FRAUD, CORRUPTION IN THE PRIVATE SECTOR AND INTERNAL CONTROL QUALITY

Luminiţa IONESCU, Assoc. Prof. Ph.D.
Faculty of Financial and Accounting Management
Spiru Haret University

Abstract

The global economic crunch had a big impact on the private sector all over the world. Media and controllers presented cases of corruption in business and identified special areas where companies, governments, investors, consumers and stakeholders can contribute to stop fraud and corruption. Controllers and auditors are rebuilding public trust in the accounting profession, in order to provide high-quality training, regulation, specialist knowledge and professional advice.

Fraud and corruption are strongly connected in the private sector and the level of corruption in the last few years remains very high, despite the efforts of governments to reduce it. It is well known that local and multinational companies are paying bribes in order to win public contracts or benefits. The level of fraud became very high during the economic crunch, due to the globalization and expansion of computer systems. All the data is on-line on the computer systems and has became very vulnerable. Thus, the governments are becoming more interested in securing the computer information and financial data.

Key-words: *fraud, corruption, internal control, business risks, control framework*

JEL Classification: H_{83}, M_{41}, M_{42}

Introduction

We propose in this paper a concise overview of fraud, corruption and internal control for the private sector. Fraud and corruption became more and more common in the economic crunch and people are concerned about identifying methods to eradicate fraud. Although fraud and corruption cannot be fully eradicated, there are some strategies to prevent fraud and to minimize corruption. Based on the controller's experience many companies can do a better job of identifying fraud risks and managing them. In addition to preventing some occurrences of fraud, companies can minimize the damaging effects of fraudulent events and curtail their impact on the corporation.[1] This research is relevant to the fraud and controlling sector because fraud and corruption could be prevented by

[1] Bishop, T. and Hydoski, F. (2009), *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, John Wiley & Sons, Inc., Hoboken, New Jersey, p. 21.

internal control quality. Many business people and controllers are successful in discovering fraud and explaining the mechanism of fraud and corruption in the economic crunch.

The aim of this paper is to present how fraud has grown in the last few years and how the economic crunch has facilitated the fraud context. Corruption is related to fraud and more people are becoming involved in scams and fraudulent techniques. "With respect to fraud and corruption, we believe resiliency means a combination of avoiding problems through appropriate planning and risk management, reducing vulnerabilities such as by using early warning systems, and limiting impact by establishing processes that help effect a quick return to business."[2]

Literature review

The paper has based its conclusions on the findings of the most recent papers in this area:

Bishop, T. and Hydoski, F. (2009), *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, who presented the fraud and corruption consequences and a chain reaction resulting in serious corporate harm or failure. They explained how in addition to reducing profits, fraud can lead to a host of other negative consequences, including losses of reputation, customer support, access to capital, brand power, market position, competitive advantage, momentum, innovation, and talent. The same consequences could be found in discussing corruption.

Bryan, K. et al. (2009) in *Cyber Fraud. Tactics, Techniques, and Procedures*, presented the Cyber Fraud: principles, trends, and mitigation techniques, with an extensive survey of the structure and dynamics of both the practice of cyber fraud and the underground community that commits it. They explained the Russian and Brazilian cyber threat environments, with care taken to balance the comparative power of apt generalizations with the specific familiarity available only in an abundance of rich detail. "Within the past 4 years, cyber crime has evolved from a minor nuisance to a major concern involving well-organized actors and highly sophisticated organizations. Simplifying the operations of the cyber criminal helps provide perspective into the general incentives and risks the fraudsters face and, therefore, into their behavioural patterns. Moreover, such understanding is also helpful in determining expenditure on countermeasures and crafting tactics to disrupt the fraud underground."[3]

COSO (2006), *Internal Control over Financial Reporting. Guidance for Smaller Public Companies*, is an important study to understand internal control. Thus, the characteristics of smaller companies provide significant challenges for cost-effective internal control. "Among the challenges are: obtaining sufficient

[2] Bishop, T. and Hydoski, F. (2009), *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, John Wiley & Sons, Inc., Hoboken, New Jersey, p. 21.

[3] Bryan, K et al. (2009), *Cyber Fraud. Tactics, Techniques, and Procedures*, CRC Press, Taylor&Francis Group.

resources to achieve adequate segregation of duties; management's ability to dominate activities, with significant opportunities for management override of control; recruiting individuals with requisite financial reporting and other expertise to serve effectively on the board of directors and audit committee; recruiting and retaining personnel with sufficient experience and skill in accounting and financial reporting; taking management attention from running the business in order to provide sufficient focus on accounting and financial reporting".

Ronald J. Burke and Cary L. Cooper (2009) in *Research Companion to Corruption in Organization* presented causes, consequences and choices to corruption situations. "Individuals are likely to participate in corrupt behaviour or turn a blind eye towards it in order to fit into or belong to the organization, and if they strongly identify with the organization. Organizations with a short-term financial emphasis were more likely to exhibit corrupt behaviours, and in particular, pay and incentive systems were more likely to foster corrupt practices."

Fraud, corruption and internal control in the private sector

Bishop, T. and Hydoski, F. empirically examined fraud considering it as the tip of the iceberg. "Since the *Crash of 2008* led to economic conditions softening dramatically around the globe, fraud risks for businesses appear to be on the rise. A slowing economy may increase pressure on corporate executives to meet performance goals set in rosier times, or to demonstrate that the current executive team should be retained by shareholders. Individual managers may feel a much greater risk of job loss than usual, potentially making them eager to avoid having to report a performance shortfall in their operating unit.

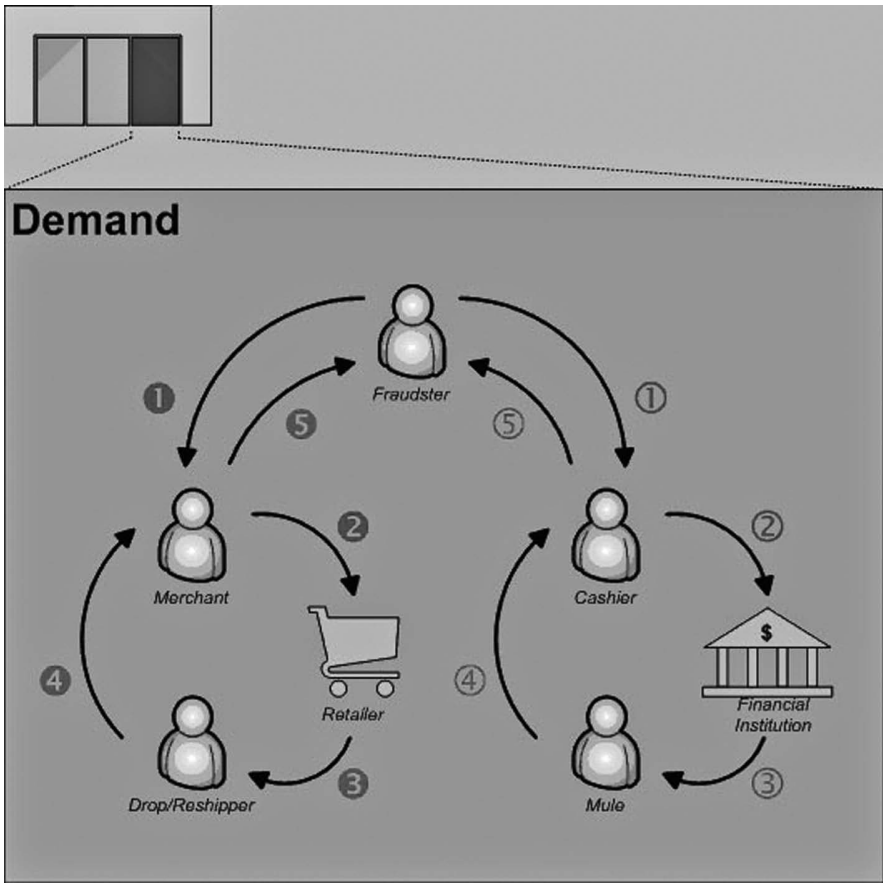
At the same time, employees may be under greater personal financial pressure, whether due to potential foreclosure on their home, the loss of a spouse' s income due to layoffs, or other impacts of the economic downturn." [4]

In early 2008, the UK's Financial Services Authority published its annual Financial Risk Outlook in which it stated that, "Tighter economic conditions could increase the incidence or discovery of some types of financial crime or lead to firms' resources being diverted away from tackling financial crime."

Bishop and Hydoski explained how managing the risk of fraud and corruption became very important for any organization: "Managing the risk of fraud and corruption requires an ongoing commitment to acquiring fresh knowledge and putting it to work. Quite often this fresh knowledge must be obtained from outside your company. Organized criminal groups constantly evolve new fraud schemes to part companies from their money. Customer and vendor frauds develop new twists, taking advantage of new technologies." They suggested that "the danger of fraud has been amplified by the ability of fraudsters to leverage modern technologies such as computers and the Internet. Conversely, the ability of companies to monitor business processes for potential fraud and to respond quickly when fraud events occur has been greatly enhanced by the availability of technologies such as anti-money laundering (AML) software, advanced analytics, and enterprise financial management systems." [5]

Bryan, K. et *al*. presented the most common fraud in the economic crunch: the cyber fraud.

"Because cyber criminals find easy success in targeting consumers and retail banks, they, until quite recently, have had few incentives to expand their activities; this is changing. Stock manipulation through compromised accounts is gaining in popularity, indicating that the more competent fraudsters are becoming more capable and knowledgeable. Others are finding ways to "cash out" accounts that would previously have been too large (therefore salient) to use once stolen. As a result, brokerage and retirement accounts are new favorites in the fraud underground. Trojan toolkits are rapidly outstripping phishing, and the relatively new threat of harming is maturing into an almost invincible attack vector." [6]



Source: **(**Bryan, K et al. (2009), *Cyber Fraud. Tactics, Techniques, and Procedures*, CRC Press, Taylor&Francis Group, p. 25).

Fig. 1. *Model of a cash-out process*

Bryan, K. et *al*. developed a model of fraud. "Like any other market, the carding underground consists of some resource input (here, account credentials) that is extracted and processed by suppliers (usually phishers), brought to market and retailed by middlemen (carding forum leaders), and finally purchased and consumed by the demand pool (end-user carders). Also reflected in the model shown in Figure 1 are the economic categories of wholesalers, retailers, and independent contractors who provide specialized services to create additional value. In fact, the only serious departure of this model from traditional economic models is the fact that incurring risk (through possession or transmission of illegally held data) is a pervasive source of value." [7] The model of fraud explains the process by which criminals are able to translate the stolen credentials into valid currency, or in some cases merchandise, is illustrated in Figure 1.

Bryan, K. et *al*. presented some variants of "cashing out", but the two most prominent utilize either a "money mule" or a reshipper. In many instances, individuals recruited as reshippers act as money mules after establishing trust, but before the reshipper or mule becomes a victim him- or herself. They explained the steps to perform a scam like that:

1. The fraudster contracts a cashier to perform the financial transaction. The cashier or merchant receives the stolen account credential, the fraudster's account information, and instructions regarding the amount to transfer.

2. The cashier uses the stolen account to perform a financial transaction with the account's bank or the merchant uses the account to purchase goods through a retailer.

3. The bank transfers the funds to the mule's account, supplied by the cashier, or the retailer sends the merchandise to the reshipper's address, which may be nothing more than a drop site.

4. The mule then transfers funds to the cashier's account or to another mule to further disguise the transaction chain. When dealing with merchandise, the reshipper forwards the goods to another address, possibly that of another reshipper or that of the merchant.

5. The cashier or merchant then delivers the funds or merchandise to the fraudster, keeping a certain portion as compensation for his or her service.

In order to prevent any kind of fraud we need to respect the internal control over financial reporting. Thus, management control became important to stop the fraud and corruption. Internal control quality could be relevant to any organization. Thus, "over the past decade, organizations have invested heavily in improving the quality of their internal control systems. They have made the investment for a number of reasons, notably: (1) good internal control is good business – it helps organizations ensure that operating, financial and compliance objectives are met, and (2) many organizations are required to report on the quality of internal control over financial reporting, compelling them to develop specific support for their certifications and assertions."

Fraud is strongly connected with corruption and the economic crunch accelerated the rhythm of corruption and opportunities. Corruption means violating the public norms and trust.

Burke and Cooper presented how people are exposed to corruption and temptation. “For decades, many studies have investigated the effects of corruption and the unethical acts of government and big business. People around the world, in small and large countries alike, have been exposed to a barrage of examples of corruption and unethical acts. Research has attempted to understand these acts by examining such topics as ethical decision making and by considering possible antecedents of corruption. Here we address related issues by way of a dual focus: (a) by considering ethics perceptions as a key antecedent of corruption (namely, because corruption can spread if unethical acts come to be perceived as acceptable), and (b) by presenting a statistically efficient way of investigating perceptions of ethical misbehaviours.”

Only a strong internal control could prevent any form of corruption and fraud. Olsen explains how a recent survey performed by a global business consulting firm discovered that only 50 percent of senior corporate executives are “highly confident” that business control systems are managing their organizations business risks effectively. “The survey also revealed that fewer than 10 percent of these senior executives rated their control systems as “excellent” in providing early warning signs to catastrophic risks. In an increasingly competitive global marketplace, this could mean trouble for U.S. businesses competing on an uneven international playing field, where foreign competition does not have to adhere to such laws as the Foreign Corrupt Practices Act (FCPA).”

Olsen thinks that an effective anti-corruption program must have the foundation of a strong code of conduct that communicates the organization’s position on conflicts of interest, bribery, kickbacks, confidentiality of proprietary information, and compliance with all applicable laws and regulations. “To be effective, the program must have the support and oversight of top management. The communication of the organization’s policies and procedures is also critical in this type of program. Employees need to be constantly apprised of industry trends and new regulations through ongoing training programs.”

Conclusion

Fraud and corruption have adopted new techniques since the development of the computer and the Internet. Also, the economic crunch presented a new context for fraud and corruption. “Corruption has a corrosive impact on both overseas market opportunities and the broader business climate. It also deters foreign investment, stifles economic growth and sustainable development, distorts prices, and undermines legal and judicial systems. More specifically, corruption is a problem in international business transactions, economic development projects, and government procurement activities.”

The globalization and Europeanization created new opportunities for scammers and fraudsters. Thanks to the rapid emergence of global markets, the rise of high-speed digital information technologies, and the development of the Internet, fraud can now evolve, mutate, and spread with mind-numbing speed. A special cause could be the free circulation of the people inside European Union and

overseas, as well. New young researchers are trying to develop new Internet techniques to improve the fast growing transactions and businesses all over the world.

Bishop and Hydoski explained how managing the risk of fraud and corruption requires an ongoing commitment to acquiring fresh knowledge and putting it to work. They highlighted how quite often this fresh knowledge must be obtained from outside your company. Usually, organized criminal groups constantly evolve new fraud schemes to part companies from their money. Thus, customer and vendor frauds develop new twists, taking advantage of new technologies. "Entering new markets creates new business opportunities, but also new risks that may be outside your previous experience. You will need a proactive strategy for staying abreast of new fraud risks as they emerge, and a process for sharing critical knowledge across the company as it becomes available. Ignorance, whether accidental or willful, will not help your company manage the risks of fraud and corruption."

In order to stop the growing fraud and corruption we need to enforce internal control and to develop auditing procedures. Internal control is one of the most important sources of audit evidence.

REFERENCES

- Bishop, T. and Hydoski, F. (2009), *Corporate Resiliency. Managing the Growing Risk of Fraud and Corruption*, John Wiley & Sons, Inc., Hoboken, New Jersey.
- Bryan, K et al. (2009), *Cyber Fraud. Tactics, Techniques, and Procedures*, CRC Press, Taylor&Francis Group, p. 21.
- COSO, *Internal Control over Financial Reporting. Guidance for Smaller Public Companies*, Vol. 1, 2006.
- Ronald J. Burke and Cary L. Cooper (2009), *Research Companion to Corruption in Organization*, Edward Elgar Publishing Limited, The Lypiatts, Cheltenham, UK.
- Olsen, W. P. (2010), *The Anti-Corruption Handbook. How to Protect Your Business in the Global Market Place",* John Wiley & Sons, Inc., Hoboken, New Jersey, p. 2.