

Fatma Ulucan Özkul and Ayşe Pamukçu

---

## 2.1 Definitions of Fraud

A quick search for the meaning of fraud in the dictionary states that fraud is “deceit, impersonation with intent to deceive, criminal deception done with the intention of gaining an advantage.” The Institute of Turkish History explains the word fraud as “a deceptive trick, scam, game, artifice, cabal which is committed to cheat, mislead someone” and “contributing something useless to something in order to gain advantage” (Institute of Turkish History 1998, p 995). According to another definition, fraud is “to create a misjudgment or maintain an existing misjudgment to induce somebody to make a contract” (Arzova 2003, p 118). Another definition says “it is to enrich oneself by intentionally reducing the value/worth of an asset in secret.”

Fault is another term encountered when studying the concept of fraud. Fault is defined in the dictionary as “wrong, mistake, error,” “wrong, mistake, error committed involuntarily and unconsciously.” Fault stems from the deficiencies originated from the person or environment.

Intention is the most important element which distinguishes fraud from fault. Moreover, the person committing fraud has an objective of moral or material gain.

Debugging frauds, which are heavily committed on documents, from faults and bringing them to light is a difficult but not impossible task. Experienced auditors could detect frauds, thanks to their knowledge and experience. Fraudsters definitely leave traces, and experienced auditors could find the fraud and the fraudster by tracking traces (Arzova 2003, p 119).

---

F.U. Özkul  
Vocational College, Bahçeşehir University, İstanbul, Turkey  
e-mail: [fatma.ozkul@bahcesehir.edu.tr](mailto:fatma.ozkul@bahcesehir.edu.tr)

A. Pamukçu  
Faculty of Business Administration and Economics, Marmara University, Istanbul, Turkey  
e-mail: [apamukcu@marmara.edu.tr](mailto:apamukcu@marmara.edu.tr)

## 2.2 Types of Fraud

There are two types of fraud committed in business (Bozkurt 2003, p 2):

- Personal use of business resources
  - Drawing up financial statements of the business falsely
- Examples of frauds that employees commit to benefit themselves are given as follows (Bozkurt 2003, p 2):
- Embezzlement of the money during its collection but before it is recorded in accounts
  - Stealing the cheques of business
  - Tampering the bank records and taking monetary advantage
  - Gaining advantage through forgery of documents
  - Making payments which should not be made or previously made
  - Creating fictitious debts and having payments done in favor of oneself
  - Giving discount improperly or without authority
  - Creating ghost suppliers and having payments made in their favor
  - Inventory and scrap theft
  - Office supplies and fixed asset theft
  - Creating fictitious expenses and obtaining disbursements
  - Padding expense items
  - Benefiting from placing redundant order
  - Creating ghost employees and embezzling their wages/salaries
  - Accepting bribes from the customers and suppliers of the business with various reasons
  - Using credit cards of the business for personal objectives
  - Benefiting from overstated personal expenditures
  - Manipulating the overtime periods and obtaining extra payment
  - Benefiting from padded travel expenses
  - Selling business assets under the market value
- Objectives of financial statements fraud:
- Increasing the market value of the business
  - Making financial statements consistent with budgets
  - Obtaining unfair earnings by presenting falsely the value of the business

---

## 2.3 Statistics on Committed Frauds

Statistical information given below will give you an idea about the size of fraud:

- It is estimated that employee frauds cost businesses \$400 billion per year in the USA (Bozkurt 2003, p 1).
- Studies conducted in developed countries reveal that businesses lose 6% of their annual income due to fraudulent activities.
- It is estimated that the amount of the daily loss per person due to fraud is about \$9 in the USA.
- Research studies have shown that the amount of the loss businesses suffer because of their employees' fraudulent activities is far greater than the loss they suffer because of the customers.

- With an average of \$185,000, male employees lose four times higher than female employees (\$48,000) (Arzova 2003, p 119).
- There exists a linear correlation between the position of the employee and the losses.
- 5% of the employees is determined to commit fraud no matter what (Bozkurt 2003, p 1).
- 10% of the employees is inclined to commit fraud.
- 85% of the employees might be inclined to commit fraud under suitable conditions.

Here, attention should be paid to the third group with 85%. They will be the target mass when taking precautions against fraud (Bozkurt 2003, p 1).

---

## 2.4 Characteristic Features of the Fraudsters

Under this title, we will examine the characteristic features of people who commit or are likely to commit fraud on businesses. However, it does not imply that the person with these traits will definitely commit fraud. These characteristics should hopefully guide investigative auditors to detect the fraud.

- (a) Gender: A survey by Association of Certified Fraud Examiners (ACFE) with 2,000 fraudsters revealed many characteristics of fraudsters. According to this survey, three out of four of the people who commit fraud in businesses are male. This difference is explicit also in the monetary value of the fraud.
- (b) Marital status: It is shown that the number of married employees who attempt to commit fraud is higher than unmarried employees. With respect to the amount of fraud, the difference is 1–3. In addition, many of them have children and a happy marriage.
- (c) Education status: Generally as the level of education increases, the number and amount of the fraud also increase. The amount of the fraud is much higher, especially with employees who had received good education.
- (d) IQ level: Employees with higher IQ levels or those claiming to be so have a higher level of desire to commit fraud. The underlying reason of this situation is that this kind of people challenges the internal control structures and security systems of business they work in, and satisfies themselves by breaking through them.
- (e) Age level: Employees of any age could attempt to commit fraud, but the number and amount of the fraud are higher with older people. The number of fraud older people commit is 28 times higher than those young people commit.
- (f) Working conditions: Generally employees who come earliest and leave latest commit fraudulent activities more. Especially employees who present their unfinished jobs as an excuse and want to work alone until late hours of the night have higher probability of committing fraud. Moreover, it is estimated that many of the managers who are caught as a result of fraudulent activities do not take a leave unless they have to. The reason is predicted that they think whoever is assigned to replace them when they are away would discover and report the irregularities before their return.

- (g) Position at the business: Any person working in the business has a probability to somewhat commit fraud. However, studies indicate that with respect to the amount of fraud, employees at managerial positions are by far ahead of other employees. When employees have a trustworthy position, they are monitored less; this is considered as the underlying reason of the preceding fact. Moreover, due to their position, they are in a better position to understand the entity's internal control structures and gaps in them and are thus able to conduct fraudulent activity more easily. Unfortunately, the first reaction of many fraud victims is "I could never expect him/her to do that."
- (h) Relations outside of business: Another indicator is the level of relations employees have with third parties of the business. When an employee becomes very intimate with people buying/selling goods and services from the business, conditions become congenial for fraud to be perpetrated.

---

## 2.5 Reasons Why Employees Commit Fraud

When business frauds are analyzed, it is ascertained that three components come together when committing the white-collar crime. These are pressure, opportunity, and justification that constitute the "fraud triangle." Components of the fraud triangle are similar to the fuel, spark, and oxygen which together cause fire. When the three come together, inevitably fire breaks out (Bozkurt 2003, p 3).

### 2.5.1 Pressure Factors (Bozkurt 2003, p 4)

Pressure factors could be gathered into three groups:

- Pressures with financial content
- Pressures stemming from bad habits
- Pressures related with job

Pressures with financial contents generally show up when people are in need of cash. These pressures could be classified as below:

- Itching palm and greediness
- Desire to live well
- High amounts of personal debts
- High amounts of health expenditures
- Unexpected financial needs

The very first reason of employee fraud is that they are poor due to lower income they receive, and want to live under better conditions.

Pressures with financial content could come into view in the long term as well as in the short term. An employee who has been working in business for a number of years could commit fraud for some reason.

Studies show that on average 30% of employees conduct fraudulent activity in the first 3 years, and the remaining 70% attend to forgery processes between the 4th and 35th years of their professional life.

Pressures arising from bad habits have attributes related with pressures with financial content. Being a gambler, drug or alcohol addict, and keen on nightlife are among the several reasons causing fraud. This kind of habit is accepted as the worst kind of factors motivating fraud. There are many examples of women employees committing fraud to buy drug or alcohol for their children or husbands; or of managers who are very successful in their professional lives but commit fraud because of their gambling ambition.

Pressures related with the job could be explained as being dissatisfied with the job, the idea of an unfair attitude, not getting promoted when expected, having worked with lower wage, or not being admired by supervisors.

### 2.5.2 Opportunity Factors (Bozkurt 2003, pp 4–5)

Opportunity factors are the third component of the fraud triangle. They directly involve top management and owners of the business in particular. Providing the opportunity to commit fraud is one of the most important factors arising from frauds. Since the business could greatly influence opportunity factor, this point should receive particular attention for fraud prevention.

The control structure of the business and fraud has an inverse correlation. The most effective way of reducing employee frauds is to establish an “Internal Control System.” The important points when establishing the system are given below:

- A healthy internal control environment
- A proper accounting system
- Control procedures which operate effectively

Other factors which provide employees with the opportunity to commit fraud are as following:

- Weak moral policies
- Undisclosed contracts made with third parties and partners
- Incapability to assess the quality of the job employees performed
- Absence of a well-disciplined environment in which fraudsters will be punished
- Weakness of the information flow among employees within the business
- Ignorance, indifference, and inabilities of top management
- Lack of healthy audit works

When there is a situation where environment to punish the fraudster is absent because of the concerns such as loss of prestige and counter threat, the feeling of “you can get away with it” will be evoked among employees, thus the business will be exposed to frauds.

### 2.5.3 Efforts to Justify Fraud (Bozkurt 2003, p 5)

The third component of the fraud triangle is fraudster’s developing defense mechanisms in order to justify his/her action. Some efforts of the fraudsters to justify themselves and the excuse they made up are given below:

- (a) I had borrowed the money, I would pay back
- (b) This is in return for my efforts for the business
- (c) Nobody has suffered as a result of this
- (d) I have taken the money for a good purpose
- (e) I did not know that this was a crime
- (f) Business had deserved this
- (g) Since business evades tax, I have taken something which was already mine

At the macro-level, in order to overcome these justifying excuses, business should explain ethic rules to employees, inform them that fraudsters would definitely be penalized, establish moral code in the organization, and provide training on them.

## 2.6 Fraud Detection

Once committed, those involved in the fraudulent acts would normally find it difficult to end the habit. We could explain development process of fraud with an example as below.

Let us assume that a teller in the bank commits fraud. Some of the dates when this crime was committed are presented in Table 2.1 (Albrecht and Albrecht 2003, p 65).

When arrested, the teller made the following explanation: “I can’t believe that I could take high amounts for a long time before anyone suspected” (Albrecht and Albrecht 2003, p 68).

**Table 2.1** Development of fraud crime

April		May		June		July		August		September	
1st	10\$	1st	20\$	2nd	40\$	8th	400\$	4th	20\$	2nd	400\$
4th	20\$	5th	30\$	3rd	50\$	9th	700\$	8th	20\$	5th	100\$
7th	20\$	6th	30\$	4th	50\$	14th	400\$	11th	30\$	12th	100\$
9th	20\$	7th	20\$	5th	50\$	15th	600\$	14th	30\$	15th	200\$
10th	20\$	8th	20\$	9th	30\$	16th	600\$	19th	20\$	16th	400\$
14th	40\$	9th	30\$	10th	40\$	23rd	600\$	22th	40\$		
16th	30\$	12th	30\$	11st	30\$			26th	400\$		
22nd	30\$	13th	30\$	12th	50\$			27th	600\$		
23th	30\$	14th	30\$	13rd	50\$			28th	400\$		
24th	30\$	15th	30\$	16th	50\$						
25th	30\$	16th	40\$	17th	50\$						
28th	30\$	19th	40\$	18th	30\$						
29th	30\$	20th	40\$	20th	70\$						
30th	30\$	21st	40\$	23rd	100\$						
		22nd	20\$	24th	200\$						
		27th	30\$	25th	400\$						
		28th	40\$	26th	600\$						
		29th	40\$								

As seen from the table, the theft originally started with a very small amount but there was an increasing trend as the time progressed on. When the fraudster observed that he was not caught, he started to act more greedily and the amount taken from the safe started to increase day by day. Actually, in a 2-week period following the 23rd July, the theft stopped. The reason for that was because the auditor came to the branch and started his job. As seen from the table after the auditor had completed his task, the teller continued to the crime; this time he once again started to steal with smaller amounts. He observed the system for a short period of time to see whether the auditor could easily have spotted the theft. When he was satisfied that it might be difficult for the auditor to reveal the fraudulent activity and he might not be caught easily, he once again started to steal higher amounts (Albrecht and Albrecht 2003, p 69).

The amounts in this example are small; however, almost all fraudulent activities would normally start with small amounts, but if not discovered, it would then increase to higher amounts. If in the interim any situation were to threaten or frighten the fraudster, the theft would stop. But if that situation were to cease, the fraudulent activity would continue. It is more difficult to prevent frauds committed by top management or owners of the firm. Due to this fact, initial detection of fraud is a critical factor. For instance, the president of a New Hampshire Company had presented his employees as independent contractors. Thus, he did not pay the payroll taxes for 3 years which in total amounted to \$211,210. Moreover, he also abstained from paying indemnity fee by misinforming an insurance company about the number of people he had working for the company.

Fraud could not be prevented when committed by the owners of a small business who at the same time performed accounting duties themselves, as in our New Hampshire company example above. There would be nobody to stop the crime if the fraudsters were in fact owners of the business. In that case, what should be done is that the relevant authority should find a way of detecting the fraud.

Over time, the importance of initial detection of fraud has increased because the number of fraudulent events has increased. Detection of fraud begins with the notification of red flags which indicates that something is wrong. This might come to light as a result of trends in the number of employees, managers, and victims concerned about the loss in business assets. There are two main ways to detect frauds:

- (a) Detection by chance
- (b) Conducting a proactive research and encouraging initial identification of symptoms

Many fraudulent acts have been detected in the past by chance. Unfortunately, the incidence of fraud proceeds during detection and losses consequently increase. In many cases, people who are exposed to fraud in the organization do know that fraud was being committed, but could not bring it to light either because they are not sure and unwilling to blame someone directly or are unsure of how to go about reporting it and might also be afraid of being labeled as whistleblower.

In recent years, organizations perform a series of efforts to detect fraud. The most frequent one is establishing hotlines through which employees make

anonymous calls to draw attention to the fact that the crime is being committed. Some of these hotlines are within the organization while others are outsourced to some independent organizations. For instance, ACFE provides paid hotline service. Experience has indicated that organizations which establish these hotlines have detected many fraudulent events. However, it must be noted that there might also be false reports made to these hotlines by disgruntled employees.

Apart from the hotline, organizations also take some proactive precautions. Technological developments could be used by these organizations to analyze their databases in order to detect red flags. For instance, banks regularly utilize some software to detect fraudulent overdraft balances. These programs would be used by banks to draw attention to customers' accounts with unreasonable volume of transactions within a short period of time well before customers are aware of these fraudulent transactions. Insurance companies also use relevant software in order to identify fraudulent claims by customers immediately after taking out insurance policies (Albrecht and Albrecht 2003, pp 69–70). Research studies have supported the view that many fraudulent events are detected not by auditors but by employees and managers. For instance, the ratios of detection by different groups given in a study by Durant (2002) are depicted in Table 2.2.

According to the result of a study conducted by the ACFE in 2002, respondents were asked to explain how they detect the incidence of fraud in their companies. The results of the 532 responses received are shown in percentages in Table 2.3 (ACFE 2002, p 11).

In total, 8 exceed 100% because some participants cited more than one method for initial discovery of the frauds.

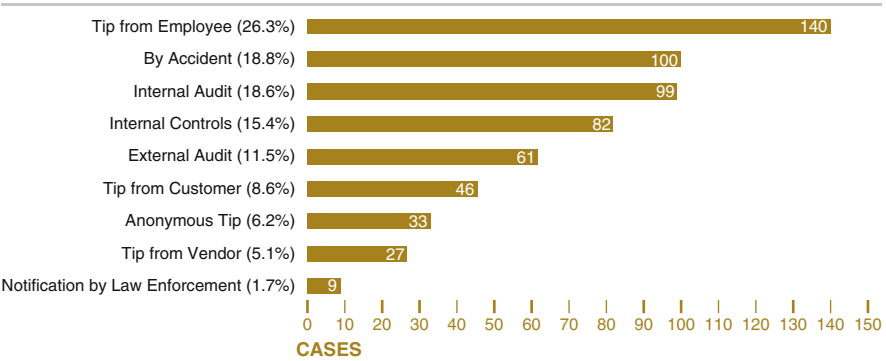
Fraud is quite a costly problem for organizations. Nevertheless, it is often the case that the person in charge of preventing fraud in most organizations is “someone” but not a particular individual(s). Independent auditors often claim that detecting fraud is not their responsibility. Internal auditors also claim that their functions are to assess controls and increase the organization's operational efficiency. Security personnel of a company would argue that in many organizations, their role is to investigate and file fraud cases in the court of law. Managers would similarly state that their main job is to manage the business, albeit fraud could be committed anywhere in the organization. Employees, despite being in the best position to detect fraud, are unsure of where and whom to refer suspected cases of fraud to when they happen; as a matter of fact, some employees believe that reporting fraud will be considered a disgrace (Albrecht and Albrecht 2003, p 68). The current model employed to fight against fraud in many organizations is shown in Fig. 2.1 (Albrecht and Albrecht 2003, p 98).

**Table 2.2** Percentage of fraud identified and reported by different groups

Management	20%
Internal auditors	25%
Employees	40%
External auditors	10%
Chance	5%



**Table 2.3** Initial detection of fraud



**Fig. 2.1** Dealing with fraud:  
current model



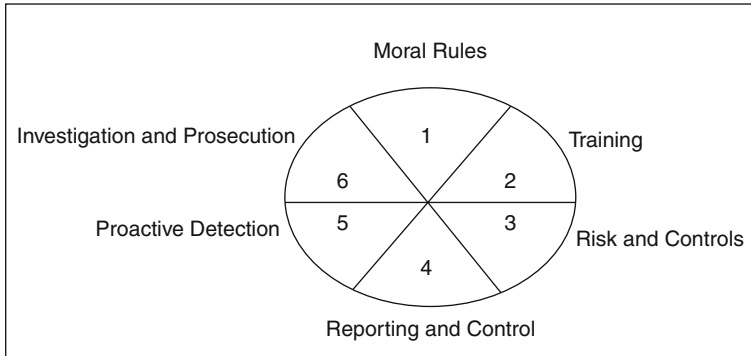
There are four stages in the model shown in Fig. 2.1. The first stage—fraud incident—raises consciousness, while training and other prevention criteria are out of question. In such an environment, fraudulent event occurs. Then the company moves to crisis mode because it wants to identify the fraudster and is too eager to prevent the event from becoming known publicly, save losses, and reduce the impact of fraud on the organization.

The second stage is the investigation stage. All security procedures and internal control are included in this stage. Much of the investigation is conducted by interviewing and document examination. The investigation might not end up with a decision but could take long time and be costly at the end of the day.

Before the third stage begins, investigation is completed and the company decides how to take action against the fraudster. There are four possible decision actions: do nothing, fire the fraudster, transfer the fraudster to another section, or fire the fraudster and start legal proceeding.

In fourth stage, the file is closed, the employee is changed, new controls are applied or not applied, and the problem is resolved.

In this model, nothing is done after this fourth stage until a new fraudulent event takes place. Fraudulent events do not decrease; they might in fact become a chronic



**Fig. 2.2** Organizations with fraud awareness reduce fraud

problem. Fraud savvy model which is a better approach in fighting against fraud is depicted in Fig. 2.2.

There are six elements in fraud savvy model. The most important element is the establishment of moral rules (Lindborg 2005). Two points are important in establishing these rules:

1. The developed rules must be embraceable by everyone working in the company
2. Creating a proper behavior model

The second element in the model is training of employees on a series of consequences of fraud and how to act when fraud is suspected. As mentioned before, what will provide benefit is not detecting or investigating but preventing the incidence of fraud (Albrecht and Albrecht 2003, p 99).

The third element in fighting against fraud includes risk assessment and a good internal control system. The important point in internal control systems is identifying where each fraud is stemming from, thus preventing possible frauds in the future from its very source.

The fourth element is the use of reporting and monitoring systems. The reporting of fraud should be facilitated. There is no doubt that murder and bank robbery are crime. However, fraud is such a crime which could continue for several years. Because hotlines and other reporting systems are not used very frequently, employees could abstain from reporting suspected frauds. Monitoring includes watching the performance of internal auditors, external auditors and managers, and audits and investigations. In companies with tight monitoring and reporting systems, fraudulent events are likely to decrease. Reporting also includes conveying the fraud-related information to the people concerned. This does not contain giving all details of fraud in local newspapers. It involves communicating the fraudulent activity to auditors, security personnel, managers, employees, and those concerned.

The fifth element is the application of proactive detection methods. No matter how good the prevention efforts are, fraud could still be committed. Since the loss

that fraud causes increases as time period gets longer, initial detection is important. Today computer software is used for initial detection of fraud.

The last element in fraud savvy model is investigation and prosecution. In investigation procedure, the following issues must be determined (Albrecht and Albrecht 2003, p 100):

1. Who will conduct the investigation?
2. How will the event be communicated to management?
3. Whether or not the law enforcing authorities should be brought in.
4. Who will determine the scope of investigation?
5. Who will determine the methods of investigation?
6. Who will trace secret information in suspected fraud?
7. Who will interview, examine documents, and undertake other stages of investigation?
8. Who will determine the company's reaction against fraud?

Doing nothing about the perpetrators should not be preferred; in contrast, taking lawsuit against the perpetrator should be preferred.

Since the 1980s in some Western countries, particularly in the USA, a new profession in the field of accounting and auditing has emerged. This profession is referred to as "forensic accounting" with its original name (Bozkurt 2000). Forensic means "pertaining to court," "being accepted as a standard in legal cases." This profession identifies a field composed of accounting, auditing, and investigative skills.

In this concept, forensic accountants provide an account analysis to determine the facts necessary to resolve a dispute before it is brought before the court or the lawsuit process takes its course. The term forensic accountant is generally used for certified public accountants (CPAs) who perform the activities of analyzing, examining, investigating, auditing, and questioning that follow an organized way in order to find the truth or reach an expert opinion by starting with the truth. Forensic accounting and litigation support involve the services provided by CPAs on legal issues (Crumbley 1995, p 25).

---

## 2.7 Forensic Accounting Definition and Literature Review

Maurice E. Peloubet is credited with developing the term forensic accounting in his 1946 essay "Forensic Accounting: Its Place in Today's Economy." By the late 1940s, forensic accounting had proven its worth during World War II; however, formalized procedures were not put in place until the 1980s when major academic studies in the field were published (Rasey 2009).

Forensic accounting is the specialty area of the accountancy profession which describes engagements that result from actual or anticipated disputes or litigation. "Forensic" means "suitable for use in a court of law," and it is to that standard and potential outcome that forensic accountants generally have to work (Crumbley et al. 2005).

Forensic accounting uses accounting, auditing, and investigative skills to conduct investigations into theft and fraud. It is listed among the top 20 careers of the future. The job of forensic accountants is to catch the perpetrators of the estimated \$600 billion theft and fraud occurring in the US companies per year. This includes tracing money laundering and identity theft activities as well as tax evasion. Insurance companies hire forensic accountants to detect insurance frauds such as arson, and law offices employ forensic accountants to identify marital assets in divorce cases (Weygandt et al. 2008, p 30).

Forensic accounting has been pivotal in the corporate agenda after the financial reporting problems which took place in some companies around the world (see, for example, Enron, Tyco, and WorldCom, just to mention a few). These scandals resulted in the loss of public trust and huge amounts of money. In order to avoid fraud and theft, and to restore the badly needed public confidence, several companies took the step to improve the infrastructure of their internal control and accounting systems drastically. It was this development which increased the importance of accountants who have chosen to specialize in forensic accounting and who are consequently referred as “forensic accountants.”

### **2.7.1 Fraud Triangle**

Forensic accounting relies on the fraud triangle to identify weak points in the business systems and find possible suspects in cases of fraud. It consists of three core concepts which together create a situation ripe for fraud: incentive, opportunity, and rationalization. People must have the incentive and opportunity to commit financial fraud, as well as the ability to justify it. Recent analysis has suggested adding a fourth concept to make a diamond—capability. Just because someone has the opportunity or incentive to steal does not necessarily mean that they have the capability to do so. For example, if someone does not understand how to make journal or ledger entries in the books of accounts, they would not know how to manipulate numbers no matter what the incentive or opportunity is (Rasey 2009).

### **2.7.2 Forensic Accounting Versus Fraud Examination**

Forensic accounting and fraud examination are different but related. Forensic accounting work is done by accountants in anticipation of litigation and can include fraud, valuation, bankruptcy, and a host of other professional services. Fraud examinations can be conducted by either accountants or non-accountants and refer only to antifraud matters (<http://www.journalofaccountancy.com/Issues/2003/Oct/TheFraudExaminers.htm>).

## 2.8 Forensic Accounting and the Accounting Profession

The accounting scandals involving Enron, WorldCom, Global Crossing, and other companies have put accountants in the public spotlight as never before in their history. After these accounting scandals, public confidence in the accounting profession has been seriously undermined. However, the scandals have created business for forensic accountants and developed opportunities for forensic and investigative accounting. Forensic accountants have been conducting these activities for quite some time in a quiet professional manner. New laws and regulations resulting from these scandals will make the role of forensic accountants more important than ever before in the business world (Sutong 2005).

Forensic accountants, also referred to as forensic auditors or investigative auditors, often have to give expert evidence at the eventual trial (Crumbley et al. 2005). All of the larger accounting firms as well as many medium-sized and boutique firms have specialist forensic accounting departments. Within these groups, there may be some further sub-specializations: some forensic accountants may, for example, just specialize in insurance claims or personal injury claims, fraud construction, or royalty audits.

Forensic accountants utilize an understanding of business information and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and investigative techniques, and litigation processes and procedures to perform their work. Forensic accountants are also increasingly playing more proactive risk reduction roles by designing and performing extended procedures as part of statutory audit, acting as advisers to audit committees, fraud deterrence engagements, and assisting in investment analyst research.

The skeptical mindset is something that has long been inherent in forensic accountants and other internal investigators when looking for evidence of fraud. The investigator historically has asked a set of questions different from those of conventional auditor, who is monitoring the financial statements to see whether they are in compliance with generally accepted accounting principles (GAAP) and thereby fairly represent the financial conditions of the company (Silverstone and Sheetz 2007).

What turns a well-trained and experienced accounting professional into a good financial investigator, however, is the knowledge of human behavior, a sixth sense for red flags, and a good intuitive feel for the significance of evidence. The skeptical mindset should raise questions about the reasonableness of all transactions and the evidence that underlies them. Since the magnitude of the amounts taken in a long-term fraud, for example, is often invisible except for a small irregularity in the accounts, the financial investigator must be curious and tenacious enough to follow up even the most initially unpromising clues. The judgments made through this skepticism will open up new hypotheses or close down old ones by testing them against the accumulating evidence until only one explanation is left. “When you have eliminated the impossible, whatever remains, however improbable, must be the truth” (Silverstone and Sheetz 2007).

Fraud auditing, forensic accounting, and/or fraud investigation (i.e., forensic accounting) put things together rather than take them apart, as is the case in financial classical auditing or modern method of systems analysis. The process of forensic accounting is also sometimes more intuitive than deductive, although both intuition and deduction play important parts. Financial auditing is more procedural in many regards and is not intended to work as effectively as the tenets of fraud auditing and forensic accounting (Singleton et al. 2006, p 43).

Traditional auditing has a focus on error identification and prevention. Prevention is the result of an effective internal control system. The auditor reviews the effectiveness of the internal control system by sampling transactions and not by a complete review of all transactions. The process can reveal errors. All errors are not considered equal. Some are important and are referred to as material. For example, omission of a million dollar loan that is not recorded in the accounting records might be a material error. Other errors are not material. An example of an error that might not be material would be an arithmetic error due to rounding that causes the reported amount to be ten dollars more or less than the actual amount. These examples are not meant to imply that there are absolute dollar amounts that denote the difference between material and not material (Gray 2008).

Fraud management involves a whole gamut of activities: early warnings and alarms; telltale symptoms and patterns of various types of fraud; profiles of users and activities; fraud detection, prevention, and avoidance; minimizing false alarms and avoiding customer dissatisfaction; estimating losses; risk analysis; surveillance and monitoring; security (of computers, data, networks, and physical facilities); data and records management; collection of evidence from data and other sources; report summaries; data visualization; links to management information systems and operation systems (such as billing and accounting); and control actions (such as prosecution, employee education and ethics programs, hotlines, and corporation with partners and law enforcement agencies) ([http://www.intelligententerprise.com/020528/509feat3\\_1.jhtml;jessionid](http://www.intelligententerprise.com/020528/509feat3_1.jhtml;jessionid)).

Forensic accounting profession has some requirements. Certified fraud examiner (CFE) is a designation awarded by the ACFE. The ACFE is a 41,000 member-based global association dedicated to providing antifraud education and training. In order to become a CFE, one must meet the following requirements:

- Be an associate member of the ACFE in good standing
- Meet minimum academic and professional requirements
- Be of high moral character
- Agree to abide by laws and code of professional ethics of the ACFE

### 2.8.1 Professional Requirements

At the time of certification, at least 2 years of professional experience in a field either directly or indirectly related to the detection or deterrence of fraud is required. The ACFE recognizes the following areas as qualified professional experience:

- Accounting and auditing
- Criminology and sociology (sociology is acceptable only if it relates to fraud)
- Fraud investigation
- Loss prevention (experience as a security guard or equivalent is not acceptable)
- Law relating to fraud

---

## 2.9 Forensic Accounting Applications Around the World

As we discussed above, accounting scandals have put the accountants under public spotlights as never before in their history. Then forensic accounting profession has gained increasing importance. Now let us look at the applications of forensic accounting in four developed economies around the globe.

### 2.9.1 United Kingdom

Over 160 cases of serious fraud with charges in excess of £100,000 came to the UK courts in the first half of this year, according to KPMG Forensic—the highest number of cases in a 6-month period in the 21-year history of its Fraud Barometer.

The cases had a total value of £636 million which, if replicated in the second half of the year, would also lead to the highest value of fraud in the Barometer's history (currently £1.2 billion in 1995). Professional gangs were the most active perpetrators of fraud, with 70 cases worth some £450 million, and their main victims were investors, who suffered to the tune of £320 million. Much of this stemmed from a £200 million investment fraud case involving the attempted fraudulent sale of the Ritz Hotel in London. Company managers were also active perpetrators, responsible for £150 million of fraud against their own employers in 32 cases. Government suffered £150 million of fraud, mostly in the form of tax and duty evasion and fraudulent benefit claims. The main victim in terms of number of cases was the financial sector. Over a quarter of fraud cases (44) were against financial institutions, with a value of £111 million.

Commenting on the figures, Hitesh Patel, partner at KPMG Forensic, said: “These figures are bad, but the worst is yet to come. It will be a number of years before the impact of the recession fully feeds through into the fraud statistics. Hard times mean more people driven to fraud by personal pressures, and more investors willing to believe in cooked up investment schemes. Companies too remain vulnerable to the threat within—their staff—as evidenced by the £150 million of fraud that managers have been tried for in the last 6 months alone” (<http://www.kpmg.co.uk/news/detail.cfm?pr=3541>).

### 2.9.2 Canada

In Canada, forensic accounting is accepted as a profession. The Certified General Accountants Association of Canada comments that they recognize that the profession of fraud investigation is relatively new and that such a duplication of effort by the CICA in developing standards for its IFA specialty is inefficient and may be confusing to the public and to fraud examiners designated by the ACFE. As such, CGA Canada supports efforts at establishing a national or international joint effort which promotes inclusion. Above all, the exposure draft process of the CICA should not be a vehicle for by which to embody these CA-IFA standards in the CICA Handbook. Choosing such an administrative method to approve these CA-IFA standards as part of the handbook circumvents the authority of the Accounting Standards Board and the Auditing and Assurance Standards Board to consider and approve applicable standards ([http://www.cga-canada.org/enca/ExposureDraftResponses/ca\\_exd\\_2006-02-23\\_ifa.pdf](http://www.cga-canada.org/enca/ExposureDraftResponses/ca_exd_2006-02-23_ifa.pdf)).

### 2.9.3 Australia

As noted earlier, the forensic accountant works within an environment that also includes government, industry, and professional regulators. The forensic accountant's work may be in conjunction with these entities or with consideration to the rules, regulations, and guidelines enforced by them. The regulator depends on the nature of the engagement. Some of the most relevant and commonly encountered regulatory bodies in **Australia** include the following (Dellaportas and Gibson 2005):

- Australian Securities and Investments Commission (ASIC): ASIC regulates companies, financial markets, and other professionals involved in finance, investments, superannuation, insurance, deposit taking, and credit. It enforces the relevant laws to protect the public, in conjunction with other regulators and investors and consumer protection groups.
- Australian Tax Office (ATO): The ATO administers and enforces legislation relating to taxation, superannuation, and excise. Of particular relevance to the forensic accountant, the ATO watches for the effects of aggressive tax planning, tax evasion, and persistent tax debtors. All of these could lead the ATO to take action either in or out of court.
- Financial Action Task Force (FATF): The FATF is an intergovernmental body formed to develop and promote national and international policies on combating money laundering and terrorist financing. The FATF issued a document entitled *Forty Recommendations: a global framework for combating money laundering*, in 1990, and eight special recommendations on terrorist financing following 11 September 2001.

Other notable regulators interacting with the forensic accountant's work include professional organizations such as CPA and ICAAA, as well as specialist bodies such as APRA and AUSTRAC, to name but a few. Whenever the forensic expert



undertakes an assignment, he or she needs to consider if there is a regulator relevant to this work, and the impact of that relationship on the work to be performed.

The work of Australian Federal Police (AFP), state and specialist police, or government task forces also includes areas in common with the forensic accountant. For example, the AFP's current focus includes dealing with major fraud or money laundering. A forensic investigation of corporation may uncover significant fraud or misconduct such that the corporation decides to involve the police to pursue a criminal prosecution, or it may be that the forensic accountant's investigation takes place concurrently with the ongoing police inquiries.

In addition, Australia is one of the most important countries which have educational program in forensic accounting in graduate degree. The master of forensic accounting emphasizes a forensic rather than a control-based or risk management approach to the analysis of corporate governance and the possibility of fraud, other forms of misconduct, abuse, and corruption. Both courses build on the expertise acquired in undergraduate and postgraduate studies and/or business experience in the areas of corporate regulation, corporate governance and ethics, financial accounting and audit, and finance and banking and management (<http://www.uow.edu.au/commerce/accy/current/UOW010315.html>).

## 2.9.4 The United States of America

On 30 July 2002, the landmark legislation known as the Sarbanes-Oxley Act (SOX Law) was enacted into the United States Law. The Act was named after its principal authors, Senator Paul D. Sarbanes (D-Md) and Rep. Michael G Oxley. The Act seeks to restore investor confidence in the US financial markets, corporate governance, and financial reporting.

The Sarbanes-Oxley Act was passed by the US legislature in the wake of accounting scandals such as Enron, WorldCom, and Xerox, all of which seriously undermined investor confidence. Through strictly United States legislation and its impact is far reaching on the accounting and financial markets. The Act applies to all Securities and Exchange Commission (SEC)-listed companies, and so extends to subsidiary and associated entities of SEC-listed companies outside the USA.

The Enron and WorldCom scandals highlighted the role of the auditor in ensuring the integrity of financial reporting, and in particular, the auditor, as an independent and objective professional. The Act prohibits professional accounting firms from providing non-audit services to audit clients, with the exception of tax services and specialist management advice. Non-audit services specifically include appraisal or valuation services, and fairness opinions that are traditionally the work of the forensic accountant. Investigation services, often related to audit issues, are not prohibited unless there is a requirement to provide court testimony.

The impact of the requirements of Sarbanes-Oxley is that forensic practices must seek work outside such traditional sources as existing audit clients, although this potentially opens up avenues into other clients. In turn, clients may lose benefits of

the inherent in-house knowledge and experience obtained from the audit engagement, but they may also benefit from a different expert, as perspective.

However, in so far as the nature and performance of the audit engagement were seen to threaten the forensic accountant as independence, the Sarbanes-Oxley provisions go some way to enforcing and promoting objectivity and restoring the accounting professions' reputation (Dellaportas and Gibson 2005).

In the USA, forensic accountants have been employed by the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Internal Revenue Service (IRS), Federal Trade Commission (FTC), Homeland Security, Bureau of Alcohol, Tobacco and Firearms, Governmental Accountability Office (GAO), and other government agencies. The focus is on what is referred to as *white-collar crime*, notably *fraud*. This is why financial and other skills are required. Outside of government employment, big employers of forensic accountants include financial intermediaries such as banks and insurance organizations plus divorce attorneys. Forensic accountants often testify in civil and criminal court hearings. In this capacity, they serve as expert witnesses. They do not testify as to whether fraud has occurred. This is the court's decision. The expert witness presents evidence. Forensic accountants have a number of organizations that support their work. Here is the list of key organizations that support forensic accountants' work along with the URL to access them: ACFE (<http://acfe.com>); American College of Forensic Examiners (<http://www.acfei.com>); Association of Certified Fraud Specialists (<http://www.acfsnet.org>); National Litigation Support Services Association (<http://www.nlssa.com>); National Association of Certified Valuation Analysts (<http://www.nacva.com>); American Institute of Certified Public Accountants (<http://www.aicpa.org>); and The Institute of Business Appraisers (<http://www.go-iba.org>) (Gray 2008).

The US Government Accountability Office (GAO) is encouraging people to use its FraudNet system to report waste, fraud, abuse, or mismanagement related to funds distributed under the American Recovery and Reinvestment Act of 2009. The \$787 billion stimulus act was signed by President Obama on 17 February.

FraudNet is an e-mail, phone, and fax hotline that processes allegations about federal agencies and federally funded programs. Tips may be provided anonymously, and the GAO keeps all inquiries confidential. The GAO may refer allegations for follow-up to its own investigative units, appropriate inspector general offices, or to the Justice Department.

"The Recovery Act has set aside billions of dollars to create jobs, invest in infrastructure, and fund other measures to counter the current economic downturn. Experience tells us that the risk of fraud and abuse grows when large sums are spent quickly, eligibility requirements are being established or changed, and new programs created," Gene L. Dodaro, acting comptroller general of the United States and head of the GAO, said in a press release.

Below you can see the statistics about fraudulent activities in the USA:

1. Even small businesses that have been victims of employee fraud are failing to put proper systems in place to prevent future occurrences, according to a Sage Software survey conducted by M/A/R/C Research. The findings suggest that

proper use of accounting software may be a valuable weapon in a company's fraud prevention arsenal.

The survey found that 21% of small businesses did not have a system in place to prevent employee fraud and another 13% did not know whether they did or not. Furthermore, almost a quarter of companies which have suffered fraud losses in the past have still not established preventive measures. Twenty-eight percent of small businesses that responded to the survey said they had been victimized at some time by employee fraud.

Of the respondents that had internal control systems in place to prevent fraud, 47% were using their accounting software as a fraud prevention tool ([http://www.journalofaccountancy.com/Issues/2008/Oct/High\\_Tech\\_Fraud\\_Prevention.htm](http://www.journalofaccountancy.com/Issues/2008/Oct/High_Tech_Fraud_Prevention.htm)).

2. The Financial Crimes Enforcement Network (FinCEN) released a report that showed that subjects of mortgage loan fraud (MLF) suspicious activity reports (SARs) were the subjects of SARs related to other activities—including check fraud, securities fraud, and foreign wire transfers to Nigeria—at higher rates than the overall incidence of those SAR types.

The study, MLF connections with other financial crimes, examines the activities of people reported in depository institution SARs for MLF between July 2003 and June 2008, by evaluating SARs filed by money services businesses (SAR-MSB), securities brokers and dealers of insurance companies (SAR-SF), and casinos and card clubs (SAR-C).

The report said:

- Securities fraud was identified in 23% of SAR-SFs reporting MLF subjects, compared with 16% of all SAR-SFs in the same 5-year period.
- Approximately 70% of the examined SAR-MSBs described suspicious wire transfers by MLF subjects; 34% of those reports described transfers to foreign countries by MLF subjects. Nigeria was the most frequently reported destination of those funds, accounting for 10% of MLF subject activity reported in SAR-MSBs. In contrast, wire transfers to Nigeria reported in all SAR-MSBs represented only 3% of activity.
- In SAR-SFs, FinCEN found an unusually high number of reports of suspicious documents, fraudulent identifications, and forgery among MLF subjects.
- Check fraud by MLF subjects was reported in the SAR-Cs at an unusually high level, 17%—compared with only 3% of all SAR-Cs during the same 5-year period.

FinCEN also released Advisory FIN-2009-A001 to highlight red flags that are potential indicators of loan modification/foreclosure rescue scams. The advisory notes that the red flags only show possible indications of fraud. Some of the red flags include a homeowner making payments to a third party other than the mortgage holder or servicer; the so-called foreclosure specialist charging an upfront fee; the homeowner being pressured to sign paperwork he or she did not have an opportunity to read and did not thoroughly understand; the foreclosure specialist giving a guarantee that the home would be saved “no matter what”;

and the foreclosure specialist falsely claiming to be affiliated with the government (<http://www.journalofaccountancy.com/Issues/2009/Jun/Fraud>).

3. The Deloitte Forensic Center analyzed and reported on hundreds of SEC Accounting and Auditing Enforcement Releases (AAERs) issued from January 2000 through December 2007. The results of the analysis were compiled in the report **Ten Things About Financial Statement Fraud**—Second Edition, released in December of 2008. Among the findings:

From 2000 to 2007, the SEC issued 383 financial statement fraud AAERs relating to registered companies. In the years following the Enron and WorldCom collapses, the number of AAERs issued more than doubled from 35 in 2000 to 75 in 2003. The number has since fallen to fewer than 50 per year, beginning in 2005.

The analysts identified 1,403 alleged fraud schemes in the 383 financial statement AAERs used in the study. (A single release often identifies multiple, simultaneous schemes operating in a company.) The average number of fraud schemes identified per AAER increased to an average 4.2 in 2007, up from 2.7 in 2000.

Revenue recognition fraud schemes were the most common type, at 38% of the total. Five types of manipulation schemes (A/R, assets, expenses, liabilities, and reserves) combined to make up another 38% of the total types of schemes. Rounding out the list were improper disclosures (11%), asset misappropriation (4%), bribery and kickbacks (4%), investments (2%), aiding and abetting (2%), and goodwill (1%).

Of the 1,403 schemes identified in the AAERs studied, two industries accounted for two-thirds of the total schemes identified: technology, media, and telecommunications (37%) and consumer business (29%) (<http://www.journalofaccountancy.com/Issues/2009/May/StateofSchemes>).

4. SARs for suspected mortgage fraud increased 44% in the 12-month period ending June 30, 2008, according to Filing Trends in MLF, a report compiled by the FinCEN. In the most recent reporting period, financial institutions filed 62,084 SARs relating to mortgage fraud compared with 43,054 filings in the period between July 1, 2006, and June 30, 2007 (<http://www.journalofaccountancy.com/Issues/2009/May/Fraud>).

FinCEN proposed revised rules and new guidance that would permit certain affiliates of depository institutions as well as broker-dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities to share SARs within a corporate organizational structure for purposes consistent with the BSA. FinCEN said it is seeking comment on whether the guidance should apply to other financial institutions in addition to the aforementioned ones.

Consistent with the BSA's purposes of promoting financial institutions' efforts to detect and report money laundering and terrorist financing, as well as ensuring the confidentiality of a SAR or any information that would reveal the existence of a SAR, the proposed rules and guidance permit the aforementioned financial institutions to share a SAR, or information that would reveal the existence of the

SAR, with an affiliate provided that the affiliate is subject to a SAR regulation issued by FinCEN or the Federal Banking Agencies. FinCEN believes the proposed changes will benefit industry by:

- Helping financial institutions better facilitate compliance with the applicable requirements of the BSA and more effectively implement enterprise-wide risk management.
- Helping financial institutions assess risks based on information regarding suspicious transactions taking place through other affiliates or lines of business within their corporate organizational structures.
- Enabling a filing institution to share the SAR with certain affiliates, thus eliminating the present need to create a separate summary document which has to be crafted carefully to avoid revealing the existence of the SAR itself.

---

### Conclusion

In recent years, corruption in the US companies has attracted the attention on fraud in many US organizations. Detection and prevention of corruption have given rise to the profession of forensic accounting. Forensic accounting, which has been growing rapidly as a profession in the world and has been accepted as a profession in countries such as Canada, Australia, the USA, and the UK, is beginning to gain the importance that it deserves.

The traditional auditor was following a reactive approach during the audit process. Now we see that proactive approaches have begun to replace the reactive solutions. Once the loss has occurred, neither detection nor investigation could compensate the loss. In fact, these procedures would also cost business a large sum of money. Due to this fact, the most important thing companies have to do with regard to fraud is to prevent the crime from being committed. To prevent the crime, two concepts move to the top of the corporate agenda: deterrence and motivation. Rules, regulations, and legislation play deterrence role, while motivation is provided with education and training.

The landmark legislation Sarbanes-Oxley Law has significantly contributed and consolidated the effectiveness of the code of ethics and moral standards in the organizations. Countries enact and adopt new regulations as the need arises as a result of corruptions, fraud, and bankruptcies due to unethical applications on the part of corporate entities.

Rules and legislations are one side of the issue. In order to have a solid and strong fight against fraud and other wrongdoings in the companies, employees should be trained. Here, forensic accountant comes first as the person primarily in charge of identification, investigation, and detection of fraud. Therefore, it will be meaningful for corporations to contribute authority and capabilities of the forensic accountant. Besides, related institutions should provide a good and sound theoretical education to raise awareness about the role of forensic accountants.

Australia is a good example from all of the aspects we mentioned above. They have many institutions which collaborate together in the fight against the crime. Moreover, higher institutions in the country offer graduate and postgraduate

courses on forensic accounting. As a result of these factors, the amount of loss due to fraud is by far less in Australia than in the USA and UK. As we mentioned, US loses \$600 billion per year, and a study by KPMG says that the figure for the UK is roughly about £200,000 per year, while the figure for Australia is \$4.5 billion (AUD).

In conclusion, forensic accounting will no doubt be one of the best careers of the future. As in the case of Australia, other countries and companies in other parts of the world should make material and moral investments for this profession, in order to ensure that individuals, corporations, all of an economy sectors, government departments, and countries are protected and consequently the entire world would be a better place for all.

---

## References

- Albrecht WS, Albrecht CO (2003) Fraud examination. South-Western, Mason, OH, s.65
- Arzova SB (2003) İşletmelerde Çalışanlar Tarafından Yapılan Hilelerin Kırmızı Bayraklar Yoluyla İzlenmesi. MUFAD Dergisi, Avcıol Press, vol 20, October 2003
- Bozkurt N (2000) Muhasebe ve Denetim Mesleğinde Yeni Bir Alan “Adli Muhasebecilik” Yaklaşım, vol 94, p 56, Oct 2000
- Bozkurt N (2003) Çalışanların Yaptıkları Yolsuzluklar, Bunların Ortaya Çıkarılması ve Önlenmesi, p 2. <http://www.itkib.org.tr/hedef/200203mart/arastirma1.html>. Accessed 1 Nov 2003
- Crumpley DL (1995) Forensic accountants appearing in the literature. New Accountant 10(7):25
- Crumpley DL, Heitger LE, Smith GS (2005) Forensic and investigative accounting. CCH Group, Chicago, IL
- Dellaportas S, Gibson K (2005) Ethics, governance and accountability professional perspective. John Wiley & Sons Australia Ltd., Australia
- Durant A (2002) <http://www.acfe.com/fraud/view.asp?ArticleID=307> ACFE, 2002, p 1
- Fraud. <http://www.journalofaccountancy.com/Issues/2009/Jun/Fraud>
- Fraud. <http://www.journalofaccountancy.com/Issues/2009/May/Fraud>. Accessed 7 Aug
- Gray D (2008) Forensic accounting and auditing: compared and contrasted to traditional accounting and auditing. In: ABR & TLC Conference Proceedings, 2008, USA. High-Tech Fraud Prevention [http://www.journalofaccountancy.com/Issues/2008/Oct/High\\_Tech\\_Fraud\\_Prevention](http://www.journalofaccountancy.com/Issues/2008/Oct/High_Tech_Fraud_Prevention)
- [http://www.cgacanada.org/enca/ExposureDraftResponses/ca\\_exd\\_2006-02-23\\_ifa.pdf](http://www.cgacanada.org/enca/ExposureDraftResponses/ca_exd_2006-02-23_ifa.pdf)
- <http://www.uow.edu.au/commerce/accy/current/UOW010315.html>
- [http://www.intelligententerprise.com/020528/509feat3\\_1.jhtml;jessionid](http://www.intelligententerprise.com/020528/509feat3_1.jhtml;jessionid)
- Institute of Turkish History (1998) Turkish dictionary, vol 1. Institute of Turkish History Press House, Ankara
- Lindborg H (2005) Tone at the top: value added auditing for leadership. <http://www.leanscm.net/Articles%20%20September%20%20October%2003/Team%20Management.htm>. Accessed 4 Dec 2005
- Rasey M (2009) History of forensic accounting, 30 June 2009. [http://www.ehow.com/about\\_5005763\\_history-forensic-accounting.html](http://www.ehow.com/about_5005763_history-forensic-accounting.html)
- Silverstone H, Sheetz M (2007) Forensic accounting and fraud investigation for non-experts, 2nd edn. Wiley, New York, NY, p 62
- Singleton T, Singleton A, Bologna J, Lindquist RJ (2006) Fraud auditing and forensic accounting, 3rd edn. Wiley, Toronto, ON

- Sutong Z (2005) Forensic accounting in the “big four”: a survey from their websites. *J Modern Acc Audit* 1(7). <http://www.accountant.org.cn/doc/acc200512/acc20051204.pdf>. Accessed 7 Aug 2009
- The Fraud Examiners. <http://www.journalofaccountancy.com/Issues/2003/Oct/TheFraudExaminers.htm>. Accessed 7 Aug 2009
- The state of schemes, ten things about financial statement fraud, 2nd edn. Deloitte Forensic Center, <http://www.journalofaccountancy.com/Issues/2009/May/StateofSchemes>
- Weygandt JJ, Kieso DE, Kimmel PD (2008) *Accounting principles*, 8th edn. Wiley, p 30. <http://www.kpmg.co.uk/news/detail.cfm?pr=3541>. Accessed 5 Aug 2009

Emerging Fraud

Fraud Cases from Emerging Economies

Caliyurt, K.; Idowu, S.O. (Eds.)

2012, XXVI, 186 p., Hardcover

ISBN: 978-3-642-20825-6