime committed by a person of respectability and high social status in the course of his occupation”.⁹

Sutherland was an adherent of “Symbolic Interactionism” and according to this belief criminal behavior was learned from interpersonal interactions with others. Therefore, we can say that the white – collar crime deals with the corporate crime because the possibility and opportunity for fraud, bribery, computer crime and forgery is more available for white – collar employees. The most important characteristic of white – collar crime perpetrators is that they stem from high social classes.

Modern criminology divides this issue into some topics because the criminology rejects a limitation about this term. These topics are:

- The Type of Offense: Property crime, economic crime and other corporate crimes are categorized as crimes, which violate the environmental, health and safety laws. These kinds of economic crimes occur as a result of the identity of the perpetrator. For example, asset misappropriation or money laundering require the participation

⁹ [http://en.wikipedia.org/wiki/white-collar crime](http://en.wikipedia.org/wiki/white-collar_crime)

of senior employees working within the organization. The Federal Bureau of Investigation (FBI) has accepted a narrow perception concerning this issue. The white – collar crime is defined by FBI as “those illegal acts which are characterized by deceit, concealment, or violation of trust and which are not dependent on the application or threat of physical force or violence” (1989, 3). The actual cost and extent of the white – collar crimes are unknown, but FBI estimated the cost of white – collar crime in the United States as \$300 billion annually.

- Type of Offender: Shover and Wright (2000) stated that the essential neutrality of a crime is highly related with status, characteristics and backgrounds of the involvers. The type of the offender depends on the characteristics of the perpetrator and the points that have to be taken into consideration, when examining the characteristics of the perpetrator in relation with white – collar crimes, are stated below.

- a) Social class or high socioeconomic status
 - b) The position of trust or the profession of the perpetrator
 - c) The academic education level of the perpetrator
 - d) The researches related to the motivation of the perpetrator for criminal behaviors
 - e) Fear of loss
- The Organizational Culture: The availabilities within the organization are also strictly important, when examining the cases of white – collar crimes. The organizational culture includes the structure, the capacity, the market position, the procedure and the flexibility of the organizations. Appelbaum and Chambliss (1997, 117) offer a definition concerning this part:

“Occupational crime, which occurs when crimes are committed to promote personal interests, includes the alteration of record and overcharging, or the misuse of clients by professionals.

Organizational or corporate crime, which occurs when corporate executives commit criminal acts to benefit their company includes overcharging or the fixation of the prices, false advertisements...etc.”

4.2 The Blue – Collar Crime

The blue – collar crime is a bit related to the socioeconomic culture of the perpetrator. In this category, the possibility to commit a fraud incident is related to the opportunities that the perpetrator confronts. The perpetrators of blue – collar crime are from lower social classes. For example, those who are living in a town and those who work at a situation that is irrelevant to their skills have less opportunity to commit economic crime than those who live in a region where the life standards are very high and those who work at a situation that is related with their skills (Clarke, 1997). The latter may have more knowledge about the sector, in which he is working, and should be more aware of his duties; because he may work in a job, in which he can develop himself according to his skills. Vandalism, shoplifting, crimes against a person, crimes against a specific kind of prosperity, prostitution, gambling and drug abuse can be evaluated as blue – collar crimes. At this point, we can say that the detection of blue – collar crimes require much more active police attention.

4.3 Occupational Crime

“The 2002 Report to the Nation on the Occupational Fraud and Abuse” published by Association of Certified Fraud Examiners (ACFE) defined occupational crime as “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.” Cash larceny, skimming, billing schemes, payroll schemes, expense reimbursement, check tampering, register disbursements, non – cash misappropriations, corruption schemes and fraudulent statements are among occupational economic crimes (see table – 4) .

Table 4 : Frequency and Loss Comparison of 1996 and 2002 Data				
Scheme	2002		1996	
	Fraud cases	Average cost	Fraud cases	Average cost
Cash Larceny	6.9	\$25,000	2.9	\$22,000
Skimming	24.7	\$70,000	20.3	\$50,000
Billing schemes	25.2	\$160,000	15.7	\$250,000
Payroll schemes	9.8	\$140,000	7.8	\$50,000
Expense reimbursements	12.2	\$60,000	7.0	\$20,000
Check tampering	16.7	\$140,000	11.5	\$96,432
Register disbursements	1.7	\$18,000	1.3	\$22,500
Non – cash misappropriations	9.0	\$200,000	10.7	\$100,000
Corruption schemes	12.8	\$530,000	14.8	\$440,000
Fraudulent statements	5.1	\$4,250,000	4.1	\$4,000,000

When we examine the incidents related to occupational economic crimes, we may see that there are three important indications, which show us a possibility of an economic crime. The first is related to the interest of a company. As we know there are many qualified suppliers within the emerging market, but if the company is interested in just one type of Seller Company, it may be an issue related to an economic crime. The second is related to the prices. Generally, occupational economic crimes include above- market prices. The third is related to the lifestyle of employees. People may benefit from fraud incidents and this should affect their life standards. They may tend to maintain an excessive lifestyle or they may buy expensive homes, cars, cloths and jewelry.

The sections below in relation with 4.3 include some examples of occupational economic crime types.

4.3.1 Skimming

For this case, we may give an example related to a management system within a private school. There may be many students, who apply to the school, but if the budget of the school does not increase, we may think that there may be a problem. As a result of this, the authorities within this school should hire a team of Certified Fraud Examiners (CFE). After the examination of this team, the detection of a fraud incident should be achieved. At this scheme, the most effective way to prevent a fraud incident is to charge more than one managers with the control of the budget, so that at least one of these managers would be able to detect the incident.

4.3.2 Billing

Fictitious entries to the accounting book of the company are related to this type of occupational economic crimes. For example, Company A may have stopped its relationship with Company B years ago, but if the accounting book of the company includes some payments to the Company B during the recent periods, there should be something wrong. At this point a computer security program should be employed by a company supervisor in order to detect the incident. After the detection of the incident, the company should continue to make proper controls related to the accounting book, so that they may be able to prevent another billing incident.

4.3.3 Cash Larceny

These cases are common for small companies, because there may not be a separation of duties and tasks. If there is one person charged with many duties, he may reach the opportunity to commit fraud. At this point we may give an example related to a real – estate company. As we know, they receive deposits from their clients and if an employee removes some amount from these deposits he may be committing a type of economic crime that is called cash larceny. The real estate company should not be aware of the incident, until it runs out of cash. At this time, the documents related to the received deposits are going to be examined by a professional supervisor. The company managers should get information about the fraud incident via these examinations. The economy experts offer a proper independent examination system in order to prevent such cases.

4.3.4 Check Fraud

Think of an employee, who earns an average salary. In this case, we may think that the life standard of this employee should also be at an average level, but in contrast to this idea we may see that he maintains an expensive life. When people ask him how he gained so much money, he may probably say that he won a big amount of money from lottery. The manager of the company, in which this employee is working, should find this situation a bit suspicious and he may decide to invite a team of certified fraud examiners to control books of the company. The examiners may find that this employee forged the checks of this company in order to spend the money, which he did not earn. These cases are called as check frauds and an independent review of bank statements are required in order to prevent these cases, because all checks have to be confirmed by a bank.

4.3.5 Expense Reimbursement

A company may have relationships with different international companies and they may have to visit the locations of these companies in order to maintain a good contact. In this case, there are some employees, who are charged with this task. They may visit various countries. Since they are visiting these countries in relation with their tasks, their expenses are met by the company, but the company may think that they pay a high amount under the topic of “expenses”. As a result of this suspicion the expense documents of employees should be checked and if the amount within these documents does not confirm the amount, which is spent by the company, we may say that there is a fraud incident related to the reimbursement of the expenses and those who are involved in these incidents should be

punished. As a conclusion we may say that a proper examination should be carried out in order to prevent these issues and the expenses should be documented.

4.3.6 Payroll Fraud

These cases are related to the working hours of an employee. If an employee has to work at least for 8 hours, he has to be at the office for at least 8 hours, but if he does not stay at the office during the required time periods and if he does not inform the related authorities about his staying period, there may be a type of fraud. The managers may think that he is at the office during those time periods, but when they implement an internal audit system, they may be able to discover the truth about this case.

There are two major control systems, which can be applied in order to prevent payroll frauds. The first is not to allow employees to post their own payroll records and the second is to install computer systems, which should be able to detect unreasonable entries.

5. INTERNET FRAUDS

Technology has become a part of our lives during the 21st century and as a result of this we use the internet much more than before. When someone is using the internet, it is important that he is aware of the dangerous sides of such a tool that is generally known via its advantages. Since we use internet in all fields, I think that we have to analyze the fraud incidents on the internet. Auction fraud, counterfeiting the cashier's check, credit card fraud, debt elimination, employment/business opportunities fraud, escrow services fraud, identity theft, investment fraud, lottery frauds, Nigerian letter or "419", spoofing frauds, Ponzi or pyramid frauds, spam frauds, frauds related to the third party receiver of funds...etc are types of fraud incidents that can be carried out via the internet.

There are also some red flags, from which you can understand the coming of an internet fraud. These indications are:

- **The grammatical and spelling failures within the e – mails:** Most of the fraud perpetrators live outside of U.S. Hence, their native language shall be another language than English. As a result of this fact, their emails, which are written in the global language which is English, should include grammatical and spelling failures¹⁰.
- **The excessive demand of personal information such as bank account numbers asked by employers:** There are some procedures that have to be carried out in

¹⁰ From the Monday, June 30, 2008 edition of the Augusta Chronicle

order to hire an employee. The employer has to gather some personal information about the employee, but the employee should not give his bank account number without receiving a logical excuse or reason of the employer. If the employee does not take this fact into consideration and gives his bank account number via phone or e – mail; he may have unknowingly developed the required opportunity for an internet fraud.

- **The job hunter may receive an e – mail from the job posting Web - sites, which may inform the job hunter about a problem related to his account:** A job hunter might have filled in some online forms that can be found on web sites such as Monster.com and Careerbuilder.com and after a while he can receive an e – mail mentioning about a problem related to his account. This e – mail may include various solution for his problem such as following a hyperlink or installing a new software. The aims of these mails are to convince the job hunter to follow the advised solutions and as a result of the actions of the job hunter, the perpetrators will be able to get the code number of the account of the victim.
- **The employer offers a chance to become rich without even leaving your home:** There are limited reliable job opportunities that offer the job hunter to work – at – home and become rich, but usually the perpetrators try to benefit from these opportunities. The target group of such fraud incidents includes students, handicapped or injured people.

- **An employer may ask the job hunter to pay money beforehand:** As we said there are some procedures that have to be carried out in order to hire an employer through the internet, but an employer does not have the right to ask for money beforehand. The job hunter should only pay money for a uniform. Generally, the victims have not been able to get in contact with the involved company in case they paid money beforehand.
- **The opportunities and chances to be offered may be too good to be true:** In today's world it is very difficult to earn the money you deserve. Regarding this fact, unbelievable opportunities and chances may develop a suspicious situation. At this point the job hunter has to be careful and realistic.
- **The requirement to wire money through Western Union or MoneyGram:** An employer may ask an employee to wire money to the Western Union or MoneyGram in return for a check, but usually these checks are discovered to be fraudulent. As a result of such incidents, the bank account of the job hunter may be empty without getting a job or any benefits.

5.1 Auction Fraud

As we know there are some web – sites, from which you can buy some products, but these sites are not always reliable. There may be misrepresentations related to the product or you may not be able to receive the product. This kind of fraud incidents are analyzed under the topic of “auction fraud”. According to the Internet Crime Complaint Center, which is in

relation with FBI, there are some indications, which help us when detecting a fraud risk.¹¹

These indications are:

1. The place, where the seller resides, must be stable. For example, if he states that he resides in Romania and then informs the victim that he is not in Romania, it may be a suspicious situation on behalf of the victim. The same suspicion is valid, if the seller asks the fund to be transferred to another individual, but not himself.
2. If the required money is asked to be transferred via Western Union, MoneyGram or bank – to – bank services, the amount involved may be in risk, because it is nearly unrecoverable without the awareness of the victim.
3. We have to be careful, if the buyer wants another type of shipment service in order not to pay the required custom costs and taxes.
4. If the purchase is made via a credit card, one must be careful that the address of the card holder approves the shipping address.

The security alerts on the web – sites of eBay and PayPal may also be helpful for the customers in order to carry out a perfect purchasing process without any problems. Shill bidding can also be examined under the topic of auction frauds. “It is the practice of attempting to increase the final selling price of an auction item by entering a phony bid on one’s own product”.¹² Generally, we may come across to such kind of fraud incidents on eBay. Shill bidding is preferred in order to inflate the prices of some products. At this kind

¹¹ <http://www.ic3.gov/crimeschemes.aspx>

¹² Online Auction Fraud: Ethical Perspective by Alex Nikitkov and Darlene Bay

of frauds, the price of the product may increase via the several biddings made by the seller. The buyer may think that the biddings are made by other customers and this may stimulate other buyers to bid to the involved product. According to the study of Alex Nikitkov and Darlene Bay (2007), we may say that internet frauds, such as shill bidding are illegal and unethical. Therefore they are also prohibited by eBay (www.eBay.com/help/policies/seller).

The decision tree of Alex Nikitkov and Darlen Bay, which illustrates the possibility of a shill bid, is below. The thermometers indicate the possibility of shill bidding in different situations. The thermometers, which have a higher level of red, have a higher level of possibility in terms of a shill bid. The thermometers, which are full means that there are sufficient evidences to support a fraud incidence. If the thermometer is empty, it means that there is no possibility for a fraud incidence.

Online Auction Fraud

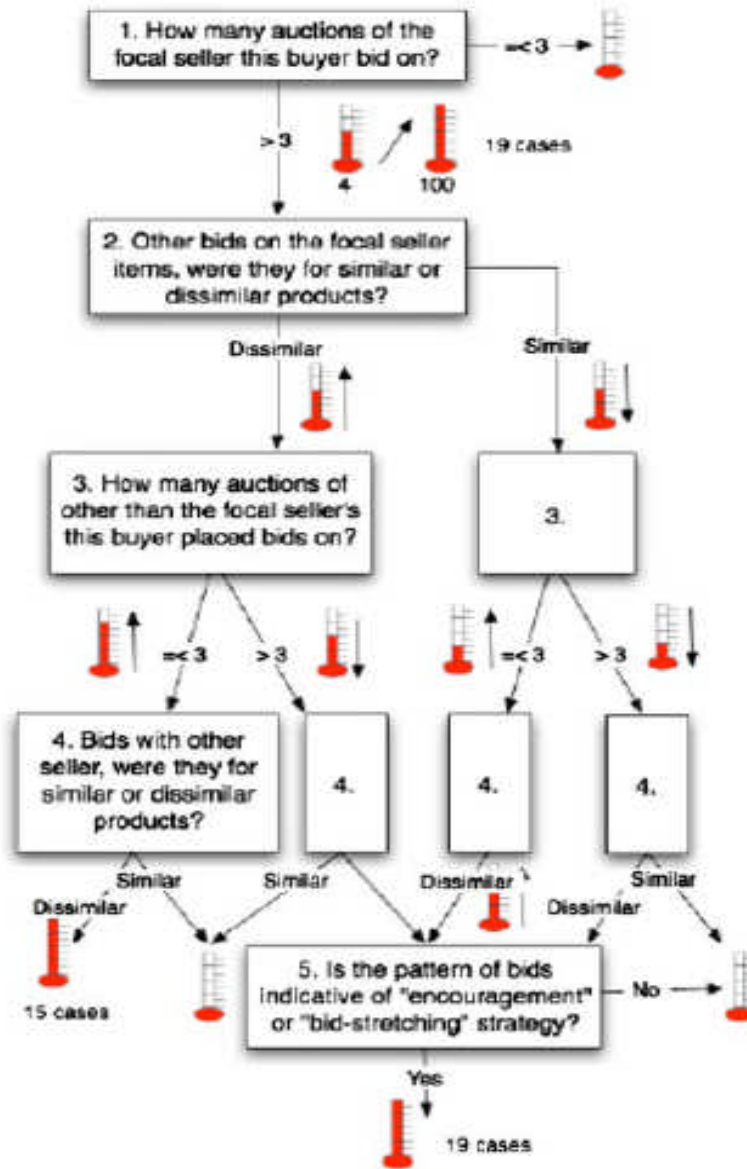


Figure 10 - Shill Bid Identification Algorithm Decision Tree, Alex Nikitkov and Darlene Bay (2007)

5.2 Counterfeiting the Cashier's Check

The target group of such cases consists of individuals that use internet classified advertisements to sell merchandise. These cases also occur as a result of the computer technology, which offers the perpetrators the ability to carry out perfect counterfeits. Many people may have fallen victim to such kinds of fraud incidents, because it is very difficult to discriminate a genuine check from a counterfeit check. The person, who accepts a counterfeit check, is responsible for the involved item. At these cases there are many possibilities:

- You may get a bad check from the counterfeiter
- You may receive an overpayment for the item you sell
- You may get a check and the counterfeiter may ask you to wire the amount on the check.

As a result of such cases, the victim may not only lose his money, but also his reputation. He may also be responsible for the check and this means that he is the one, who has to deal with the issues related to the involved check.

The victim has to be aware of some of the red flags of counterfeit cashier's check. Some of these red flags are:

1 – If the offer is outside the country of the victim (or maybe outside the USA) it may be quite suspicious.

2 – If the Buyer sends you an amount, which is quite higher than the amount you demanded, you have to take the possibility of a fraud incident into consideration.

3 – Call the related bank authorities in order to confirm that the check is genuine.

4 – Ask the other party to pay the amount in cash or to wire the amount to your bank account, so that you will not have to deal with a fraudulent check.

5.3 Credit Card Fraud

Credit card fraud is related to the cases of identity fraud incidents. The perpetrator has to be able to receive the personal information of the victim in order to commit such a crime. Namely, the internet is a reliable tool for the perpetrator to get the required information about the victim. Credit card numbers of the victims can be stolen from the unsecured web – sites. The Internet Crime Complaint Center has reported many incidents of credit card frauds during the recent years and the amount of the incidents has still been rapidly increasing.

There are also some cases that are related to a stolen credit card. When a credit card is stolen, it does not mean that it loses its validity. The one, who stole the credit card, may be able to use the credit card and he is not responsible to pay the amounts he uses via the stolen credit cards. There are signature panels on credit cards and these panels may be helpful in order to prevent the usage of a stolen credit card. However, these signature panels may also not be effective when preventing these cases, because the counterfeiters are able to forge the signature of the victims.

Shortly, we can add that the potential victims have to take care of their identity information in order to prevent these cases.

5.4 Debt Elimination

Generally, debts should be paid off in a particular order, but people hate paying their loans. If people do not pay their debts on the required date, he has to pay the interest rate of the involved amount. Debt elimination cases are usually related to the amount of mortgage loans and credit card debts. There are some specially prepared documents to eliminate the debt, but these cases are fully illegal. Dave Ramsey (2003) wrote in his book called “The Total Money Makeover” that the debts and the interest rates compose gradually a “Debt Snowball”¹³, if the amounts are not paid off in a regular order. According to the Debt Snowball method, one has to regulate his debts according to their amounts. The smallest debt has to be paid at first and then he has to pay the other smallest amount. At the end on the snowball he may be able to pay the largest amount. Namely, he eliminates the debts one by one via this method without causing any fraud incidents.

Debt elimination fraud can be carried out via the internet, because the victims enter their personal information in order to give some basic acknowledgement about them. Nevertheless, this information may be used for bad aims by the perpetrators and these cases related to the debt elimination causes to variable fraud incidents.

¹³ <http://www.daveramsey.com/etc/cms/index.cfm?intContentID=4055>

5.5 Employment/ Business Fraud Incidents

As we all know there is some work – at – home opportunities for some employers and as a result of these opportunities foreign – based companies search for employees via their internet web – sites. Some of these companies shall be quite reliable, but you should be aware of the fact that this system does not give more money then you deserve within a short period of time. These opportunities are based on high skills, abilities, good communication skills, hard – working, performance ...etc. Such working relationships depend on trust. The company has to trust employees and employees have to trust the company. However, this opportunity may cause various fraud incidents, which are more common in sales endeavors. The employee candidates write some information about their identities through their copies of identification, driver’s license, birth certificate, or social security cards.

The so – called authorities of the involved companies may promise employee to pay his salary by using a check, but this check shall include a higher amount than the employee expects. Employers tell employees to transfer the overcharged amount to the bank account of the employers. However, at the end of this transfer the involved employees shall be able to discover that the checks are fraudulent. This is often found after the transference of the overcharged amount of money.

Before making decisions related to such opportunities, people have to collect thorough information about the other party. Reliable information about the companies can be found via the Better Business Bureau and the Federal Trade Commission. Thanks to these organizations you may be able to avoid internet based scams and as a result of this you may have better business relationship with reliable companies.

5.6 Escrow Services Fraud

Some companies ask a victim to pay the required money to a third – party, which collects, holds and disburses money according to the instructions of the Buyer and the Seller. Escrow is preferable on auction sites, automobiles, motorcycles, jewelry, domain names, computer items...etc. the procedure of escrow services include the agreement of the Buyer and Seller on related terms, the submission of the payment by Buyer Escrow.com, the shipment of merchandise by the Seller, acceptance of the merchandise by the Buyer, the payment to the Seller carried out by Escrow.com. This system is usually beneficial for the Seller and the Buyer, but there are of course some people with bad intentions, who try to benefit from this system.

The fraud incidents are related to the payment by the victim unknowingly to the perpetrator. The victim may be unaware about the accuracy of the escrow site and he may not receive anything in return for his payment. These cases can be evaluated from two different perspectives. These are:

- Buyer as victim: The Seller may ask the Buyer to pay money to the escrow site, which he recommends. If the Buyer does not receive his merchandise, he can be evaluated as a victim of escrow services.
- Seller as victim: The Buyer may recommend the Seller an escrow site by informing that he will feel himself comfortable via this site. The fraudulent escrow site may inform the Seller that they received the involved amount. The Seller may think that the involved money is secure and he may send the goods. The Buyer receives the goods, but the Seller may never be able to receive his money.

Escrow.com is a reliable site about escrow services. If the perpetrator refuses to use these kinds of sites offered by the victim, there may of course be a risk of a fraud incidence. Both parties have to agree on using a reliable escrow service in order to protect their own rights. A good escrow service procedure is stated below:

- 1) The escrow service confirms the fund of the Buyer before the shipment of the goods.
- 2) The service verifies the shipment of the goods and they make sure that the Buyer receives the involved goods.
- 3) If there is a fraudulent case, the service has to defend the rights of both parties.

5.7 Identity Theft

Identity theft is a fraud incidence that is carried out by using the personal information related to another individual. The victim of such cases may suffer from various consequences, because he may be unaware of someone else, who is pretending to be him by using his identity information.

There are also some kinds of identity frauds. These are:

Financial identity theft: At this point the perpetrator uses the personal information related to the victim in order to receive some goods and services.

Criminal identity theft: The perpetrator uses the personal information of the victim in order to prove that he is not involved in any types of crime. At this case the victim is blamed of a crime because of his personal information used by the perpetrator.

Identity cloning: The perpetrator prepares a copy of his victim's identity so that he can use it during his daily life.

Business/Commercial identity theft: The perpetrator may use the name of another business brand in order to receive credit.

The 2006 Identity Theft Survey Report of the Federal Commission of Trade (FTC) demonstrates how the existing accounts of a victim can be misused. The existing accounts of a person, such as credit cards, checking/ saving, telephone services, internet payment accounts...etc. can be used by a perpetrator and this is analyzed under the name of fraud. According to the figure below, we can say that the most common type of identity frauds are related to the credit cards of a person.

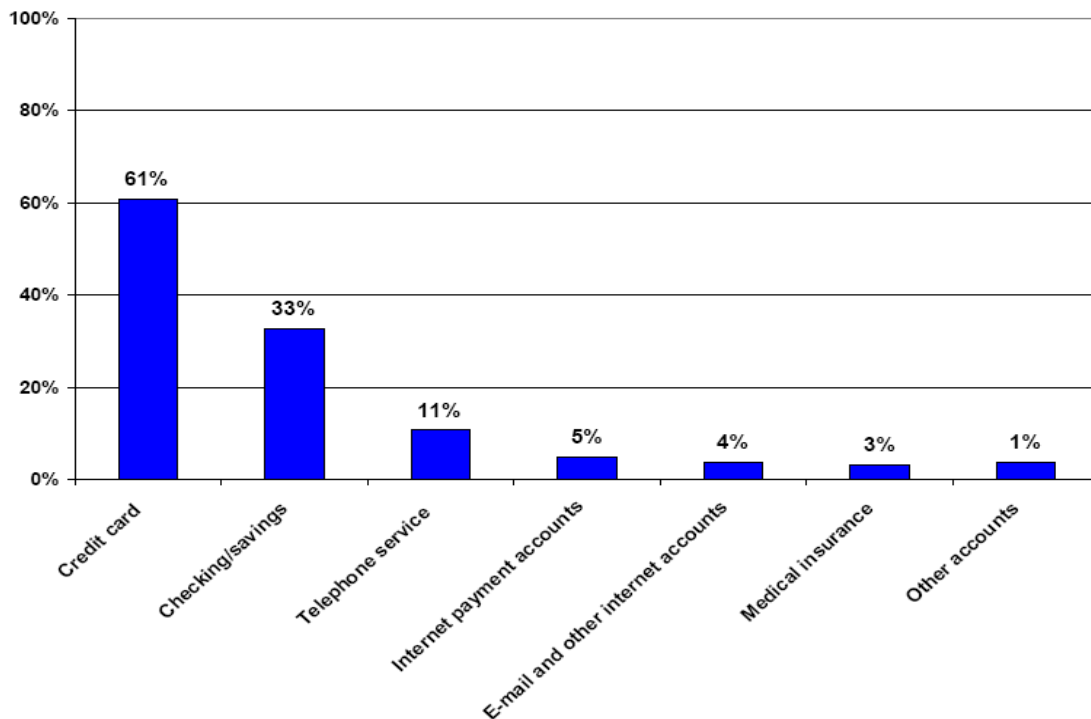


Figure 11 - Different Types of Accounting Frauds Related to the Identity Frauds¹⁴

¹⁴ 2006 Identity Theft Survey Report of FTC

Some perpetrators do not only steal the personal information of their victims, but they also open new accounts via those stolen information. The survey of FTC in 2006 revealed that seventeen per cent of the victims informed that the perpetrator benefited from their personal information to open at least one new account. (see figure 12)

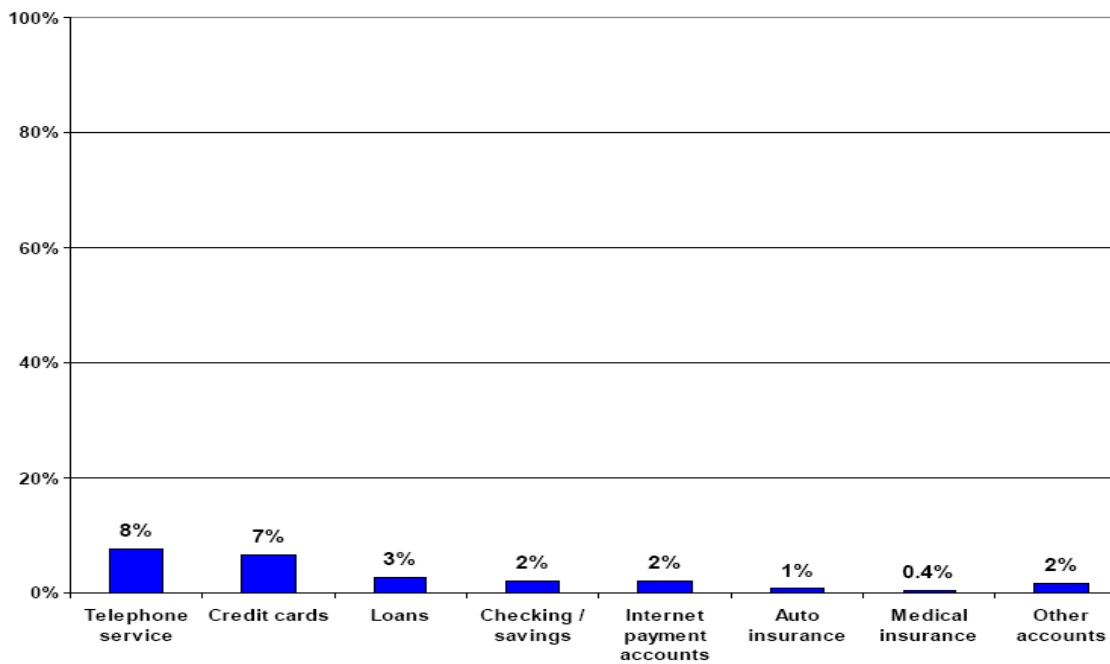


Figure 12 - The New Accounts Opened By The Perpetrators In The Name Of The Victims¹⁵

Some countries have been trying to avoid such kinds of fraud incidents with the help of legal responds. Some of these legal responses are:

¹⁵ 2006 Identity Theft Survey Report of FTC

AUSTRALIA:

135.1 General dishonesty

(3) A person is guilty of an offence if: a) the person does anything with the intention of dishonestly **causing a loss to another person**; and b) the other person is a Commonwealth entity. Penalty: **Imprisonment for 5 years**.¹⁶

CANADA:

Every one who fraudulently personates any person, living or dead, (a) with **intent to gain advantage** for himself or another person, (b) with **intent to obtain any property** or an interest in any property, or (c) with **intent to cause disadvantage** to the person whom he personates or another person, is guilty of an indictable offence and liable to imprisonment for a term **not exceeding ten years** or an offence punishable on summary conviction¹⁷.

HONG KONG:

(1)

If any person by any deceit (whether or not the deceit is the sole or main inducement) and with **intent to defraud** induces another person to commit an act or make an omission, which results either-

(a) In **benefit to any person** other than the second-mentioned person; or (b) in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person, the first-

¹⁶ Criminal Code Amendment Act 2000 (Fraud, Theft, Bribery and Related Offences Part)

¹⁷ Criminal Code of Canada, Section 403

mentioned person commits the offense of fraud and is liable on conviction upon indictment to **imprisonment for 14 years.**¹⁸

Data Protection Act includes the protection of identity information too and it has been widely used in The United Kingdom.

5.8 Investment Fraud

The internet is a significant tool for the investors who look for reliable resources, but it is also a significant tool for the fraud perpetrators. Therefore, the investor should be quite careful when investing via the internet. Investment fraud incidents include commodities, futures, foreign currency, gemstones, real estate, bills and invoices, resources...etc.

The online bulletin boards have become very common around the world during the recent years. Thanks to these boards the companies catch the opportunity to share some of their information with other companies and so a relationship between the involved companies may come out. Generally, these boards may be beneficial, but the involved parties should never forget that it is nearly impossible to know with whom they are dealing.

If you want to make an investment wisely and in a secure way, there are some basic points which you have to take into consideration. At first you have to analyze the size of the company. If the company is small and unknown, you have to be more careful. Secondly, you may demand the financial statements of the involved company in order to analyze them. Then you may call the customers or the suppliers of the company so as to get some

¹⁸ Hong Kong Laws Chapter 210 Theft Ordinance, section 16A Fraud

information and you should compare the responses of the customers and the suppliers with the information you got from the company. You should pay attention that the information is consistent. At last you may search, whether the company made money for the investors before.

5.9 Lottery Frauds

Earning money is very difficult nowadays and all people try to earn the highest amount of money by working the least. Therefore, lotteries may be a chance for some of those people, but they have to be careful because there are also lottery fraudsters. These kind of fraudsters send at first an e – mail to the victim and this mail informs the victim about a lottery, which he may have won. The lottery fraudsters pretend to be organizations under governmental or international control. As a result of this they prefer names such as “Spanish National Lottery, Sweepstake Lottery Company”.

They send another mail to the victim to inform that they have to get in contact as soon as possible and they emphasize that if the victim does not get in contact with them, the involved amount would return to the lottery association or to the related governmental association. If the victim gets in contact, he has to share his personal information via a copy of his identity or some other kinds of documents like that. As a result of this process, the fraud perpetrators receive the personal information of their victims.

The authorities advise the potential victims not to answer such mails and not to send their personal information to anyone they do not know. Nevertheless, if you have already been in contact with such fraudsters, it will be beneficial to save the send and received messages

and save all the documents related to this incidence. At last you have to call the local police and they may deal with this issue. The most important advice of the authorities is that the victims should be very selective, if they are to send money through the internet to someone, whom they do not actually know.

5.10 Nigerian Letter or “419”

“Lagos, Nigeria.

Attention: The President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce and Industry, I have the privilege to request your assistance to transfer the sum of \$47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank. We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

- (a) Your banker's name, telephone, account and fax numbers.
- (b) Your private telephone and fax numbers —for confidentiality and easy communication.
- (c) Your letter-headed paper stamped and signed.

Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

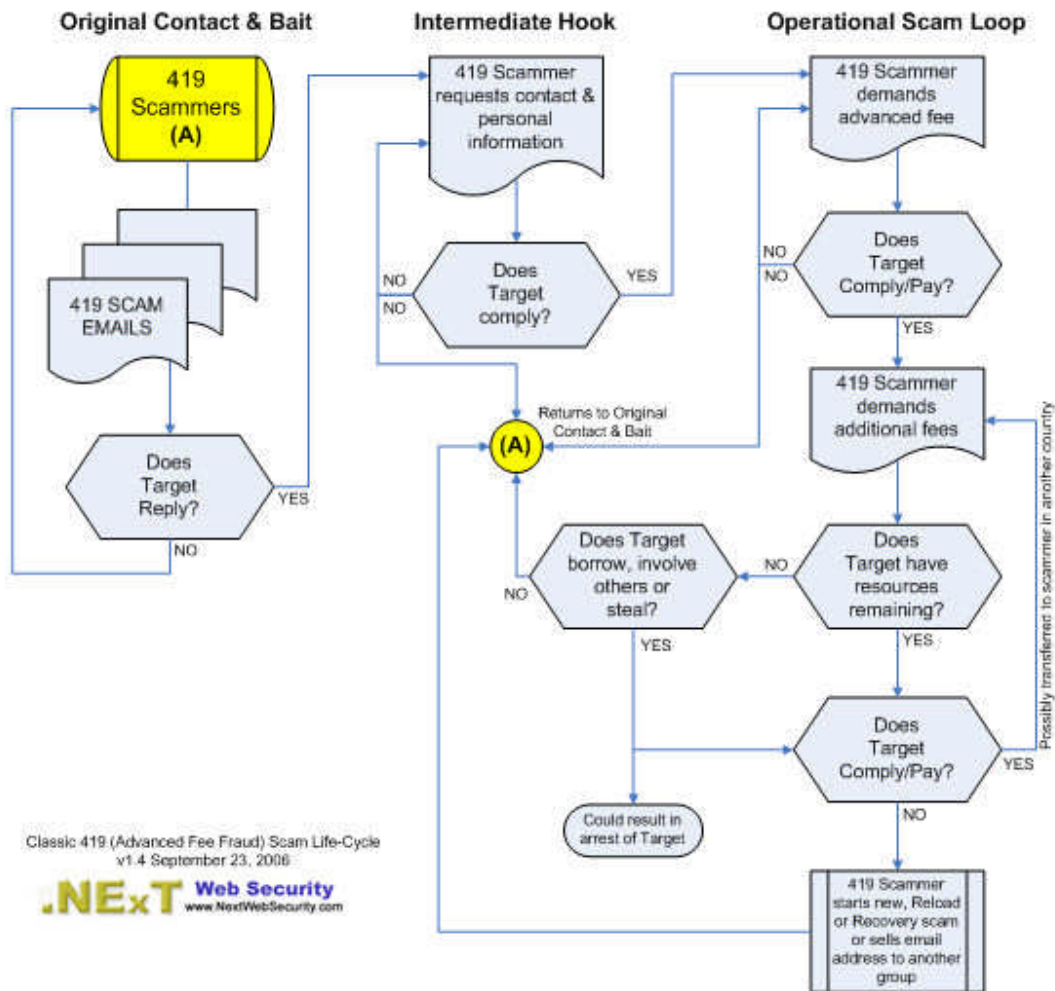
Best regards

*Howgul Abul Arhu*¹⁹

A sample of a Nigerian Letter is given above and we can say that these kinds of fraud incidents aim people of middle class and middle age, who would not be deceived by lottery scams. These kinds of fraud incidents are commonly known as “419”. We can say that 419 is a sub – division of the Advance Fee Fraud incidents.

¹⁹ <http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm>

Classic 419 (Advanced Fee Fraud) Scam Life-Cycle



Classic 419 (Advanced Fee Fraud) Scam Life-Cycle
v1.4 September 23, 2006



Figure 13 – The Cycle of the Nigerian Letter or “419”²⁰

The fraud incidents, which are the result of the violation of Section 419 of the Nigerian Criminal Code, are called the Nigerian Letter. The potential victim receives letters, e – mails or posts and they are asked to pay some advance fees. The victims are asked to pay such fees as a result of various reasons and the perpetrators are thought to be Nigerian. (See Figure 13).

²⁰ <http://www.nextwebsecurity.com/419LifeCycle.asp>

6 – TRANSPARENCY AND FRAUD INCIDENTS

Fraud incidents are not surprising results for companies, which are not transparent. The Transparency International (TI) Study found out that transparency is still a nightmare for the Czech economy. It costs the government nearly \$ 1.3 billion. A similar situation is valid for Turkey, because Turkey takes place as one of the 4 dirtiest countries among 30 countries according to the Transparency International Bribe Giver Index. Namely, we can say that the transparency situation is very bad in Turkey. Some conclusions of the Transparency International Bribe Giver Index are stated below:

- The most clean 5 countries and their scores over 10 are;

Switzerland (7, 81)

Sweden (7, 62)

Australia (7, 59)

Austria (7, 50)

Canada (7, 46)

- The dirtiest 5 countries and their scores over 10 are;

India (4, 62)

China (4, 94)

Russia (5, 16)

Turkey (5, 23)

Taiwan (5, 41)²¹

The study above demonstrates us that there is a lack of transparency within the Turkish companies. Especially, bribery is a vital problem for the Turkish companies that work together with international companies. We can say that the rich businessmen and the poor governors are the main reasons of these shaming tables. As a conclusion it can be said that fraud incidents have been a part of life for Turkey concerning the internal and external relationships with the companies.

Bribery and corruption compose a hindrance against transparency. Some people think that they can solve their problems when money changes hands, but they ignore the bad sides of such a trend. As we see bribery and corruption has been one of the most common types of economic crime threats within the emerging market and according to a study of Pwc (2007), outside Western Europe and North America, 20% to 30% of respondents emphasized that they had to pay bribe so as to solve their company problems and to regulate their company relationships. As it is seen in the figure 14 below, bribery, which is a type of fraud, cases are more seen in emerging 7 (E7) countries. From this study, we can analyse that Turkey is one of the countries, in which bribery and corruption is at an increase. Namely, this result is associated with the transparency level of a country and we cannot say that Turkey is one of the most transparent countries among the world due to the high trend of corruption and bribery.

²¹ <http://www.saydamlik.org/turkce.html>

Percentage of companies asked to pay a bribe

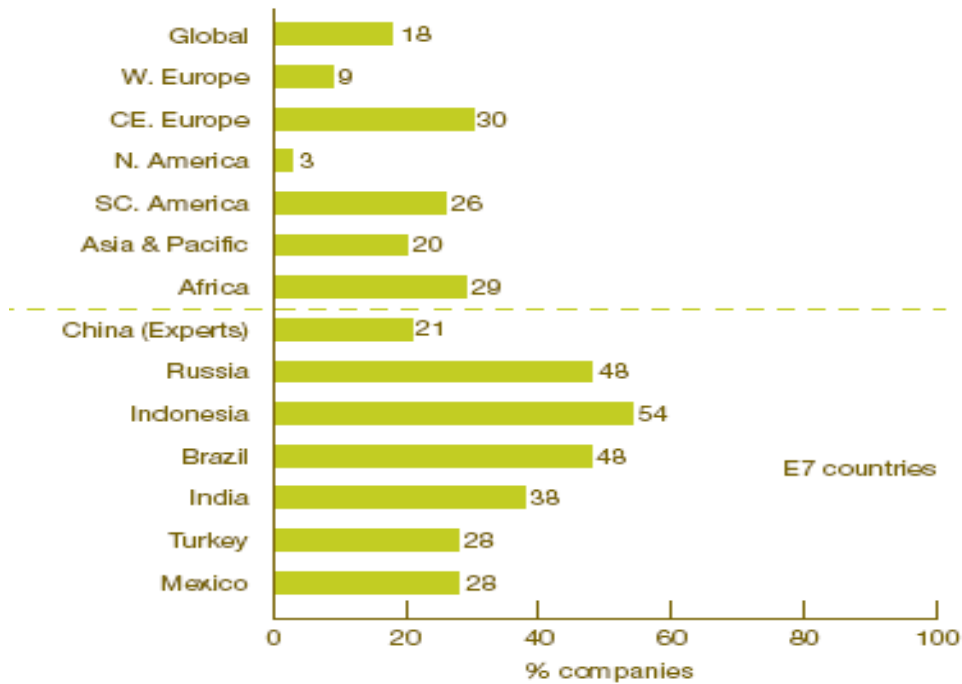


Figure 14 – Percentage of Companies Asked to Pay Bribe.²²

There are many key points about transparency, from which we may understand whether an organization is transparent or not. The Global Corruption Barometer 2007 revealed some of these key points as:

- The poor in developing countries are the most affected people by corruption. These people, who are penalized by corruption, do not have a hope for less corruption in the future.

²² The Global Economic Crime Survey in 2007 by PwC.

- 10% of the people around the world had to pay bribe in the recent years and the reported bribery incidents have increased in some regions such as Asia-Pacific and South East Europe.
- Bribery is widespread especially when people have to have contact with police, judiciary, and registry and permit services.
- Generally, there is a common belief among the public concerning that the political parties, parliament, the police and the judicial/legal systems are the most non – transparent entities in their societies.
- According to an interview, which was carried out about four years ago, half of the respondents pointed out that they expect an increase related to the corruption incidents in their countries within the next three years.
- Again according to the same interview, half of those respondents thought that the governmental measures related to the prevention of fraud and bribery incidents were ineffective.

TI points out that Albania, Cameroon, Macedonia, Kosovo, Nigeria, Pakistan, Philippines, Romania and Senegal are among the most affected countries by bribery. The new report of TI examined 11 sectors and as a result of this examination it has been found out that people have to combat bribery, when they have to solve a problem through the police forces. Namely, one in every four citizens around the world who had contact with the police forces was asked to pay a bribe amount. Bribery has also been a dangerous problem for the judiciary, registry and permit services, education and medical services as well as electricity providers.

Table 5 – The Bribery Index of the Countries in 2006 Published by the Transparency International

Degree	Country	Number of Respondents	Average Degree	Standard Deviation	Failure Margin
1	Sweden	1744	7,81	2,65	0.12
2	Switzerland	1451	7,62	2,66	0.14
3	Australia	1447	7,59	2,62	0.14
4	Austria	1560	7,50	2,60	0.13
5	Canada	1870	7,46	2,70	0.12
6	England	3442	7,39	2,67	0.09
7	Germany	3873	7,34	2,74	0.09
8	Holland	1821	7,28	2,69	0.12
9	Belgium	1329	7,22	2,70	0.15
10	USD	5401	7,22	2,77	0.07
11	Japan	3279	7,10	2,87	0.10
12	Singapore	1297	6,78	3,04	0.17
13	Spain	2111	6,63	2,73	0.12
14	United Arab Emirates	1928	6,62	3,09	0.14
15	France	3085	6,50	3,00	0.11
16	Portuguese	973	6,47	2,79	0.18
17	Mexico	1765	6,45	3,17	0.15
18	Hong Kong	1556	6,01	3,13	0.16
19	Israel	1482	6,01	3,14	0.16
20	Italy	2525	5,94	2,99	0.12
21	South Korea	1930	5,83	2,93	0.13
22	Saudi Arabia	1302	5,75	3,17	0.17
23	Brazil	1317	5,65	3,02	0.16
24	South Africa	1488	5,61	3,11	0.16
25	Malaysia	1319	5,59	3,07	0.17
26	Taiwan	1731	5,41	3,08	0.15
27	Turkey	1755	5,23	3,14	0.15
28	Russia	2203	5,16	3,34	0.14
29	China	3448	4,94	3,29	0.11
30	India	2145	4,62	3,28	0.14

Also, when we examine the Corruption Perception Index 2006, prepared by Transparency International, it is obvious that Turkey again comes up in low scores which means approximate highly corrupt.

Table 6 – The Corruption Perception Index 2006

Country	2006 CPI Score	Surveys used	Confidence range
1 Finland	9,06	7	9.4 - 9.7
2 Iceland	9,06	6	9.5 - 9.7
3 New Zealand	9,06	7	9.4 - 9.6
4 Denmark	9,05	7	9.4 - 9.6
5 Singapore	9,04	9	9.2 - 9.5
6 Sweden	9,02	7	9.0 - 9.3
7 Switzerland	9,01	7	8.9 - 9.2
8 Norway	8,08	7	8.4 - 9.1
9 Australia	8,07	8	8.3 - 9.0
10 Netherlands	8,07	7	8.3 - 9.0
11 Austria	8,06	7	8.2 - 8.9
12 Luxembourg	8,06	6	8.1 - 9.0
13 United Kingdom	8,06	7	8.2 - 8.9
14 Canada	8,05	7	8.0 - 8.9
15 Hong Kong	8,03	9	7.7 - 8.8
16 Germany	8,00	7	7.8 - 8.4
17 Japan	7,06	9	7.0 - 8.1
18 France	7,04	7	6.7 - 7.8
19 Ireland	7,04	7	6.7 - 7.9
20 Belgium	7,03	7	6.6 - 7.9
21 Chile	7,03	7	6.6 - 7.6
22 USA	7,03	8	6.6 - 7.8
23 Spain	6,08	7	6.3 - 7.2
24 Barbados	6,07	4	6.0 - 7.2
25 Estonia	6,07	8	6.1 - 7.4
26 Macao	6,06	3	5.4 - 7.1
27 Portugal	6,06	7	5.9 - 7.3
28 Malta	6,04	4	5.4 - 7.3

29	Slovenia	6,04	8	5.7 - 7.0
30	Uruguay	6,04	5	5.9 - 7.0
31	United Arab Emirates	6,02	5	5.6 - 6.9
32	Bhutan	6,00	3	4.1 - 7.3
33	Qatar	6,00	5	5.6 - 6.5
34	Israel	5,09	7	5.2 - 6.5
35	Taiwan	5,09	9	5.6 - 6.2
36	Bahrain	5,07	5	5.3 - 6.2
37	Botswana	5,06	6	4.8 - 6.6
38	Cyprus	5,06	4	5.2 - 5.9
39	Oman	5,04	3	4.1 - 6.2
40	Jordan	5,03	7	4.5 - 5.7
41	Hungary	5,02	8	5.0 - 5.4
42	Mauritius	5,01	5	4.1 - 6.3
43	South Korea	5,01	9	4.7 - 5.5
44	Malaysia	5,00	9	4.5 - 5.5
45	Italy	4,09	7	4.4 - 5.4
46	Czech Republic	4,08	8	4.4 - 5.2
47	Kuwait	4,08	5	4.0 - 5.4
48	Lithuania	4,08	6	4.2 - 5.6
49	Latvia	4,07	6	4.0 - 5.5
50	Slovakia	4,07	8	4.3 - 5.2
51	South Africa	4,06	8	4.1 - 5.1
52	Tunisia	4,06	5	3.9 - 5.6
53	Dominica	4,05	3	3.5 - 5.3
54	Greece	4,04	7	3.9 - 5.0
55	Costa Rica	4,01	5	3.3 - 4.8
56	Namibia	4,01	6	3.6 - 4.9
57	Bulgaria	4,00	7	3.4 - 4.8
58	El Salvador	4,00	5	3.2 - 4.8
59	Colombia	3,09	7	3.5 - 4.7
60	Turkey	3,08	7	3.3 - 4.2
61	Jamaica	3,07	5	3.4 - 4.0
62	Poland	3,07	8	3.2 - 4.4
63	Lebanon	3,06	3	3.2 - 3.8
64	Seychelles	3,06	3	3.2 - 3.8
65	Thailand	3,06	9	3.2 - 3.9
66	Belize	3,05	3	2.3 - 4.0
67	Cuba	3,05	3	1.8 - 4.7

68	Grenada	3,05	3	2.3 - 4.1
69	Croatia	3,04	7	3.1 - 3.7
70	Brazil	3,03	7	3.1 - 3.6
71	China	3,03	9	3.0 - 3.6
72	Egypt	3,03	6	3.0 - 3.7
73	Ghana	3,03	6	3.0 - 3.6
74	India	3,03	10	3.1 - 3.6
75	Mexico	3,03	7	3.1 - 3.4
76	Peru	3,03	5	2.8 - 3.8
77	Saudi Arabia	3,03	3	2.2 - 3.7
78	Senegal	3,03	5	2.8 - 3.7
79	Burkina Faso	3,02	5	2.8 - 3.6
80	Lesotho	3,02	5	2.9 - 3.6
81	Moldova	3,02	7	2.7 - 3.8
82	Morocco	3,02	6	2.8 - 3.5
83	Trinidad and Tobago	3,02	5	2.8 - 3.6
84	Algeria	3,01	5	2.7 - 3.6
85	Madagascar	3,01	5	2.3 - 3.7
86	Mauritania	3,01	4	2.1 - 3.7
87	Panama	3,01	5	2.8 - 3.3
88	Romania	3,01	8	3.0 - 3.2
89	Sri Lanka	3,01	6	2.7 - 3.5
90	Gabon	3,00	4	2.4 - 3.3
91	Serbia	3,00	7	2.7 - 3.3
92	Suriname	3,00	4	2.7 - 3.3
93	Argentina	2,09	7	2.7 - 3.2
94	Armenia	2,09	6	2.7 - 3.0
95	Bosnia and Herzegovina	2,09	6	2.7 - 3.1
96	Eritrea	2,09	3	2.2 - 3.5
97	Syria	2,09	3	2.3 - 3.2
98	Tanzania	2,09	7	2.7 - 3.1
99	Dominican Republic	2,08	5	2.4 - 3.2
100	Georgia	2,08	6	2.5 - 3.0
101	Mali	2,08	7	2.5 - 3.3
102	Mongolia	2,08	5	2.3 - 3.4
103	Mozambique	2,08	7	2.5 - 3.0
104	Ukraine	2,08	6	2.5 - 3.0
105	Bolivia	2,07	6	2.4 - 3.0
106	Iran	2,07	3	2.3 - 3.1

107	Libya	2,07	3	2.4 - 3.2
108	Macedonia	2,07	6	2.6 - 2.9
109	Malawi	2,07	7	2.5 - 3.0
110	Uganda	2,07	7	2.4 - 3.0
111	Albania	2,06	5	2.4 - 2.7
112	Guatemala	2,06	5	2.3 - 3.0
113	Kazakhstan	2,06	6	2.3 - 2.8
114	Laos	2,06	4	2.0 - 3.1
115	Nicaragua	2,06	6	2.4 - 2.9
116	Paraguay	2,06	5	2.2 - 3.3
117	Timor-Leste	2,06	3	2.3 - 3.0
118	Viet Nam	2,06	8	2.4 - 2.9
119	Yemen	2,06	4	2.4 - 2.7
120	Zambia	2,06	6	2.1 - 3.0
121	Benin	2,05	6	2.1 - 2.9
122	Gambia	2,05	6	2.3 - 2.8
123	Guyana	2,05	5	2.2 - 2.6
124	Honduras	2,05	6	2.4 - 2.7
125	Nepal	2,05	5	2.3 - 2.9
126	Philippines	2,05	9	2.3 - 2.8
127	Russia	2,05	8	2.3 - 2.7
128	Rwanda	2,05	3	2.3 - 2.6
129	Swaziland	2,05	3	2.2 - 2.7
130	Azerbaijan	2,04	7	2.2 - 2.6
131	Burundi	2,04	5	2.2 - 2.6
132	Central African Republic	2,04	3	2.2 - 2.5
133	Ethiopia	2,04	7	2.2 - 2.6
134	Indonesia	2,04	10	2.2 - 2.6
135	Papua New Guinea	2,04	4	2.3 - 2.6
136	Togo	2,04	3	1.9 - 2.6
137	Zimbabwe	2,04	7	2.0 - 2.8
138	Cameroon	2,03	7	2.1 - 2.5
139	Ecuador	2,03	5	2.2 - 2.5
140	Niger	2,03	5	2.1 - 2.6
141	Venezuela	2,03	7	2.2 - 2.4
142	Angola	2,02	5	1.9 - 2.4
143	Congo, Republic	2,02	4	2.2 - 2.3
144	Kenya	2,02	7	2.0 - 2.4
145	Kyrgyzstan	2,02	6	2.0 - 2.6

146	Nigeria	2,02	7	2.0 - 2.3
147	Pakistan	2,02	6	2.0 - 2.4
148	Sierra Leone	2,02	3	2.2 - 2.3
149	Tajikistan	2,02	6	2.0 - 2.4
150	Turkmenistan	2,02	4	1.9 - 2.5
151	Belarus	2,01	4	1.9 - 2.2
152	Cambodia	2,01	6	1.9 - 2.4
153	Côte d'Ivoire	2,01	4	2.0 - 2.2
154	Equatorial Guinea	2,01	3	1.7 - 2.2
155	Uzbekistan	2,01	5	1.8 - 2.2
156	Bangladesh	2,00	6	1.7 - 2.2
157	Chad	2,00	6	1.8 - 2.3
158	Congo, Democratic Republic	2,00	4	1.8 - 2.2
159	Sudan	2,00	4	1.8 - 2.2
160	Guinea	1,09	3	1.7 - 2.1
161	Iraq	1,09	3	1.6 - 2.1
162	Myanmar	1,09	3	1.8 - 2.3
163	Haiti	1,08	3	1.7 - 1.8

Explanatory notes*

* CPI Score relates to perceptions of the degree of corruption as seen by business people and country analysts, and ranges between 10 (highly clean) and 0 (highly corrupt).

** Confidence range provides a range of possible values of the CPI score. This reflects how a country's score may vary, depending on measurement precision. Nominally, with 5 percent probability the score is above this range and with another 5 percent it is below. However, particularly when only few sources are available, an unbiased estimate of the mean coverage probability is lower than the nominal value of 90%.

*** Surveys used refer to the number of surveys that assessed a country's performance. 12 surveys and expert assessments were used and at least 3 were required for a country to be included in the CPI.²³

As it is seen in the tables above, there is a connection between the development level of the countries and the existing of fraud risk. Hereby there is a connection between the development level of the countries and transparency level of the countries. The transparency level of a country is related with its development level. If the country is developed, we can say that the transparency level in this country is high or vice versa. There are per capita GDP amounts of the countries through a descending list below and they are compared with the CPI rates.

Table 7 - The CPI Rates and GDP Per Capita Power Rates

#	Country	CPI	GDP per Capita	GDP Power Rate
1	Luxembourg	8.4	87,400	100.00
2	Ireland	7.5	47,169	53.97
3	Norway	8.7	47,098	53.89
4	United States	7.8	44,765	51.22
5	Iceland	9.2	41,680	47.69
6	Hong Kong SAR	8.3	41,614	47.61
7	Switzerland	9.0	40,590	46.44
8	Qatar	6.0	38,672	44.25
9	Austria	8.1	38,474	44.02
10	Denmark	9.4	38,438	43.98
11	Netherlands	9.0	38,252	43.77
12	Finland	9.4	37,957	43.43
13	United Kingdom	8.4	37,328	42.71

²³ http://www.transparency.org/layout/set/print/policy_research/surveys_indices/cpi/2006

14	Canada	8.7	36,984	42.32
15	Sweden	9.3	36,687	41.98
16	Belgium	7.1	36,355	41.60
17	Singapore	9.3	36,286	41.52
18	United Arab Emirates	5.7	35,516	40.64
19	Greece	4.6	35,167	40.24
20	Australia	8.6	34,943	39.98
21	Japan	7.5	34,024	38.93
22	Israel	6.1	33,299	38.10
23	France	7.3	33,078	37.85
24	Germany	7.8	33,023	37.78
25	Taiwan Province of China	5.7	32,490	37.17
26	Italy	5.2	32,319	36.98
27	Cyprus	5.3	31,522	36.07
28	Spain	6.7	29,148	33.35
29	New Zealand	9.4	26,994	30.89
30	Slovenia	6.6	26,576	30.41
31	Bahrain	5.0	25,851	29.58
32	Korea	5.1	25,840	29.57
33	Czech Republic	5.2	25,346	29.00
34	Portugal	6.5	23,867	27.31
35	Malta	5.8	23,454	26.84
36	Estonia	6.5	21,860	25.01
37	Seychelles	4.5	21,535	24.64
38	Kuwait	4.3	21,418	24.51
39	Hungary	5.3	21,040	24.07
40	Barbados	6.9	20,532	23.49
41	Equatorial Guinea	1.9	19,946	22.82
42	Oman	4.7	19,879	22.74
43	Trinidad and Tobago	3.4	18,975	21.71
44	Liberia	2.1	18,568	21.24
45	Latvia	4.8	18,005	20.60
46	Lithuania	4.8	17,749	20.31
47	Argentina	2.9	17,559	20.09
48	Saudi Arabia	3.4	17,196	19.67
49	Botswana	5.4	17,034	19.49
50	Poland	4.2	16,599	18.99
51	Croatia	4.1	15,733	18.00
52	Mauritius	4.7	14,153	16.19
53	Libya	2.5	14,108	16.14
54	South Africa	5.1	13,845	15.84
55	Chile	7.0	13,745	15.73
56	Russia	2.3	13,432	15.37
57	Uruguay	6.7	12,917	14.78
58	Malaysia	5.1	12,754	14.59
59	Costa Rica	5.0	12,683	14.51

60	Mexico	3.5	11,880	13.59
61	Romania	3.7	11,079	12.68
62	Bulgaria	4.1	10,973	12.55
63	Kazakhstan	2.1	10,658	12.19
64	Brazil	3.5	10,637	12.17
65	Dominican Republic	3.0	10,241	11.72
66	Belarus	2.1	10,167	11.63
67	Bosnia and Herzegovina	3.3	9,964	11.40
68	Turkey	4.1	9,816	11.23
69	Thailand	3.3	9,714	11.12
70	Tunisia	4.2	9,630	11.02
71	Grenada	3.4	9,623	11.01
72	Maldives	3.3	9,531	10.91
73	Turkmenistan	2.0	9,483	10.85
74	Panama	3.2	9,395	10.75
75	Namibia	4.5	9,142	10.46
76	Iran, Islamic Republic of	2.5	9,127	10.44
77	Colombia	3.8	8,891	10.17
78	China	3.5	8,788	10.06
79	Ukraine	2.7	8,624	9.87
80	Azerbaijan	2.1	8,521	9.75
	Macedonia, Former Yugoslav			
81	Republic of	3.3	8,251	9.44
82	Algeria	3	8,203	9.39
83	Tonga	1.7	8,141	9.31
84	Venezuela	2	8,125	9.30
85	Belize	3	8,108	9.28
86	Cape Verde	4.9	7,904	9.04
87	Gabon	3.3	7,717	8.83
88	Peru	3.5	7,410	8.48
89	Serbia	3.4	7,265	8.31
90	Suriname	3.5	6,995	8.00
91	Samoa	4.5	6,738	7.71
92	Albania	2.9	6,197	7.09
93	Dominica	5.6	6,180	7.07
94	Morocco	3.5	6,003	6.87
95	Lebanon	3.0	5,965	6.82
96	Jordan	4.7	5,964	6.82
97	El Salvador	4.0	5,885	6.73
98	Sri Lanka	3.2	5,839	6.68
99	Armenia	3.0	5,769	6.60
100	Philippines	2.5	5,738	6.57
101	Paraguay	2.4	5,638	6.45
102	Bhutan	5.0	5,477	6.27
103	Swaziland	3.3	5,466	6.25
104	Guyana	2.6	5,404	6.18

105	Egypt	2.9	5,272	6.03
106	Ecuador	2.1	5,021	5.75
107	Indonesia	2.3	4,684	5.36
108	Jamaica	3.3	4,654	5.32
109	Guatemala	2.8	4,547	5.20
110	Angola	2.2	4,346	4.97
111	India	3.5	4,183	4.79
112	Georgia	3.4	4,176	4.78
113	Nicaragua	2.6	4,055	4.64
114	Cambodia	2.0	3,743	4.28
115	Vanuatu	3.1	3,689	4.22
116	Honduras	2.5	3,378	3.86
117	Mongolia	3.0	3,181	3.64
118	Sudan	1.8	3,093	3.54
119	Moldova	2.8	3,090	3.54
120	Bolivia	2.9	3,062	3.50
121	Ghana	3.7	2,963	3.39
122	Pakistan	2.4	2,943	3.37
123	Papua New Guinea	2.0	2,908	3.33
124	Djibouti	2.9	2,665	3.05
125	Kiribati	3.3	2,567	2.94
126	Uzbekistan	1.7	2,541	2.91
127	Mauritania	2.6	2,530	2.90
128	Guinea	1.9	2,438	2.79
129	Myanmar	1.4	2,432	2.78
130	Gambia, The	2.3	2,402	2.75
131	Zimbabwe	2.1	2,395	2.74
132	Lesotho	3.3	2,379	2.72
133	Kyrgyz Republic	2.1	2,315	2.65
134	Bangladesh	2.0	2,270	2.60
135	Cameroon	2.4	2,266	2.59
136	Solomon Islands	2.8	2,216	2.54
137	Senegal	3.6	2,086	2.39
138	Comoros	2.6	2,078	2.38
139	Nepal	2.5	2,008	2.30
140	Haiti	1.6	1,914	2.19
141	Chad	1.8	1,777	2.03
142	Uganda	2.8	1,728	1.98
143	Côte d'Ivoire	2.1	1,726	1.97
144	Tajikistan	2.1	1,637	1.87
145	Mozambique	2.8	1,603	1.83
146	Togo	2.3	1,550	1.77
147	Afghanistan, Rep. of.	1.8	1,522	1.74
148	Rwanda	2.8	1,520	1.74
149	Burkina Faso	2.9	1,494	1.71
150	Congo, Republic of	2.1	1,492	1.71

151	Kenya	2.1	1,456	1.67
152	Benin	2.7	1,452	1.66
153	Mali	2.7	1,379	1.58
154	Nigeria	2.2	1,281	1.47
155	Central African Republic	2.0	1,266	1.45
156	Ethiopia	2.4	1,239	1.42
157	Zambia	2.6	1,155	1.32
158	Yemen, Republic of	2.5	1,015	1.16
159	Madagascar	3.2	1,014	1.16
160	Niger	2.6	1,012	1.16
161	Eritrea	2.8	1,011	1.16
162	Sierra Leone	2.1	959	1.10
163	Congo, Democratic Republic of	1.9	893	1.02
164	Tanzania	3.2	869	0.99
165	Guinea-Bissau	2.2	780	0.89
166	Malawi	2.7	750	0.86
167	Burundi	2.5	705	0.81

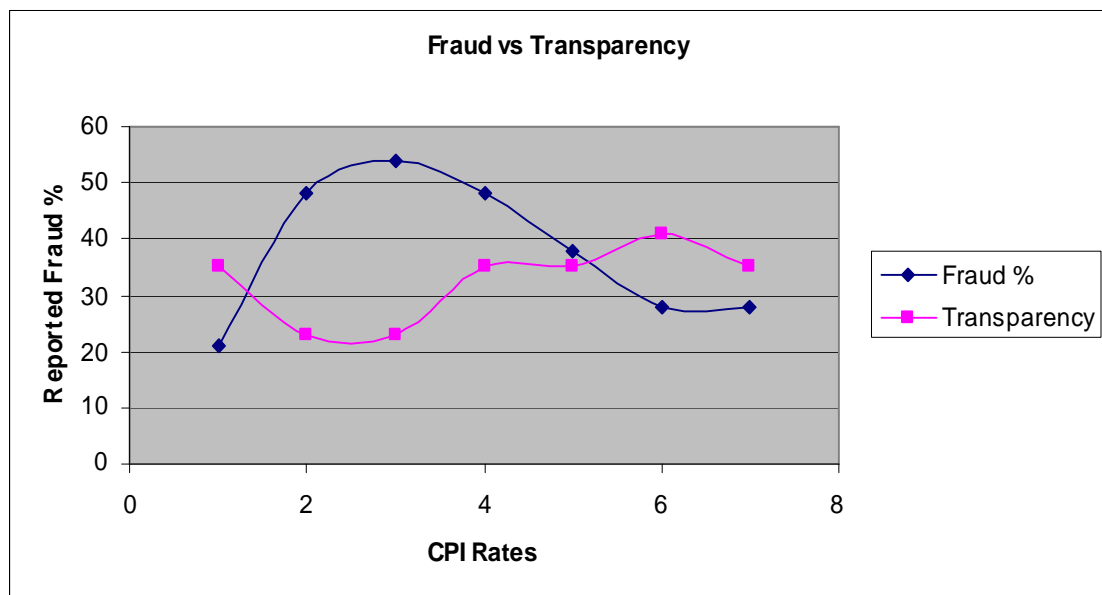


Figure 15 – Reported Fraud Percentages versus CPI Rates of E7 Countries

In order to show more clear, we multiplied the CPI rates by 10 and compared with the reporting percentages of fraud in the emerging countries (see figure 15) in the graph above.

As it is seen in the graph, there is a relation between the transparency level of the emerging countries and the fraud existence.

Since we have only the emerging 7 countries' fraud existence percentages, we expanded the analysis. We degraded the per capita over 100 points and sort them by descending and compared with the CPI rates in the table 7 which means if the GDP per Capita is high (that means more emerging country), CPI rate of the company is also high. (See graph)

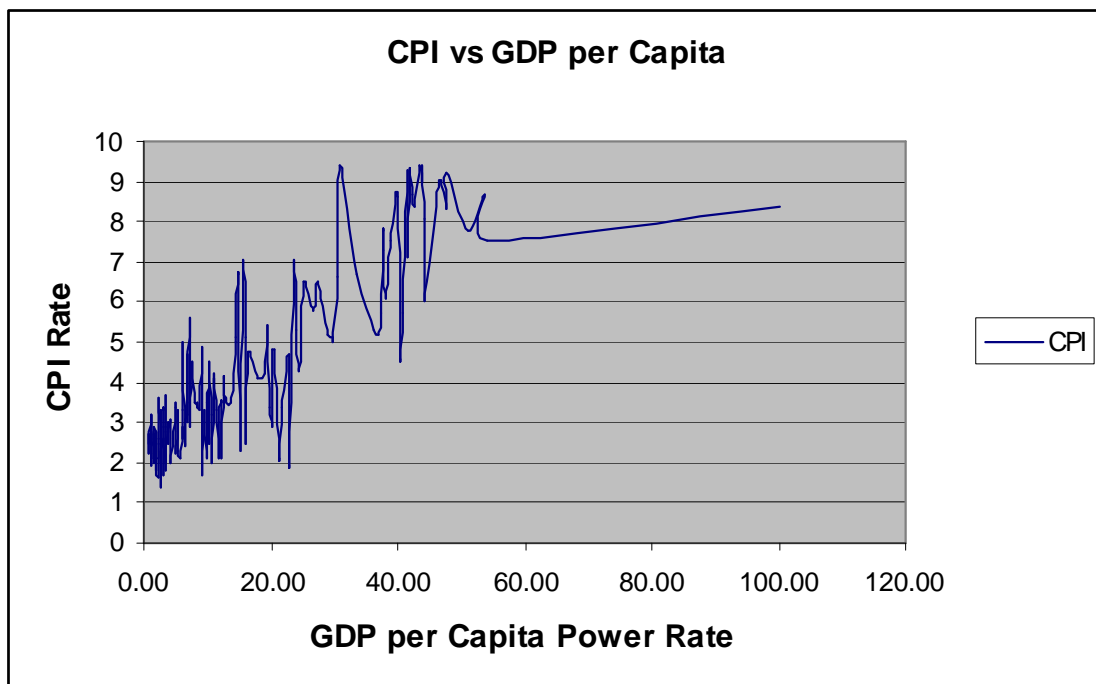


Figure 16 – CPI Rates versus GDP per Capita Power Rates

Even though it is seen in the graphs above, we performed a further work by using SPSS in order to prove that the most development (has the highest GDP per capita) country is the most transparent country. So that the fraud risk is the lowest country. For the results of the work performed, please refer to below:

REGRESSION 1

Table 8 - Descriptive Statistics for CPI vs GDP per Capita

	Mean	Std. Deviation	N
CPI	4,032	2,1167	167
GDP per Capita	13128,795407185 63000	13883,503430634 260000	167

Table 9 – Correlations for CPI vs GDP per Capita

		CPI	GDP per Capita
Pearson Correlation	CPI	1,000	,852
	GDP per Capita	,852	1,000
Sig. (1-tailed)	CPI	.	,000
	GDP per Capita	,000	.
N	CPI	167	167
	GDP per Capita	167	167

Table 10 - Variables Entered/Removed(b) for Regression 1

Model	Variables Entered	Variables Removed	Method
1	GDP per Capita(a)	.	Enter

a All requested variables entered.

b Dependent Variable: CPI

a Predictors: (Constant), GDP per Capita

Table 11 - Anova for Regression 1

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	540,118	1	540,118	437,668	,000(a)
	Residual	203,623	165	1,234		
	Total	743,742	166			

a Predictors: (Constant), GDP per Capita

b Dependent Variable: CPI

We doubt that GDP per Capital and CPI values have a relation. First of all, ANOVA table may help us to verify our claim.

The above table is the ANOVA result of GDP per Capital and CPI data. ANOVA table includes an F test result and sigma.

The most important part of the above table is the sigma value. It is close to 0. Therefore, we are almost 100% sure that we can not reject the hypothesis that GDP per Capital and CPI values are related.

In order to verify our results we had better to see residual analysis. The residuals must fit to normal distribution.

As it can be seen in below histogram and Normal P-P plot of regression the residuals clearly fit to normal distribution.

For example in P-P charts residuals accumulated almost around a straight line.

Table 12 - Residuals Statistics(a) for Regression 1

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2,418	13,681	4,032	1,8038	167
Residual	-5,2813	3,5668	,0000	1,1075	167
Std. Predicted Value	-,895	5,350	,000	1,000	167
Std. Residual	-4,754	3,211	,000	,997	167

a Dependent Variable: CPI

Charts

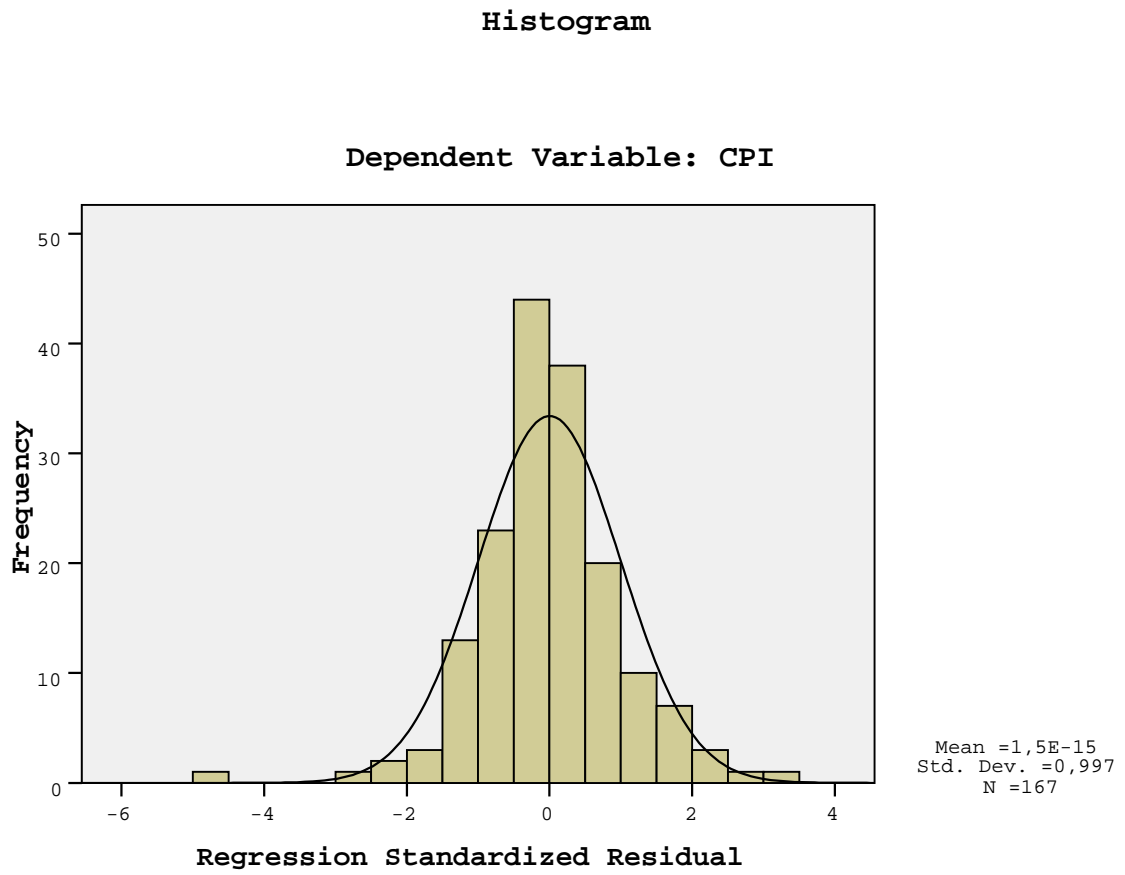


Figure 17 – Histogram 1

Normal P-P Plot of Regression Standardized Residual

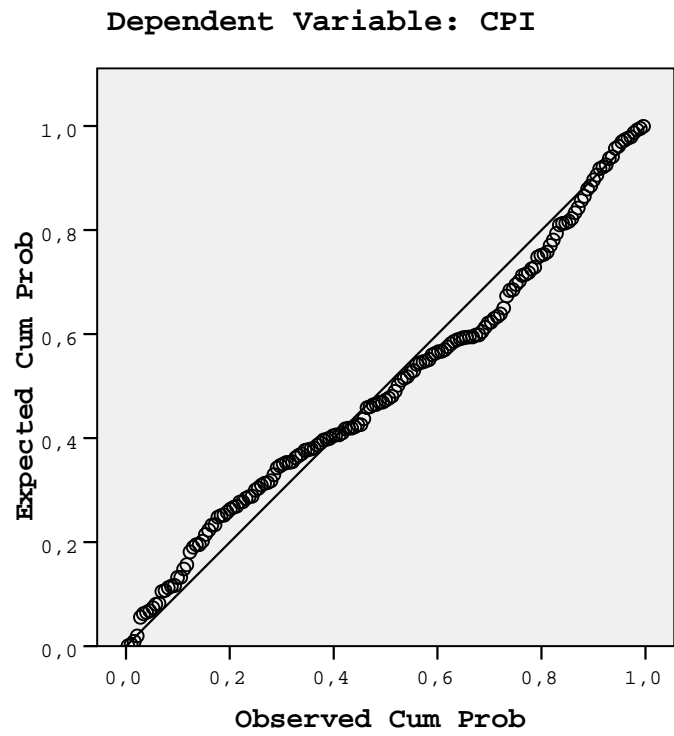


Figure 18 – Normal P-P Plot of Regression 1

POINT GRAPH

Moreover if we insert the related data on x and y axis, as it can be seen it almost fits a straight line.

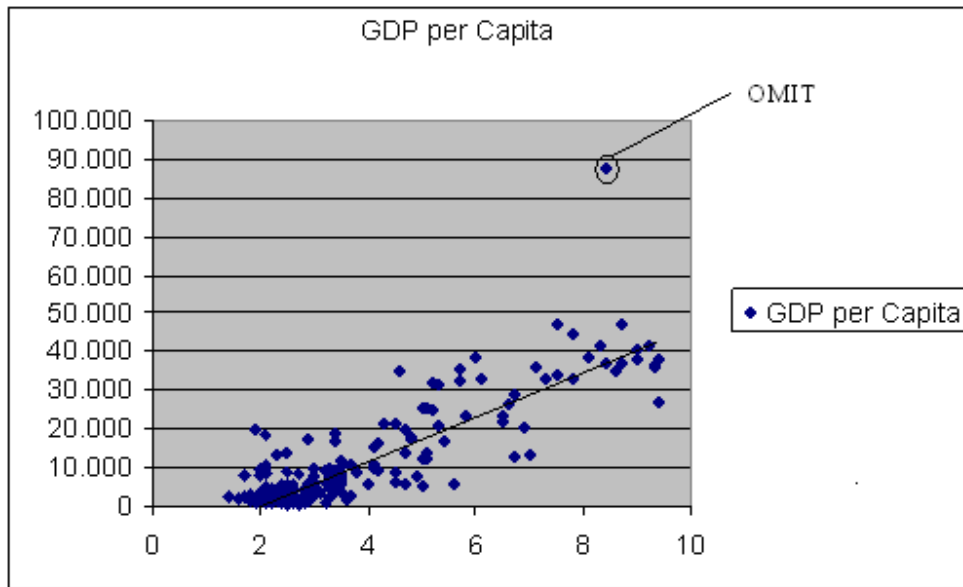


Figure 19 – Point Graph of GDP Per Capita versus CPI

While we were making the analysis, we used corruption *perception* index. However, fraud awareness is as important as the transparency. Because in order to be transparent, first of all the company has to be aware of fraud. Also the supervisors should be aware of the risk of fraud incidents.

Generally, the supervision strategies in Turkey are weak; because there is a lack of awareness among the people. There is a chart on the next page, which informs the situation of Turkey in 2002 in terms of fraud awareness. We can see from this chart that both the awareness of fraud and the awareness of a good supervision strategy is weak in Turkey and we have to know that Turkey cannot achieve its goal unless it changes its attitudes towards the importance of fraud awareness and the supervision strategies.

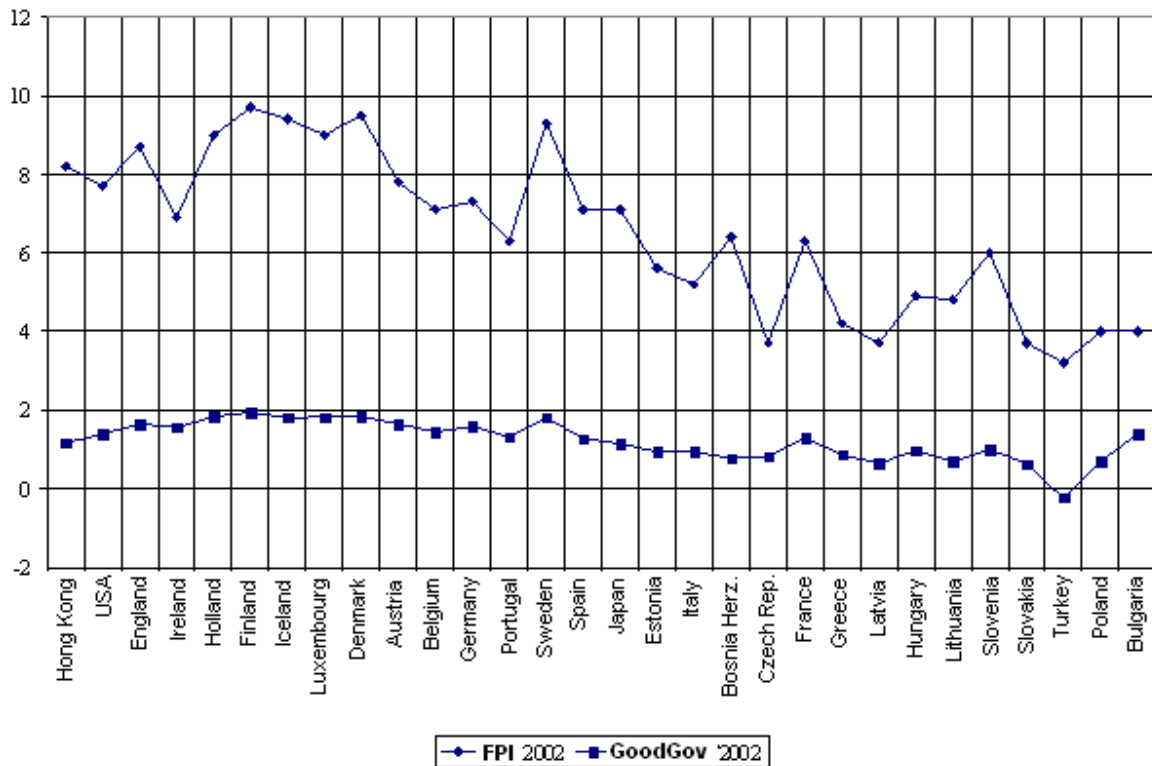


Figure 20 - Fraud Perception Index of 2002 by the International Transparency Organization

Source: <http://www.yolsuzluklamucadele.org/ymvvyo.asp>

As it is seen in the graph above, there is a connection between the perception of fraud and good governance. How much the company is aware of fraud, such the company has good governance.

In order to prove this concept, we performed another spss work. We defined the components as; Fraud Perception Index (FPI) and Good Governance (GoodGov). For the results of the work performed, please refer to below:

REGRESSION 2

	Mean	Std. Deviat	N
FPI	6,570	2,0462	30
GoodGov	1,174	,7154	30

Table 13 – Descriptive Statistics for FPI vs GoodGov

Correlations

		FPI	GoodGov
Pearson Correlation	FPI	1,000	,748
	GoodGov	,748	1,000
Sig. (1-tailed)	FPI	.	,000
	GoodGov	,000	.
N	FPI	30	30
	GoodGov	30	30

Table 14 – Correlations of FPI vs GoodGov

Variables Entered/Removed^b

Model	Variables Entered	Variables Removed	Method
1	GoodGov ^a	.	Enter

a. All requested variables entered.

b. Dependent Variable: FPI

Table 15 – Variables Entered/Removed for Regression 2

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,748 ^a	,559	,543	1,3829	,559	35,489	1	28	,000

a. Predictors: (Constant), GoodGov

b. Dependent Variable: FPI

Table 16 – Model Summary for Regression 2

First of all, ANOVA table may help us to verify our claim.

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	67,872	1	67,872	35,489	,000 ^a
	Residual	53,551	28	1,913		
	Total	121,423	29			

a. Predictors: (Constant), GoodGov

b. Dependent Variable: FPI

Table 17 – Anova for Regression 2

The above table is the ANOVA result of GoodGov and FPI data. ANOVA table includes an F test result and sigma.

$F_{0.01,1,28} = 7.636 < 35,849$ so accept the null hypothesis

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	4,060	,491		8,266	,000	3,054	5,066
	GoodGov	2,138	,359	,748	5,957	,000	1,403	2,874

a. Dependent Variable: FPI

Table 18 – Coefficients for Regression 2

Coefficient Correlations^a

Model		GoodGov
1	Correlations GoodGov	1,000
	Covariances GoodGov	,129

a. Dependent Variable: FPI

Table 19 – Coefficient Correlations for Regression 2

Since the sigma value is close to 0, we are almost 100% sure that we can not reject the hypothesis that GoodGov and FPI values are related.

In order to verify our results we had better to see residual analysis. The residuals must fit to normal distribution.

As it can be seen in below histogram and Normal P-P plot of regression the residuals clearly fit to normal distribution.

Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,211	8,230	6,570	1,5298	30
Residual	-3,1609	3,0890	,0000	1,3589	30
Std. Predicted Value	-4,157	1,085	,000	1,000	30
Std. Residual	-2,286	2,234	,000	,983	30

a. Dependent Variable: FPI

Table 20 – Model Summary for Regression 1

Charts

Histogram

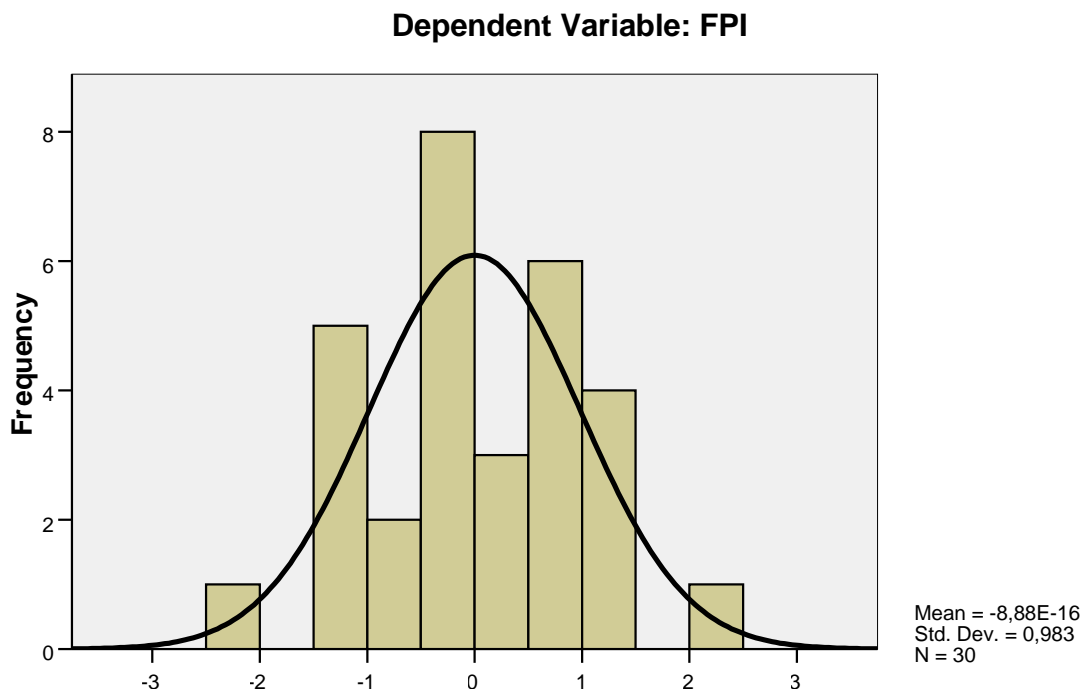


Figure 21 – Histogram 2

Normal P-P Plot of Regression Standardized Residual

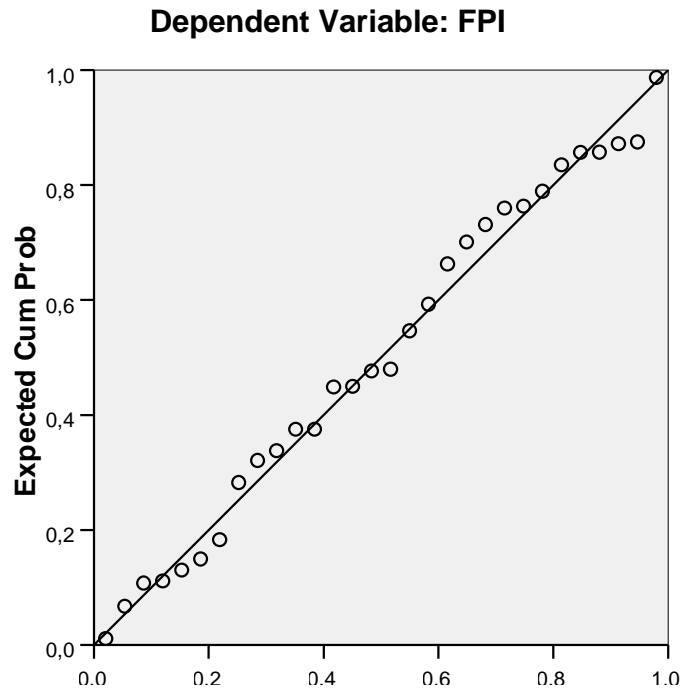


Figure 22 - Normal P-P Plot of Regression 2

7 – A GOOD DETECTION SYSTEM

There are many systems that help to prevent the occurrence of fraud incidents. I want to focus on the model of the Cap's Handbook of Fraud and Commercial Crime.²⁴ According to this handbook, there are four main steps when combating fraud risks. These are; internal controls, supervision, audit and whistle-blowing system and are discussed in this order below.

7.1 Internal Controls

- a) **Defining internal controlling objectives:** The first thing we have to do when dealing with an issue is to determine our aim, so at this level we have to know what we want to achieve at the end of this process. At this stage we can benefit from the victims as a tool. The victims may give us the required information related to the fraud risks and our strategy may include the consequences of such experiences. To gather information about the risk of fraud is not enough to define our control objectives, we have to get also information about the management system and the reports of the company. There are some basic rules in order to carry out an effective control system. Especially according to a study of Dr. Genç Osman Yaraşlı (2005)²⁵, the system of controlling should aim to be independent. Namely, it should not be easily affected from external factors. The supervision and auditing system should be prepared without taking some political objectives into consideration and the company has to have enough funds in order to support such kinds of controlling

²⁴<http://antifraud.aicpa.org/Resources/Auditors/Understanding+Programs+and+Controls/Internal+Controls+and+Fraudproofing.htm>

²⁵http://209.85.135.104/search?q=cache:14qjFHBu9jcJ:www.yolsuzluklamucadele.org/sunumlar/Genc_Osman_yolsuzluk.ppt+yolsuzluk+ve+denetim+y%C3%B6ntemleri&hl=en&ct=clnk&cd=1

programs. Professional supervisors and auditors should be involved in this process.

At last the system should aim to achieve accountability.

According to Section 56 of Public **Financial Management and Control Law numbered 5018**, the main objectives of an internal control strategy should be:

- To manage the public income, outcome and properties in an effective and economic way.
- To control the public associations and determine whether they perform within the framework of the related laws and regulations.
- To prevent any type of misuse and fraud during the decision making process related to a financial issue.
- To arrange regular reports and gather reliable information in order to facilitate the decision – making process and the performance of the implementations.

b) Basic Controls: At this level we can say that there are three main stages. These are:

- **Physical access:** It is related to the access of employee or manager to the financial or other type of resources. If there is a lack of preventions against easy physical access, coming across a fraud incident may not be surprising for the related authorities. If the company wants to prevent physical access, the authorities should lock the doors, desks and file cabinets. Each employee should have an access card and this card should record when and how long an employee accessed the departments of the company. Each employee should be responsible for his own task. Namely, there are some basic places

for each employee and he should be restricted access to other departments of the company as he is unauthorized.

If the company does not take the required measures they may experience asset misappropriation and as we know this is one of the most common types of fraud incidents. One of the most important measures is the control of physical access. There should be authorities, who control employees and their activities. An effective control within the company should be deterrent for the perpetrators. If the company takes the required measures, it may prevent the opportunity of an economic crime at some level.

- **Job Description:** Employees should be aware of their responsibilities and this awareness can be shaped by an effective job description. An employee is just expected to do his own duties and as we said before if he is enthusiastic to do more than what is expected from him, he may demonstrate a red flag.

An employee should not be responsible for more than one department. He may just do his own task and this may give him the authority that he requires, but not more.

When we look at Turkey, we may see that “an internal control” system was prepared in 2003 within the framework of **Public Financial Management and Control Law numbered 5018**. According to this law, the job description is not enough. The performance of employees should also be evaluated and if he is not suitable to the job description, the authorities may change his position. According to the 9th part of the **Public Internal**

Control Standards²⁶, different employees should be responsible for the confirmation of documents, implementation of programs and the saving of the reports within the domain of financial decision – making. The companies, which do not have the required number of employees, should be aware of the problems related to the job description and should also, take some measures in order to prevent a big chaos.

- **Accounting Reconciliations and Analyses:** This part focuses on the most important third stage of the controlling strategy. Generally, perpetrators try to conceal all the evidence after the occurrence of a fraud incident and if the company wants to prevent such concealment, it should give the authority to a group of people, so that they can perform accounting reconciliations and analyses. Accounting reconciliations should regularly be carried out and some basic points about this issue are:
 - The reconciliation of all bank accounts
 - All kinds of receivable reconciliation accounts
 - Accounts payable reconciliations

The nature of the accounting reconciliations and the nature of the organization's operations are interrelated. Namely, we can explain this via the examples below:

²⁶ <http://www.memurlar.net/haber/97108/>

- “Variance analysis of general ledger accounts (budget to actual, current year versus prior year, and so on)
- Vertical analysis of profit and loss accounts (that is, calculation of expenses as a percentage of sales, and comparison of these percentages with historical standards, or budgets, or both)
- Detailed sales and major expense analyses (for example, by product line or territory)”²⁷

7.2 Supervision

A good supervision is another step of an internal control, which is vitally important for a company. Actually, we can say that a supervisor is like a coach for employees. If the supervisor coaches well, employees will reach the required goals within the desired time period. The supervisor teaches employees, guides and motivates them, so that they can achieve their goals. A supervisor is also interested in the career and the performance of the employee. Therefore, the employee can consider the supervisor as a model for direction and development. The supervisor is like a mediator between the organization and employees. If there is a change within the operation of the organization, the supervisor is the one, who informs employees about these changes and if there is a problem among employees, the supervisor is the one, who informs the organization about this issue.

Now, as we know the duties of a supervisor, we can mention about the steps of a good supervision. There are two main points within the framework of an effective supervision.

These are:

27

<http://antifraud.aicpa.org/Resources/Auditors/Understanding+Programs+and+Controls/Internal+Controls+and+Fraudproofing.htm>
<http://www.managementhelp.org/suprvise/roles.htm>

- **Fraud awareness:** Fraud awareness is the key point, when selecting the supervisors. The supervisors should be aware of the risk of fraud incidents and how dangerous they can be. The supervisor should take the possibility of a fraud risk whenever he comes across a red flag, which can be an indication for him. As we said, the supervisor is like a mediator between the company and employees. Therefore, he is also the one, who has to inform employees about the fraud awareness and he has to teach them.

As we mentioned before, the company's awareness of fraud is also strictly important at this point, because if the company is not aware of the dangerous situation, it will not appoint a supervisor in order to follow the latest changes within the company. According to a study of Pwc, the awareness of fraud has changed between the years 2003 and 2007. The figure below, gives us information about the fraud incidents that have been reported during the involved years and this figure may be a guide for us when understanding the change of fraud awareness.



Figure – 23: Respondent’s Perceptions of the Prevalence of Fraud in Their Industry, in Their Country (2003 – 2007) ²⁸

- Approval, Review, Double-checking and Redoing:** After being aware of the potential situation, the supervisor should take action in order to prevent any risk. At this point the supervisor should both approve the typical invoices or performing and duties of employees and managers and check the performance of employees twice. Namely, he has to redo some tasks in order to be sure about the current situation.

Generally, the supervision strategies in Turkey are weak; because there is a lack of awareness among the people and redoing a task has always been difficult for Turkish people. A good supervision and a good awareness of fraud may be one of the key points of a good managed strategy against fraud incidents.

²⁸ The 4th biennial global economic crime survey of Pwc in 2007

At first, the companies within Turkey have to develop their supervision strategies and they should provide a qualified supervision management, so that they can prevent the possibility of fraud risks at some level. A good supervision strategy for Turkey should include a professional team of employees and managers, a well – built infrastructure and a regular maintenance. Namely, to achieve a good supervision strategy is not enough. If the company wants to be successful, it should maintain the strategy properly.

The supervision system within Turkey is generally based on the financial aspect of fraud incidents, but this may not always be successful; because the fraud incidents do not only cause financial damages. The incidents can also cause some social damages, which can be much more dangerous than financial damages. Some of these damages are:

- To prevent the execution of human rights, democracy, rule of law within the country.
- To deteriorate the public management system.
- To prevent a sustainable development within the domain of economy.
- To harm the ethic norms of the society.

7.3 Audit

From a fraud prevention perspective, we can say that the auditing process is also strictly important. According to a study of Wells²⁹, the audit function had a substantial impact on the size of the typical fraud and companies who had internal or external audit centers were 35% less damaged by fraud risks than other companies, which do not have any type of auditing centers (see table 8).

²⁹ <http://www.aicpa.org/pubs/jofa/apr2002/wells.htm>

Internal or external audit conducted?	Number of cases	Average Financial Loss
Yes	81.5	\$100,000
No	18.5	\$156,000

The audit process includes the examination of documents, analyses of trend data and verification of assets. The risk of fraud can be detected during the auditing process or after the fraud incidents, but we have to know that auditing strategies are a deterrent for employees and managers, who have the potential to commit an economic crime.

There are two types of auditing strategies. These are:

1 – Internal Audit: The work of internal auditors is defined by a senior manager and it includes the internal activities within a company. According to the Committee of Sponsoring Organizations of Tread way Commission (COSO), the success of an internal audit depends on three basic points that are stated below:

- a) Effectiveness and efficiency of operations.
- b) Reliability of financial reporting.
- c) Compliance with laws and regulations.”³⁰

In other words, we can say that an internal auditor is like a senior manager.

³⁰ http://en.wikipedia.org/wiki/Internal_audit

2 – External Audit: “An **External auditor** is an audit professional who performs an audit on the financial statements of a company, government, individual, or any other legal entity or organization, and who is independent of the entity being audited.”³¹ As we know, external auditors are independent of the company and they have their own methods when auditing the involved organization. They base their studies on financial statements and other independent reviews.

“Watchdog” is another name that has been used instead of external auditors, because it has been known that the role of an external auditor is to inform the related authority about the fraud risks whenever he sees something suspicious and dogs also bark when they realize something suspicious. Therefore, the external auditors are also known as watchdogs.

At some stages the regulator of the company and the external auditor work together in order to prevent the risk of fraud. The regulator of the company may inform the external auditor about the regulations within the company. The aim of the external auditor is to evaluate the financial performance of the company and then to determine whether all the implications within the company are suitable to some laws and regulations of the company. The external auditor can also evaluate the profit and loss trend of a company. If the external auditor analyses something suspicious, he may inform the regulator about this issue and the regulator may be the one, who seeks for new options.³²

As an auditor, I want to share a sample inquiry which I performed with the CEO of a feed company below. According to the CEO’s answers, I made my fraudulent findings as *italic*.

³¹ http://en.wikipedia.org/wiki/External_auditor

³² Role of External Auditor and Implications of the New Companies Act by Dr. Raneey Jayamaha, the Deputy Governor, Central Bank of Sri Lanka
http://www.cbsl.gov.lk/pics_n_docs/02_prs/docs/speeches/speeches_20070612.pdf

QUESTIONS

- 1- What do you perceive to be the 2 or 3 most significant risks for the company (business or other)?
- 2- In the past, what kinds of fraud have been committed against the company by employees or executives, including defalcations and employee thefts?
- 3- What is the role of senior management in the company's antifraud program? Do you believe senior management recognizes it has ultimate accountability for anti-fraud programs within the company?
- 4- Are you aware of a fraud hotline or other similar avenues that exist for employees to report suspected fraud? What training is provided to employees regarding hotlines, etc?
- 5- Is there pressure on management or operating personnel to meet financial targets?
- 6- Is there increased pressure on management due to market competition, industry changes, declines in customer demand, or regulatory requirements? If so, in the interviewee's view, how could these pressures compromise financial reporting?
- 7- Does the company have realistic goals and forecasts?
- 8- Are there procedures to perform background investigations for employees, business partners, vendors, or customers? If so, what are these procedures?
- 9- Are incentives aligned with ethical values in any manner?
- 10- Do you believe management (either local, division or corporate) have an aggressive manner with accounting treatments?

11- Do you have any plans or intentions that may materially affect the carrying value or classification of assets and liabilities?

12- Do you have any knowledge of anyone in the company withholding information from management, altering documents or committing fraud?

ANSWERS

- 1) The sudden changes occur in the climate conditions cause the insufficient harvest productivity. Besides the productivity of the harvest, the quality level also declines regarding to this condition. Due to the volatility in the productivity, the prices fluctuate. From time to time, the prices may fall significantly in the sector.
- 2) In the time of the harvest collection, during the purchase of products, the responsible persons cannot confirm a certain purchase price since the sellers are not educated, the recordings frequently come out with errors and inappropriately.
- 3) In the sector no anti-fraud program exists. The sellers generally consist of land-owning persons and farmers. The transactions occur casually thus no anti-fraud program can be established.
- 4) There is no such hotline. However the informal information flow occurs within the villages but this issue cannot be proved thus it is not valid for us.
- 5) Experts are organizing the land-owner persons and farmers for the transactions. We warn the experts to provide sufficient quantity of products otherwise we do not pay their premiums.

- 6) There is no difficulty in financial reporting. Profit/ loss is not important. (*Cost changes may lead to fraud issues. However it must be noticed that the unproved actual findings cannot be reflected to the reports.*)
- 7) Regarding to the plantation performed in the prior year and the expected climate conditions, the experts estimates a deviation of (+)/ (-) 10%. However we cannot reconcile the deviation margin through this expectation. The promises of the government does not shape the budget so the experts does the budget . (*This causes fraud.*)
- 8) These kinds of issues does not belong to our perception. Most of the persons in the sectors have close relations and the reporting is done regarding to the revenue. (*However also subvention is distributed to the farmers and this may lead to fraud.*)
- 9) Sometimes it is faced that an expert is a relative of a farmer or a land-owning person. Sellers claim to sell less in tonnage but the actual quantity is generally noted to be higher. These are ordinary situations. (*There is no recording control for the transactions and this is another fraud risk.*)
- 10) There are many inappropriate issues such as the lack of physical stock count and control. Since the persons in the field know each other, sometimes the accountant, the seller, the buyer can all have close relations and the invoices and records can be done in their will. (*There is no control point fort his issue and this creates fraud risk.*)
- 11) The products shall be segmentated on the basis of the quality levels but we cannot deal with it. The experts make the purchase and claim the acquisition as; X% from product A, Y% from product B etc. We claim the quality level as an assumption to

the government. (*There is weakness in the control system of the government. Also the prices can change regarding to the reporting destination.*)

12) We do not accept this kind of issues within our perception. The documents sent to the government claims that 90% of the products are “A” quality. Some samples are sent for the control of the government. They focus on the control points of the government and acts accordingly. (*The government control system does not seem to be efficient.*)

It was just a small inquiry which helped to expose noticeable fraudulent situation. Except the auditing of financial position of the company, an auditor should investigate the fraudulent situations for all topics at all level of the company.

7.4 Whistle – Blowing System

Professional whistle –blowing systems are usually implemented by private and public organizations in order to encourage their employees to report issues that can influence their business and responsibilities in a serious manner. When we look at the history of whistle – blowing system, we may see that it has evolved during the past 50 years in America. At these times, the whistleblowers were not as important as they were today, because many economic crimes were concealed. Employees could be fired and hired without giving any logical reasons. Namely, we can say that this system is also beneficial so as to protect the rights of the involved employees. The objectives of a whistle – blowing system include:

- To minimize the damage of a fraud incident to an organization when employees violate the mechanisms within the involved organization.

- To make employees aware of the fact that the organization is serious about adherence to codes of conduct.
- To let employees work in an ethical and legal way.

There are also some hindrances, which are against the implementation of a whistle – blowing system; because a whistle – blowing system may be harmful to both the organization and the employee. For example, an external whistle – blowing to media or government agencies may harm the brand name of the company. Therefore, companies usually prefer to implement internal whistle – blowing systems. Some of the hindrances related to the implementation of a whistle – blowing system are:

- A lack of trust within the internal system of the company
- Unwillingness of employees to be “spies”; because this may affect their relationships with other employees.
- Fear of retaliation

Some tips so as create a well – built whistle – blowing system:

1. At first the company has to determine a policy about informing the violations within the company. Moreover, the communication process between the organization and employees should also be well determined.
2. The second step is related to the endorsement of the top management.
3. To publicize the organization’s commitment, is also very important when creating a whistle – blowing system, because this means the creation of an open and honest culture.

4. The managers have to investigate any kind of claim and than should prepare a report related to the issue.
5. At last the authorities should provide the assessment of the organization’s whistle – blowing system.
6. Be careful that employees, who involve in a whistle – blowing system is secure and confidentiality should be one of the most important issues within a whistle – blowing system.

More and more companies try to install the system of whistle – blowing and according to the global economic crime survey of Pwc in 2007, it has been thought that even the existence of this system can cause positive conclusions. Moreover, the companies, which have been successful in implementing an effective whistle – blowing system could benefit more from this system (see figure 24).

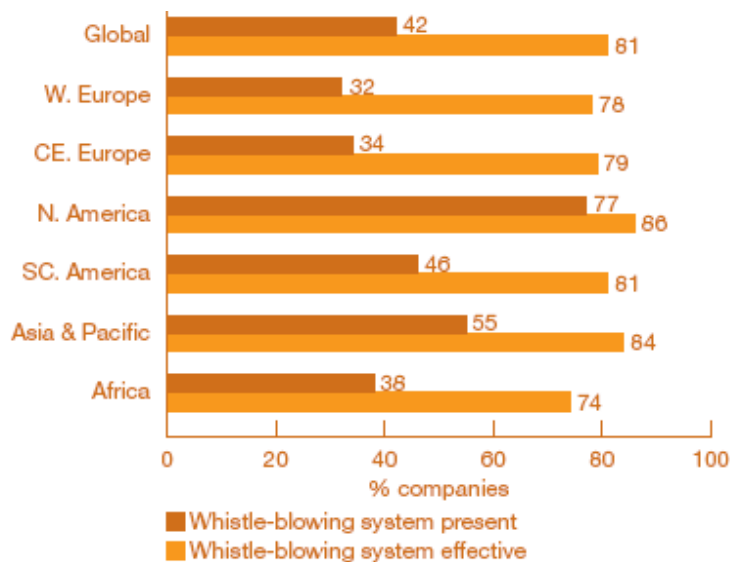


Figure 24 – The Percentage of the Companies, which Think that the Whistle – Blowing System is Beneficial³³.

³³ The Global Economic Crime Survey of PwC in 2007.

CONCLUSION

Fraud has been a common issue for all companies around the world during the recent years. Therefore, I thought that it would be worth studying this issue so as to clarify some points. It has been understood that fraud will also continue to be a big threat in the future. As a result, more studies and methods should be developed in accordance with the prevention of fraud incidences.

In Turkey we can see that the social and economic fluctuations provide the required opportunity for the fraud perpetrators. Eventhough the reported fraud incidents are low in Turkey, we know that the loss because of fraud incidences is very high. It is related with the transparency level of Turkey. As a result of our transparency analysis, how much the CPI level of country is high, such that the company is developed. When we consider that Turkey is a emerging country, CPI level is very low and fraud perpetrators are seen very much despite the reported issues are low. The incidences of fraud do not only affect the investors, but also the poor citizens of the country; because these incidences cause hindrance against a sustainable development, prevent the external investments, encourage the violation of laws and harm directly or indirectly the human rights within the country.

If the authorities want to prevent fraud incidences in Turkey, there should be a public management consisted, which is transparent, stable and accountable, saving, effective, qualified ...etc. The aim of the supervision and auditing activities should be focused on the implementation of the basic points stated above. Moreover, they have to detect the mistakes and give reliable information to the authorities so that they can arrange new solutions.

The quality of the supervision and auditing system has been a vital issue when determining the effectiveness of these systems. If the supervision and audit system is of high quality, we may say that it can achieve the goals earlier than other supervision and audit systems. A quality supervision and audit system must be able to control its own performance in accordance with effectiveness and stability.

Not only the supervision and audit authorities, but also the governments should be responsible when combating fraud incidences. The government should prepare new laws in order to prevent fraud incidents and the executive body of the government should be able to execute the new laws. Media can also be a helpful tool during this process; because it may distribute the new developments to public and as a result, we can say that this combating process can include the whole country.

Another point is related to the awareness of people towards public prosperity. As a result of the FPI analysis in this study, it is seen that how much people are aware, such the supervision is effective. So that there should be educational programs, from which the citizens can learn the ethical and legal ways of working in an organization or company.

This issue has been vitally important for our country; because the welfare of a country cannot be consisted if there have still been fraud incidences.

REFERENCES:

Agrawal A., Chadha S., (2005), Corporate governance and accounting scandals. *Journal of Law and Economics* 48:371–406

Akerlof, George A., and Paul M. Romer, (1993), “Looting: The economic underworld of bankruptcy for profit,” *Brookings Papers on Economic Activity*, 2: 173.

Aldrich, J.H. and Nelson, F.D., (1984), *Linear probability, logit and probit models*, Thousand Oaks, CA, Sage.

American Institute of Certified Public Accountants (‘AICPA’), (2003), *Statement on auditing standards # 99: Consideration of fraud in a financial statement audit*, New York, AICPA.

Anderson, J. Richard, Tirrell, Michael E., (2004), Too Good to Be True CEOs and Financial Reporting Fraud. *Consulting Psychology Journal: Practice and Research*, 1065-9293, 2004, Vol. 56, Issue 1

Apostolou, B.A., Hassell, J.M, Webber, S.A. and Summers, G.E. (2001), The relative importance of management risk factors.

Apostolou, Nicholas, Crumbley, D Larry (2008), Auditors' Responsibilities with Respect to Fraud: A Possible Shift? *The CPA Journal*. New York: Feb 2008. Vol. 78, Iss. 2; pg. 32, 5 pgs

Appelbaum, Richard P. & Chambliss, William J. (1997). *Sociology: A Brief Introduction*. New York: Longman. ISBN 0-673-98279-3

Association of Certified Fraud Examiners ('ACFE'), (2000), *Fraud Examiners' Manual*, 3rd edition, ACFE, Austin TX.

Association of Certified Fraud Examiners - UK ('ACFE - UK'), (2003), *Fraud Examiners' Manual*, 2nd edition, ACFE, Austin TX.

Australian Institute of Criminology & PricewaterhouseCoopers, (2003), *Serious Fraud in Australia and New Zealand*, Research and Public Policy Series, no. 48, Australian Institute of Criminology, Canberra.

Baucus, M.S., (1994), Pressure, opportunity and predisposition: a multivariate model of corporate illegality, *Journal of Management* 20(4): 699-721.

Baucus, M.S. and D.A. Baucus, (1997), Paying the piper: an empirical examination of longer-term financial consequences of illegal corporate behavior. *Academy of Management Journal* 40(1): 129-151

Baucus, M.S. and J.P. Near, (1991), Can illegal corporate behavior be predicted? An event history analysis. *Academy of Management Journal* 34(1): 9-36.

BDO Stoy Hayward, (2006), 'Inside Job': Fraud Track 3: Rising Fraud in the Spotlight: Annual Survey (2006) BDO Stoy Hayward UK.

Beasley, M.S., (1996), An empirical analysis of the relation between the board of director composition and financial statement fraud. *The Accounting Review* 71(4): 443-465.

Beasley, M.S., J.V. Carcello, D.R. Hermanson and P.D. Lapedes, (2000), Fraudulent financial reporting: considerations of industry traits and corporate governance mechanisms, *Accounting Horizons*, 14(4) 441-455.

Bell, T.B., W.R. Knechel, J.L. Payne and J.J. Willingham, (1998), An empirical investigation between the computerization of accounting systems and the incidence and size of audit differences. *Auditing: A Journal of Practice and Theory* 17(1): 13-38.

Bologna, G.J., (1993), *Handbook on corporate fraud: Prevention, detection and investigation*, Stoneham, MA, Butterworth-Heinemann. Bologna, G.J. and R.J. Liguori. 1995

Burch, Cathalena E., McClatchy, (2008), Promoter of big-name local concerts indicted; \$26M fraud alleged *Tribune Business News*. Washington: May 29, 2008.

Cabinet Office. *Identity Fraud*, (2002), London: Cabinet Office.

Carpenter, Tina D, (2007), Audit Team Brainstorming, Fraud Risk Identification, and Fraud Risk Assessment. *The Accounting Review*; Oct 2007; 82, 5; ABI/INFORM Global pg. 1119

Clarke, M., (1990), *Business crime: its nature and control*, Cambridge UK, Polity Press.

Clarke, Ronald R. (ed.) (1997). *Situational Crime Prevention: Successful Case Studies*. Second Edition. New York: Harrow and Heston. ISBN 0-911577-39-4

Deli, D., Gillan, S., (2000), On the demand for independent and active audit committees. *Journal of Corporate Finance* 6:427–445

Dobrzynski, J. H., (2000), 'E-Bay Fraud: In Online Auctions, Rings of Bidders, *New York Times*, June 6.

Educational Publishing Foundation and the Society of Consulting Psychology, (2004), 1061-4087/04/\$12.00 DOI: 10.1037/1061-4087.56.1.35 *Consulting Psychology Journal: Practice and Research*, Vol. 56, No. 1, 35–43

Efendi J., Srivastava A., Swanson E. P., (2007), Why do corporate managers misstate financial statements? The role of option compensation and other factors. *Journal of Financial Economics* 85:667–708

Erickson M., Hanlon M., Maydew E., (2006), Is there a link between executive compensation and accounting fraud? *Journal of Accounting Research* 44:113–143

Ferrarini, Guido Alessandro, Giudici, Paolo (2005), *Financial Scandals and the Role of Private Enforcement: The Parmalat Case*. SSRN Working Paper Series. Rochester: May 2005.

Fraud Review. Final Report, (2006), London: Attorney General's Office.

Free, Clinton., Macintosh, Norman., Stein, Mitchell., (2007), Management Controls: The Organizational Fraud Triangle of Leadership, Culture and Control in Enron, Ivey Business Journal Online. London: Jul/Aug 2007. 1 pgs

Gibeaut, John (2007), Mortgage Fraud Mess. ABA Journal. Chicago: Jul 2007. Vol. 93 pg. 50, 7 pgs

Greenlee, Janet, Fischer, Mary, Gordon, Teresa, Keating, Elizabeth (2007), An Investigation of Fraud in Nonprofit Organizations: Occurrences and Deterrents Nonprofit and Voluntary Sector Quarterly. San Francisco: Dec 2007. Vol. 36, Iss. 4; pg. 676

Hanford, D. J., (2005), Fraud Fears Slow Online Shopping, Wall Street Journal 13, 1.

Holtfreter, Kristy, Leeper Piquero, Nicole, R Piquero, Alex (2008), And justice for all? Investigators' perceptions of punishment for fraud perpetrators. Crime, Law and Social Change. Dordrecht: Jun 2008. Vol. 49, Iss. 5; pg. 397, 16 pgs

Holthausen, R., Leftwich, R. (1983), The economic consequences of accounting choice: Implications of costly contracting and monitoring. Journal of Accounting and Economics, 5, 77–117.

House of Commons Committee of Public Accounts, (2003), Tackling Fraud against the Inland Revenue: First Report of Session 2003–04.

Hutchins, Holly M., Wang, Jia, (2008), Organizational Crisis Management and Human Resource Development, *Advances in Developing Human Resources*. San Francisco, Vol. 10, Iss. 3; pg. 310

Jayamaha, Dr.Ranee, the Deputy Governor, Central Bank of Sri Lanka, (2007), Role of External Auditor and Implications of the New Companies Act

Jimenez, Ignacio Gomez (2008), Tax fraud and shady buildings, *Organization for Economic Cooperation and Development. The OECD Observer*. Paris: Mar 2008. , Iss. 266; pg. 27, 2 pgs

Koehn, D., (2003), The Nature of and Conditions for Online Trust, *Journal of Business Ethics* 43, 3–19

Ko-Yung, Tung Vice President and General Counsel the World Bank, (2002), The World Bank's Institutional Framework for Combating Fraud and Corruption, Remarks delivered at Seminar on Monetary and Financial Law International Monetary Fund May 8, 2002

Lamsdorff, Johann Graf, (2007), The Methodology of the TI Corruption Perceptions Index 2007, University of Passau, Sept.2007

Leatherwood, M., and Spector, L, (1991), Enforcements, Inducements, Expected Utility and Employee Misconduct, *Journal of Management (JofM)*, 17(3), 553 - 569.

Levi M., Burrows J., (2008), Measuring the Impact of Fraud in the UK, *British Journal of Criminology* 2008 48(3):293-318; doi:10.1093/bjc/azn001

Maremont, M., Spurgeon, D. (2000), Rite Aid faces possible criminal probe of accounting practices. *The Wall Street Journal*, p. B2.

Mawhood, J. and D. Tysver, (2000), Law and the Internet, in D. Langford (eds. *Internet Ethics* (St.Martin's Press, New York, NY), pp. 96–126

McPhail, K., (2001), The Other Objective of Ethics Education: Re-humanising the Accounting Profession
– A Study of Ethics Education in Law, Engineering, Medicine and Accountancy, *Journal of Business Ethics* 34, 279–298.

McPhail, K, (2004), An Emotional Response to the State of Accounting Education: Developing Accounting Students Emotional Intelligence, *Critical Perspectives in Accounting* 15, 629–648.

National Audit Office, (2003), Tackling Fraud against the Inland Revenue, London: National Audit Office.

National White Collar Crime Center, (2003), 'IFCC 2002, Internet Fraud Report.

Nikitkov, A. and D.N. Stone, (2006), 'Towards a Model of Online Auction Deception, Working paper.

Nikitkov, A., Bay, D., (2007), Brock University, Journal of Business Ethics 79:235-244

Pesola, M., (2005), 'Vietnam, Romania and US Top Internet Fraud List, Financial Times, March 1, 11.

PriceWaterhouseCoopers, (2005), Global Economic Crime Survey: United Kingdom London: PwC.

PriceWaterhouseCoopers. (2007), Global Economic Crime Survey

PriceWaterhouseCoopers. (2007), The 4th biennial global economic crime survey

Ramsey, Dave; Sharon Ramsey (2003). Financial Peace Revisited. Harmondsworth, Middlesex, England: Viking Penguin, Preface, x. 0-670-03208-5.

Robb, G., (1992), White-Collar Crime in Modern England: Financial Fraud and Business Morality, 1845-1929 Cambridge, 189

Robison H., Santore R., (2006), Managerial incentives and corporate fraud, unpublished working paper, LaSalle University.

Rosen, C. M. and G. M. Carr, (1997), Fares and Free Riders on the Information Highway, *Journal of Business Ethics* 16, 1439–1445.

Russell, G. Smith , (2008), Coordinating individual and organizational responses to fraud. *Crime, Law and Social Change*. Dordrecht: Jun 2008. Vol. 49, Iss. 5; pg. 379, 18 pgs

Schnatterly, K. 2003. Increasing firm value through detection and prevention of white-collar crime, *Strategic Management Journal* 24(7): 587-614.

Shane, A. Johnson, Harley E. Ryan, JR. and Yisong S. Tian, (2008), Managerial Incentives and Corporate Fraud: The Sources of Incentives Matter, *Review of Finance*, Oxford Journals.

Shearer, T., (2002), Ethics and Accountability: from the For-itself to the For-the-other , *Accounting, Organizations and Society* 27, 541–573.

Shover, Neal & Wright, John Paul (eds.) (2000). *Crimes of Privilege: Readings in White-Collar Crime*. Oxford: Oxford University Press. ISBN 0-19-513621-7

Stead, B. A. and J. Gilbert, (2001), Ethical Issues in Electronic Commerce, *Journal of Business Ethics* 34, 75–85.

Sutherland, Edwin H. (1949) 'White Collar Crime' New York: Holt Rinehart and Winston.

Taylor, James (2007), Company Fraud in Victorian Britain: The Royal British Bank Scandal of 1856 *University of Lancaster English Historical Review* CXXII:700-724, 2007
doi:10.1093/ehr/cem093

Three Miami Area Doctors and Six Others Charged in \$56 Million Health Care Fraud Schemes, (2008), Anonymous. PR Newswire. New York: May 29, 2008.

Uluslararası Saydamlık Örgütü (Transparency International), (2006), 2006 Rüşvet Verenler Endeksi Sonuçları

Updated Estimate of the Cost of Identity Fraud to the UK Economy, 2 February (2006)
London: Home Office.

Xu, Yin, Ziegenfuss, Douglas E. (2008), Reward Systems, Moral Reasoning, and Internal Auditors' Reporting Wrongdoing, *Journal of Business and Psychology*. New York: Jun 2008. Vol. 22, Iss. 4; pg. 323, 9 pgs

Wells, Joseph T. (2002). Occupational Fraud: The Audit as Deterrent, The Journal of Accountancy Online, Jan-02

Wells, Joseph T ; Gill, John D, (2007), Assessing Fraud Risk, Journal of Accountancy; Oct 2007; 204, 4; ABI/INFORM Global pg. 63

Wiley, John and Sons, (2008), Fraud auditing and forensic accounting: New tools and techniques, New York, NY

Williams, Kathy (2007), Fraud Remains Pervasive, PWC Study Shows, Strategic Finance; Nov 2007; 89, 5; ABI/INFORM Global pg. 13

Wilson D., Patterson A., Powell G., Hembury R., (2006), Fraud and Technology Crime: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources London: Home Office.

W.S Albrecht, G.W. Wenz and T.L. Williams, (1995), Fraud: Bringing light to the dark side of business, Burr Ridge, Il, Irwin Professional Publishing.

Web Sites:

<http://en.wikipedia.org/wiki/Fraud>

<http://www.usdoj.gov/criminal/fraud.html>

<http://www.fbi.gov/majcases/fraud/fraudschemes.htm>

<http://www.comcavre.gov.au/fraud/imu.html>

http://www.findarticles.com/p/articles/mi_m4153/is_2_61/ai_n6152654

<http://www.aic.gov.au/publications/rpp/48/index.html>

<http://www.fraudrisk.com.au/>

<http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/014.shtml>

<http://www.blackwell-synergy.com/links/doi/10.1111%2F1099-1123.00005>

<http://www.kpmg.ca/en/services/advisory/forensic/fraudRisk.html>

http://www.ey.com/global/content.nsf/International/FIDS_9th_Global_Fraud_Survey

<http://www.securityinfowatch.com/print/Security-Technology-and-Design/Management/Managing-Fraud-Risk/9327SIW2>

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=443405

<http://www.pwc.com/extweb/service.nsf/docid/81D34184EDC6A694852570CA0017743A>

http://www.belgenet.com/eko/tobb_080201_2.html

http://www.bdeglobal.com/media/documents/reducing_an_organisations.pdf

<http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146>

<http://antifraud.aicpa.org/Resources/Educators%20and%20Students/Regulatory%20Considerations/SAS%20No.%2099%20Guidance/Outline%20of%20Statement%20On%20Auditing%20Standards%20No.%2099%20Consideration%20of%20Fraud%20In%20a%20Financial%20Statement%20Au.htm>

<http://www.saydamlik.org/haber.html>

<http://bjc.oxfordjournals.org/misc/terms.shtml>

http://findarticles.com/p/articles/mi_m4153/is_2_61/ai_n6152654

http://news.com.com/Hidden+fraud+risk+in+Sarbanes-Oxley/2100-1002_3-5602776.html

http://news.com.com/Sarbanes-Oxley+cheat+sheet/2030-7349_3-5465172.html

<http://www.maxima-group.com/maxima/s-risk.shtml>

<http://stats.oecd.org/WBOS/default.aspx?DatasetCode=CSP2007>

<http://rof.oxfordjournals.org/misc/terms.shtml>

<http://www.imf.org/external/pubs/ft/reo/reorepts.aspx>

<http://www.imf.org/external/pubs/ft/reo/2005/eng/meca0905.pdf>

http://w9.gazetevatan.com/haberdetay.asp?detay=Kadinlar_sebekesinin_45_milyonluk_vur_gunu_182102_7&tarih=04.06.2008&Newsid=182102&Categoryid=7

http://www.patronlardunyasi.com/news_detail.php?id=45334

www.bbb.org/idtheft

www.checkfree.com/idprotect

www.consumer.gov/idtheft/

www.visa.com/security

www.wellsfargo.com/privacy_security/fraud_prevention/

www.idsafety.net

www.javelinstrategy.com/reports/

www.bbb.org/idtheft

www.checkfree.com/IDprotect

www.consumer.gov/idtheft/

www.visa.com/security

www.wellsfargo.com/privacy_security/fraud_prevention/

www.idsafety.net

www.cfenet.com.

www.acfe.com/documents/2006-rttn.pdf.

www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en.pdf.

APPENDIX

SPSS OUTPUT 1

CODE PART

GET DATA /TYPE=XLS

/FILE='C:\Documents and Settings\Administrator\Desktop\Kitap1.xls'

/SHEET=name 'source'

/CELLRANGE=full

/READNAMES=on

/ASSUMEDSTRWIDTH=32767.

DATASET NAME DataSet1 WINDOW=FRONT.

REGRESSION

/DESCRIPTIVES MEAN STDDEV CORR SIG N

/MISSING LISTWISE

/STATISTICS COEFF OUTS CI R ANOVA CHANGE

/CRITERIA=PIN(.05) POUT(.10)

/NOORIGIN

/DEPENDENT CPI

/METHOD=ENTER GDPperCapita .

Regression 1

Notes

Output Created		20-JUN-2008 16:24:58
Comments		
Input	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	167
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.
Syntax		REGRESSION /DESCRIPTIVES MEAN STDDEV CORR SIG N /MISSING LISTWISE /STATISTICS COEFF OUTS CI R ANOVA CHANGE /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT CPI /METHOD=ENTER GDPperCapita .
Resources	Elapsed Time	0:00:00,03
	Memory Required	1468 bytes
	Additional Memory Required for Residual Plots	0 bytes
	Processor Time	0:00:00,00

SPSS OUTPUT 2

CODE PART

GET DATA

/TYPE=XLS

/FILE='C:\Documents and Settings\mbulut.DPTDOMAIN\Desktop\SPSS 2_source.xls'

/SHEET=name 'Sheet1'

/CELLRANGE=full

/READNAMES=on

/ASSUMEDSTRWIDTH=32767.

DATASET NAME DataSet1 WINDOW=FRONT.

REGRESSION

/DESCRIPTIVES MEAN STDDEV CORR SIG N

/MISSING LISTWISE

/STATISTICS COEFF OUTS CI BCOV R ANOVA CHANGE

/CRITERIA=PIN(.05) POUT(.10)

/NOORIGIN

/DEPENDENT FPI

/METHOD=ENTER GoodGov

/RESIDUALS HIST(ZRESID) NORM(ZRESID).

Regression 2

Notes

Output Created		20-AGU-2008 17:35:58
Comments		
Input	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	175
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.
Syntax		REGRESSION /DESCRIPTIVES MEAN STDDEV CORR SIG N /MISSING LISTWISE /STATISTICS COEFF OUTS CI R ANOVA CHANGE /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT CPI /METHOD=ENTER GoodGov .
Resources	Elapsed Time	0:00:00,05
	Memory Required	1468 bytes
	Additional Memory Required for Residual Plots	0 bytes
	Processor Time	0:00:00,00