The Role of Internal Control and Information Sharing in Preventing Fraud in the Saudi Banks

Rayaan Baz
Tunku Puteri Intan Safinaz
School of Accountancy
University Utara Malaysia, Malaysia,
Email: raybaz00@gmail.com,

Rose Shamsiah Samsudin,
Senior Lecturer,
Tunku Puteri Intan Safinaz School of Accountancy,
University Utara Malaysia, Malaysia,
Email: shamsiah@uum.edu.my

Ayoib Che-Ahmad
Profesor**,**
Tunku Puteri Intan Safinaz School of Accountancy,
University Utara Malaysia, Malaysia,
Email: ayoib@uum.edu.my

Abstract
Fraud is known to threaten companies and organizations inclusive of all financial institutions in the world. Studies have shown that weakened internal controls and technological advances may have created new fraud threats for banks. The threats have been difficult to deal with because of the rapid changes that characterize the technology industry. Generally, over 5 billion online fraud attempts took place each year globally. In Saudi Arabia alone, it is estimated that about SR 16 billion is lost each year to commercial fraud, a large part of which is perpetrated electronically. Recent data shows that the country is among the top twenty countries most affected by electronic fraud. Therefore, fraud prevention should be a crucial focus for Saudi banks. This study presents a conceptual framework on measures that can be employed by banks and government authorities in the country in dealing with the growing electronic banking fraud.

Keywords: *Fraud Prevention, Saudi Banks, Information Sharing, Internal Control, Fraud.*

1.0 Introduction

Fraud is a key problem experienced by banking systems across the world, and the Saudi Arabian banking system is no exception. Advances in technology leading to the development of electronic banking have led to the emergence of new fraud challenges for the country's banking sector. Saudi Arabia is particularly more susceptible to the new challenges given that it was ranked 16th in Kaspersky's list of the countries' most susceptive to online attacks (Kaspersky, 2014). According to Arab News (2014), currently commercial fraud costs the country about SR 16 billion each year.

2.0 Literature Review

A number of studies have investigated the causes of fraud and the measures that can be taken to prevent fraud. Arora and Khanna (2009) contend that fraud can be prevented by strengthening an organization's internal control systems. This perspective is supported by Albrecht (1996) who claims that weak internal control systems create opportunities for perpetration of fraud. Bologna (1994), on the other hand, cites environmental factors among them internal controls and employee reward systems as factors that influence the probability of fraud in an organization. On their part, Petrascu and Tieanu (2014) argue that the executive is responsible for fraud prevention and detection by instituting and maintaining appropriate internal control systems. A good internal control system is believed to be able to reduce the possibility of fraud although they cannot eliminate it completely. At the board's level, the audit committee has the role of supervising management to ensure that all significant fraud risks are identified and actively monitored, and that the internal controls put in place to deal with the risks are effective. In short, the internal audit function serves as the audit committee tool for audit committee for assessing fraud risk and effectiveness of the internal controls implemented by management. The role of internal controls in fraud prevention has also been tested empirically. For instance, Agyemang (2015) examines the impact of internal controls on fraud prevention in banking institutions. A sample of 35 management staff, including internal auditors is used for the study leading to finding that the internal control measures put in place by management helped banks to prevent fraud.

According to the Federal Reserve Bank of Minneapolis (2015), another important factor will be information-sharing between industry and government authorities, which is also crucial to preventing fraud. With regard to this, Eurofinas (2011), claims that the main tool that enables organizations to prevent fraud is the availability of accurate, timely, and relevant information. In order to obtain such information requires the establishment of relevant databases and the sharing of information between departments and also organizations. As a result, Business Analytics software and services, SAS (2013) recommends an enterprise-wide and inter-organizational approach in fraud prevention through information-sharing between the relevant departments and organizations. According to SAS (2013), majority of fraudsters are veteran, recurring perpetrators. Therefore, information-sharing can help to identify potential fraudsters before they actually commit fraud. Unfortunately, silo information systems do not promote data sharing (SAS, 2013) and consequently, organizations need to invest in an open data systems to effectively prevent fraud.

2.1 Saudi Banks

Saudi Arabian banks play a crucial role in the country's economy. The banks' deposits grew exponentially between 2010 and 2012 before embarking on a steady decline from 2013 to the present (Nyad Capital, 2016). The decline is attributed to moderation in the country's economic growth due to a fall in global oil prices. Currently the Saudi banking sector consists of both islamic and conventional banks (Samar, 2011). The banking sector also has the largest assets of islamic and conventional banks among the Gulf Cooperation Council (GCC) countries (Garbois et al., 2013).

2.2 Fraud Defined

Fraud refers to deception practiced deliberately and aimed at making a gain for the person

perpetrating the fraud or creating a loss for the victim of the fraud (Chartered Institute of Management Accountants (CIMA), 2009). Many suggested that fraud can be perpetrated internally or externally. Internal fraud is carried out by members of the organization and includes misappropriation of assets, financial statement fraud, bribery and corruption. While external fraud, on the other hand, is conducted by outsiders (CIMA, 2009). Forms of external fraud include card skimming, identity theft, and virus attacks among others (Berney, 2008). Incidences of external fraud have increased exponentially across the world due to the growth of electronic banking. In 2014, for example, over 5 billion electronic hackings were attempted across the world, majority of which were directed at financial institutions. Also, the world is believed to have witnessed an attempt at online fraud every 14 seconds (Arab News, 2014).

2.3 Fraud Prevention

As most of the fraud issues currently facing banking institutions emerge from advances in technology, reciprocally technological solutions are needed to deal with the fraud (Subramanian, 2014). The possible technological solutions include profiling customers using special algorithms to establish their probability of perpetrating fraud and using the results as the basis for monitoring the customers' transactions with the bank (Katz, 2010); information-sharing between the public authorities and banks to increase the effectiveness of monitoring potential fraud perpetrators; cooperation between government, banks and systems security bodies; and increasing awareness regarding the sound practices of using ATMs, credit cards, and other electronic banking channels (Arab News, 2014).

2.4 Internal Controls and Fraud Prevention

Internal controls are the processes put in place by management to provide reasonable assurance regarding the achievement of the organization's objectives. With respect to fraud, internal controls are put in place to prevent or detect fraud. Internal controls play an important role in fraud prevention by limiting the opportunities available to insiders and outsiders for perpetrating fraud (Rothberg, 2012). Weak internal controls increase the likelihood of fraud occurring in an organization (Albrecht, 1996). Indicators of weak internal controls include lack of segregation of duties; a poor control environment; lack of proper documentation and records; lack of proper checks; lack of proper authorizations; an inadequate accounting system; and management overriding of controls (Albrecht, 1996). In addition, lack of updated technology-based controls is an important sign of weak internal controls in industries that rely heavily on information technology like the banking sector. The strength of internal controls is also particularly affected by the tone at the top. The tone at the top is the attitude of management towards the organization's internal control environment. For example, if management condones fraud, internal controls in the organization are likely to be weak. In contrast, management that punishes fraud effectively will create an environment with strong internal controls.

2.5 Information-Sharing and Fraud Prevention

Information-sharing between the banking sector, government authorities and systems security firms can be a key component of fraud prevention as it helps in monitoring notorious perpetrators of fraud and along the way, developing solutions to deal with the prevalent cases of fraud. Sharing information between banks and the relevant government authorities enables the development of a database of repeat perpetrators of fraud which facilitates monitoring of the most likely sources or causes of fraud. Cooperation with systems security firms, on the other

hand, aids in developing solutions to the sources of fraud that pose the highest threat to the banking sector.

Information sharing is also important not only between agencies that fight fraud but within the organization itself. This is because fraud occurring on an enterprise system is easier to detect than fraud occurring on a silo system (SAS, 2013). More specifically an enterprise system involves inter-connection between the programmes and data in different departments of an organization. Thus, when fraud occurs in an enterprise system, therefore, it can be detected from multiple fronts. In contrast, programs and data of different departments exist separately in a silo system. As a result, fraud occurring in a silo system can only be detected in the department where the fraud occurs. Data sharing within an organization should not be done only on data where fraud is suspected but with all forms of data that are susceptible to fraud.

2.6 Research Objectives

Based on the abovementioned discussion, this study aims:

a) To examine the relationship between internal control and fraud prevention in Saudi Arabia banking sector;
b) To investigate the relationship between information sharing and fraud prevention in Saudi Arabia banking sector.

3.0 Conceptual Framework

A conceptual framework refers to a set of ideas or concepts organized in a way that makes them easy to communicate to others (Yearwood, 2011). The conceptual framework developed in this study indicates how banks in Saudi Arabia can prevent the increasing incidences of fraud as result of growth in online banking. The framework is based on the measures discussed in the study for curbing fraud. The framework is as presented in Figure 1.

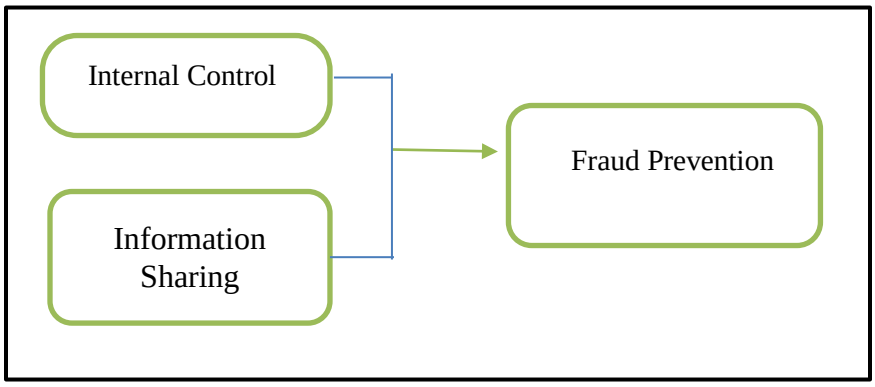

Figure 1: Conceptual framework for preventing fraud in the Saudi Arabian banking sector

The above conceptual framework is guided by extant literature in relation to fraud prevention. Two main themes emerge in literature on fraud prevention, namely; internal controls and information-sharing (Rothberg, 2012). Important internal controls in prevention of fraud include segregation of functions, electronic controls, and documentation. In the banking industry for example, in particular, segregation of cash inflows and outflows is important to enable establishment of appropriate fraud prevention practices.

Internal controls should be monitored consistently to ensure that they are effective and updated as necessary. Moreover, care should be taken to ensure that the controls are in line with the latest technology (Rothberg, 2012). Disparity between the organization's controls and technological advances creates opportunities for perpetration of fraud.

3.1 Theoretical Framework and Hypothesis Development

Internal controls and information-sharing between banks and the relevant agencies play a crucial role in prevention of fraud. Internal controls reduce the opportunities for committing fraud (Rothberg, 2012). Over the years, advances in technology have reduced the effectiveness of the traditional internal controls in fraud prevention. For example, in the past, banks have relied on physical security features that were embedded in cheques to prevent fraud. The availability of advanced duplication technology, however, makes this form of prevention no longer effective. Technology has also created opportunities for new forms of fraud such as identity theft. Moreover, as new forms of technology continue to emerge, the opportunities for fraud will also increase. Consequently, banks have to continuously update their internal controls systems to accommodate the changes and also effectively prevent fraud. Based on this view, this study proposes the following hypothesis:

H1: There is a direct positive relationship between investment in internal controls and fraud prevention.

According to this hypothesis, firms with appropriate internal controls are able to prevent fraud effectively than firms without appropriate internal controls in place.

Information-sharing, on the other hand, promotes coordination between banks, regulators, governments and other agencies engaged in fighting fraud such as system security firms (Federal Reserve Bank of Minneapolis, 2015). This also presumably leads to more effectiveness fraud prevention. In some jurisdictions, for instance, banks can confirm whether cheques purportedly issued by the government for example, are genuine by comparing the cheque number and amount against government records available to the bank through a centralized system (Government Finance Office, 2012). By increasing the number of hurdles that fraudsters have to overcome, information-sharing reduces the opportunities for fraud significantly. Consequently, fraud prevention is expected to be more effective where there is information-sharing between banks, regulators, governments, and system security firms. Based on this perspective, this study proposes the following hypothesis:

H2: There is a direct positive relationship between information-sharing and fraud prevention.

This hypothesis means that information-sharing between banks, governments, regulators, and systems security firms and other relevant organizations is associated with promotion of effective prevention of fraud.

4.0 Methodology

This study examines the relationship between internal control, information-sharing and fraud prevention in the Saudi banks by initially working on the development of a conceptual framework. Lack of the published secondary data and the confidential announcing of fraud cases in Saudi banks led researcher to consider the use of self-administered questionnaires via survey technique as possible appropriate means of examining the hypothesis formulated in this study.

5.0 Concluding Remarks

In summary, fraud is a fundamental problem facing all financial institutions across the world. Advances in technology have led to exponential growth in the incidences of fraud. In addition, banks are the main target of electronic fraud because of the fast change in technology used this sector and also their role in the monetary systems. Being among the top twenty countries that are at high risk of electronic fraud, therefore banks in the country have to be keener on fraud prevention than most of their counterparts in other parts of the world. As most of the new fraud threats are based on advances in technology, technological solutions are needed to prevent the frauds. The solutions should be geared towards strengthening the internal control systems of banks; increasing information-sharing between banks, relevant government authorities and systems security firms; and increasing customer awareness of proper practices in the use of electronic banking channels.

References

Agyemang, J. (2015). Internal Control and Fraud Prevention. *International Journal of Management and Scientific Research*, 1(1), 230-257.

Albrecht, W. (1996). Employee fraud. *Internal Auditor*, 26.

Arab News (2014). *KSA banks set high security standards*. Retrieved August 1, 2016 from http://www.arabnews.com/news/economy/615751

Arora, B. and Khanna, A. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry. *International Journal of Business Science and Applied Management*, 4, 2-21.

Berney, L. (2008). For online merchants, fraud prevention can be a balancing act. *Cards & Payments*, 21, 22-27.

Bologna, J. (1994). *How to detect and prevent embezzlement?* The White Paper

CIMA (2009). *Corporate Fraud*. Retrieved August 1, 2016 from http://www.cimaglobal.com/documents/importeddocuments/cid_tg_corporate_fraud_may09.pdf.pdf

Eurofinas (2011). *Fraud Prevention and Data Protection*. Retrieved August 4, 2016 from http://www.eurofinas.org/uploads/documents/Non-visible/Eurofinas-Accis_ReportOnFraud_WEB.pdf

Federal Reserve Bank of Minneapolis (2015). *Industry and Government Information-Sharing Resources Related to Payments Fraud*. Retrieved August 1, 2016 from https://www.minneapolisfed.org/~/media/files/about/what-we-do/2015-industry-government-information-sharing-resources-related-to-payments-fraud.pdf?la=en

Garbois et al.. (2013). *Online Banking in the GCC*. Retrieved August 1, 2016 from https://www.atkearney.com/documents/10192/707238/Online+Banking+in+the+GCC.pdf/bc3dadf2-25f4-4127-bde7-c2bad974abde.

Government Finance Office (2012). *Bank Account Fraud Prevention*. Retrieved December 3, 2016 from http://www.gfoa.org/bank-account-fraud-prevention.

Kaspersky (2014). *Kaspersky security Bulletin, Overall statistics*. Retrieved August 1, 2016 from https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014. -Overallstatistics-for-2014.pdf

Katz, J. (2010). *Digital Signatures*. New York: Springe.

Nyad Capital (2016). *Loan and Deposit Pressure Ahead*. Retrieved August 1, 2016 from http://www.riyadcapital.com/en/Images/Banking%20Sector%201Q2016%20Preview%2

0EN_tcm10-8032.PDF.

Petrascu, D. and Tieanu, A. (2014). The Role of Internal Audit in Fraud Prevention and Detection. *Procedia Economics and Finance*, 16, 489-497.

Rothberg, A. (2012). *The Role of Internal Controls in Fraud Prevention*. Retrieved August 1, 2016 from http://www.cfoedge.com/resources/articles/cfo-edge-internal-controls-and-fraud-prevention.pdf

Samar, S. (2011). *Performance analysis of Islamic banking: Some evidence from Saudi Arabian banking*. Retrieved August 1, 2016 from http://r-cube.ritsumei.ac.jp/bitstream/10367/2589/1/Bintawim%20Samar%20Saud%20S.pdf

SAS (2013). *An Enterprise Approach to Fraud Detection and Prevention in Government Programs*. Retrieved August 4, 2016 from http://www.rockinst.org/forumsandevents/audio/2013-11-06/fraud_wp.pdf

Subramanian, R. (2014). *Bank Fraud*. Retrieved August 1, 2016 from ttps://www.sas.com/

Yearwood, L. (2011). *A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses*. Research Paper Concordia University College of Alberta.