



President:	Dato' Akhbar Satar, CFE, AIMB
Vice President:	Mr. Yunus Bin Yusop, MIBM
Secretary:	Mr. Aaron Lau, CFE
Assistant Secretary:	Ms. Helen Quat, CFE
Treasurer:	Mr. M. Kanakaraja, CFE
Training Director:	Mr. Lee Long How, CFE
Council Members:	Dr. Jon Tay
	Mr. Khairuzzaman Khan
	Mr. Balachandar
	Ms. Loh Siew Yuen

We are the largest anti-fraud organization and premier provider of anti-fraud training and education.

[Details and Benefits — CFE Membership](#)

Certified Fraud Examiner (CFE) Membership is open to associate members who are interested in taking their career to the next level by earning the standard of professional excellence in the anti-fraud profession. The CFE credential is increasingly being designated as a preferred credential in the hiring practices of businesses, government entities and law enforcement agencies.

The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 50,000 members, the ACFE is reducing business fraud world-wide and inspiring public confidence in the integrity and objectivity within

Content

- Fraud During A Recession
- Issues Faced in Forensic Accounting Education
- Fraud on The Net

Fraud During A Recession

Fraud increases during economic slowdowns for a number of reasons. Individuals under stress are more likely to do things that they would not normally do during normal times, from outright theft of company assets such as cash, fixed assets and intellectual property to fraudulent acts to enhance job security. Unhappy employees may seek revenge. Distributors and suppliers are more likely to seek unfair advantage to boost their businesses and may conspire with procurement or sales departments (Hawke 2009, p.34).

When times are good, companies tend to concentrate on generating profits and many types of fraud like those involving marketing, advertising, travel, entertainment, and procurement are easy to hide. During hard times, management focus more on expenses and on operations thus discovering more fraud and non-compliance as a result. As staff are retrenched or relocated, more fraud is uncovered.

Most fraud examiners would say that crime requires motive, opportunity and self-rationalisation. During difficult times, stresses build and normally rule abiding people are tempted to stray. Individuals with high lifestyles are tempted to break rules. Senior executives, motivated by selfish urges to save the firm and preserve jobs, may be tempted to cook the books which leads to serious financial, legal and reputational consequences (Hawke 2009).

We start by mentioning about sales and marketing fraud which comprises of kickbacks or illegal commissions, parallel non-approved sales channels, and theft of customer information. 'On a grander scale, a company may inflate its sales by creating a separate "trading" business that books sales to shell companies established by connected parties. The enhanced performance of the company leads to increased financing with additional debtors, creditors and inventories that has to be financed, some of which can be siphoned off. These actions defraud the firm by falsely expanding it' (Hawke 2009, p. 35).

Secondly, there is procurement fraud which means not only theft of product and supplier information but also supplier "commissions" paid to purchasing staff. It can be in the form of monetary or non-monetary inducements. 'Dummy companies sometimes provide dummy products and services or buy real products and services through dubious agents, who are sometimes related to the purchasing officer' (Hawke 2009).

Third is product development and R&D fraud, which comprises of the theft of IP. The speed with which IP can be converted to a marketable product or the first move status gained is destroyed by IP leakage.

Fourth, is fraud occurring in warehousing where there is theft and sale of products mostly attributable to poor warehousing supervision.

Fifth, is finance and accounting fraud where documents are falsified or the occurrence of value added tax fraud and embezzlement.

Sometimes, top executives are accountable for fraud. Senior executives sometimes perpetrate the most damaging frauds because of the power that they hold. Their position in the firm makes them resist monitoring and detection of any non-compliance. 'To be effective, antifraud efforts must cover top executives' (Hawke 2009).

Finally, as more IP and other private data is stored in digital format and communicated over the Net, the risk of theft and leakage via the IT system grows and can become a problem.

Hawke (2009) states 8 steps to avoid fraud. We start by making it clear that senior management takes compliance seriously. Delegation of compliance down the organisation hierarchy does not mean that perceived responsibility is shirked. Second, encourage a small-company atmosphere within the organisation which encourages trust and loyalty, managers must take an interest in the lives of their employees and organise bonding activities outside work.

Third, compliance materials should be communicated pervasively and acknowledged by all employees. Activities like role playing emphasize that compliance is imperative in the survivability of the company as well as the maintenance of employment. Fourth, IP protection should not only encompass product aspects but also business information and trade secrets such as vendor and customer lists which when lost can be disastrous.

IP protection should be internal. Since the sharing of information contributes to innovation, this sharing must be facilitated by loyal employees. Creating this sense of loyalty can be a challenge especially in Asian corporate environments.

Next, conduct due diligence on new hires especially if they are going to use proprietary information. Background checks done on new recruits should be done. It is also important to review employment contracts with local employment and labour law.

Finally, establish a corporation wide whistle blowing campaign and take it seriously. Outside investigators like fraud examiners may be brought in to evaluate evidence of whistle blowers.

Reference

Hawke, F. (2009). Fraud in Hard Times. *Chinabusinessreview.com* September-October 2009: 34-37.

Issues Faced in Forensic Accounting Education

Current push in accounting education is the creation of basic knowledge for future accountants on which life long learning and knowledge application is built. Forensic accounting is an emerging area especially in light of fraud detection. Results of a study by Rezaee & Burton (1997) showed that forensic accounting education has several benefits but also were faced with problems such as lack of faculty interest, lack of resources, and lack of flexibility in curriculum.

There should be an integration of forensic accounting into accounting curricula but there were differences in opinion between CFEs and academicians. CFEs preferred offering a separate course in forensic accounting while academicians favored integration of forensic accounting topics throughout all accounting and auditing courses. Both groups agreed that present accounting syllabus is not responsive to society's demand for forensic accounting and that future curriculum should include forensic accounting training.

Modules in forensic accounting for courses could include investigation and the law, fraud and fraud auditing, financial reporting process and finally ethics.

Reference

Rezaee, Z. & Burton, E. J. (1997). Forensic accounting education: insights from academicians and certified fraud examiner practitioners. *Managerial Auditing Journal*. 12/9. 479-489.

Fraud on The Net

Baker (1999) examined the question of fraud on the Internet and looked at three areas comprising of securities fraud, fraud in electronic commerce and fraud arising from the rapid growth of Internet firms.

The SEC (U.S.) has pointed out a number of individuals for committing securities violations on the Net. Activities prohibited under US law are being conducted through the Internet and the SEC is taking action to reduce these activities. Examples of securities fraud are stock price manipulation and non-existing investments.

Secondly, fraud on the Internet lies within the vicinity of electronic commerce. The growth of electronic commerce and the desire by consumers to feel secure has led to the creation of a WebTrust that uses logo assurance services and other forms of encryption techniques, which may help to reduce concerns about fraudulent use of data. Examples of fraud in electronic commerce are the misuse of information and non-existent products.

Third, fraud has occurred due to the rapid growth of Internet companies, often based on little economic substance and without traditional management and internal controls. In other words, the fundamentals are weak. Examples of fraud in Internet companies are due to lack of controls and non-existent earnings, sales or assets.

The expansion of Internet Commerce is a development that is perceived to be beneficial for society. Thus, it is important that fraud on the Internet be combated (Baker 1999).

Reference

Baker, C. R. (1999). An analysis of fraud on the Internet. *Internet Research: Electronic Networking Applications and Policy*. Vol: 9. 5. 1999. 348-359.