An investigation of risk management practices in electronic banking in Sultanate of Oman

Amira Mohammed Musabah Nasser Al Siyabi MIDDLE EAST COLLEGE
Sarah Muslem Mubarak Al Araimi Middle East College
Jitendra Pandey Middle East College

The growth in Internet has led to expansion of e-banking, forming online services, like financial services, account opening and facilities (Kolodinsky et al, 2004). Banks manage risks in some areas like: strategy, credit, market, liquidity etc. (Gorgisco, 2006). However, the growth of e-banking become vulnerable to the challenges it faces. All organisations conducting their business on-line have to focus on controlling the associated risks; e-banking is no exception. Malisuwan (2006) categories these e-banking risks into three main areas to be managed: Board and Management Oversight, Security Controls and Legal and Reputational Risk Management based on the fourteen “risk management principles” identified by the Electronic Banking Group (EBG) of the BCBS. Georgescu (2006) suggests that the competitive pressure to launch new innovative products in very short time scales intensifies the management challenge to ensure that adequate strategic assessment, risk analysis and security reviews are undertaken. Over the past two decades, e-banking has become an increasingly important area of interest, with the risks associated with e-banks during this period of significant growth requiring effective risk management processes. Based on the results of our research, the security risks are clearly identified as the most important as banks are working hard to mitigate the risks and this is very encouraging and effective.

The main objectives are to investigate the risks of e-banking services in Oman, and their impact on population. Initially a semi-structured interview is conducted as a pilot study with four knowledgeable and experienced staff from one of the leading banks in Oman, to study employee views on risk management issues in e-banking. After the pilot study, the questionnaire was developed and used in major banks in Oman to determine whether it operates in line with basic risk management principles.

Introduction

Fraud is one of the major threats to the development of the banking sector worldwide. It is studied in cases of fraud prevention in the Nigerian banking sector. Data were obtained from the main building, through the management of this questionnaire 200 people from ten commercial banks in Lagos revealed the results that greed is the first reason. In any economy, the banking sector plays a very important role in development (Adeyemo 2012).

Fraud is considered to be a forgery exclusion or disguise of the truth for the purpose of betraying the administration's financial stage or the secretariat may harm the organization or the individual. Fraud is any action that it intends to acquire to deceive another person in other words. Fraud usually requires financial theft accounts, manipulated them frequently and attaches cover up to theft.

Problem

Logically as expected subscription fraud in multiple forms and forms usually insiders are employees and foreigners who cooperate to implement the act effectively (Adeyemo 2012). Some common types of bank fraud in Nigeria that are by no means complete will be mentioned Alashi (1994) and Adeyemo (2012):

Fraudulent operations involving the use of deceptive copies of the customer's signature in the payment of large sums of customer account without the prior permission of the customer, Such fraud can be targeted such as current deposit accounts, savings accounts or transfer instruments such as drafts. It has been demonstrated through these experiments that the perpetrators of most of these fraudulent operations are committed by external or internal staff in the plot of bank employees who are usually the ones who launch the forms of forged signatures (Idolor, 2010).

Informal assumptions in cases where the bank employee assumes the cashier and safes are inclined from the register. These unauthorized loans are made in exchange between employees I.O.U. Or a deferred check or even nothing. Most of these groups spread during the end of months and weekends when salaries were not paid. These loans are used from the basement and can be up to 1000 Naira, work lasting a few hours or days and a quick ticking and then replaced the supplier without any proof in the place that was transferred. Like exercise when you do it without any official records and very frequently. They become vulnerable to manipulation quickly, and then resort to other means to balance the money and the vault of the bank and replace these amounts of money collected.

The incidence of fraud increases when exposed to poor internal controls and includes, poor environment for control and lack of continuous and independent inspections, lack of attention to appropriate licenses and lack of appropriate documentation, and the inefficiency of the accounting system (Albrecht, 1996)

There are environmental factors that greatly enhance the embezzlement processes, including the inefficiency of internal controls, lack of administrative procedures when performance levels fall below the acceptable level where the functional roles become ambiguous, lack of operational and timely references to periodic reviews and inspections, failure to monitor the implementation of policies and procedures honestly.) (Bologna, 1994)

Reductions involving the misappropriation of funds held by bankers as acting on behalf of customers where the value of customer deposits is reduced either by fraudulent change in the deposit section by the customer or bank staff or the other way is money transfer. When customers and bank employees conspire to cancel restrictions, this fraud is committed by their number and takes time to figure out which can only be as easily revealed during the settlement of the bank account of the customers.

Embezzlement and theft are another form of precaution which involves A collection of illegal financial elements such as foreign currencies, travelers checks and cash. It is also possible to involve an dishonest combination of banking property such as equipment, stationery, computers or cars and various other types of bank-owned electronics.

Taking over another person with the intention of betraying honesty and committing fraud is called spoofing. Identity versus third parties to obtain a new check book used to commit fraud is another form of bank fraud. Impersonations have been particularly successful with those who can easily provide signatures, samples and pictures to suspicious customers.

This study contains 114 cases of fraud where this phenomenon arose due to false documents and limited separation of duties, It has done results to reduce fraud, such as the development and use

of basic principles of good internal control where internal auditors should ensure that prevention systems are in place, and that the quality of internal audits to detect and investigate fraud is ensured.) (Calderon and Green 1994)

Figure 1. *Fraud originators*

Figure 1 tells the various sources which can initiate the fraud. Manipulate vouchers Change or replace account entries from one account to another used to commit fraud. They transfer funds of unsuspecting clients to banks in a fabricated account. The quantities that are usually taken in a small amount so as not to be observed by the staff of the bank or the top of the administration to be non-morib. Manipulation of vouchers can bloom in the banking system with insufficient balances or checks such as, and also like all bank records, lack of detailed daily voucher examination, and poor segregation of employees.

Computer frauds are fraudulently manipulated by computer banks. Either in the data collection phase, or the data dissemination stage, or the input processing stage. These computer scams can also occur due to system software input, cyber theft, transaction manipulation, viruses, or incorrect input. Computer fraud arising from threat, cybercrime and theft (Olorunsegun, 2010). Usually what sends an enormous amount is spent annually in the banking sectors in reducing and helping in combating computer and Internet fraud.

Harris and William, 2004) studied the causes of bank fraud and the institution should establish policies and procedures to provide due diligence to all customers. It is prevented from submitting requests for financial statements, as these symptoms arise as a result of the lax corporate culture

Regarding the application and reduction of internal controls, employee indifference and excessive confidence.

When opening an account, fraud usually begins without doubt by the bank as a transaction with a fictitious identification.

Fraud in banks usually requires technical expertise in order to access assets and funds (wiseGeek, 2013), from the types of fraud to which banks are exposed to purchase fraud, sales fraud, payment check fraud and ATM fraud (Benjamin, 2011), Internal staff fraud is a major threat as they have direct access to customer banking systems, information and personal records, exploiting opportunities when organizations fail.) (Sidden, 2005).

Fraudsters use phishing to get personal details of customers as they use them in fraudulent activities, as these challenges result in the company losing a lack of adequate security measures. (Amtul, 2011)

Fraudulent transfers occur as a result of a request solely to commit a fraudulent transaction or to change the request for transfer of project funds. The real order can be changed by changing the transfer amount, account number or beneficiary name. There is a name given to fraudsters in Nigeria, "Yahoo Boys" sends messages by fake e-mail to some victims and requests them to apply for a fake lottery or fake contracts and thus earn non-existent money from the account of the dead billionaire in different parts of the world where he gets involved with fraudulent bankers In Western Union the Ministry to withdraw their hard bad currencies.

Solution

Bank fraud is a serious risk to the bank's regulatory growth and may lead to a bank's relief (Ojo, 2008). Fraud is a difficult cost because it reduces depositors' deposits and ultimately leads to the

collapse of capital from banks. Fraud is a difficult habit to detect because it is difficult to estimate and find and also did not detect frauds or even reported. Because some banks have the ability to cover up the fraud that they face in banks. And all this in order to continue to profit and good faith customers and motivate their customers all the time (Asukwo, 1999). These distant and remote frauds proposed by Aderibigbe can be eliminated (1999) and Idolor (2010),

Providing training is of great importance in this regard because the employee needs good training not only helps him to develop skills, but also contributes to increase the possibilities of employee performance and provide knowledge and understanding of banking practices and principles.) (Barnes 1995)

There should be adequate internal control, effective audits and security systems, and checks for employees, customers and non-customers for fraud. And also reduce and eliminate fraud.

There are many methods to protect against fraud including password protection, employee reference checks, vendor contract reviews, analysis of financial ratios through analytical reviews, firewalls, digital analysis and many types of technological software.) (Beirstaker, Brody, Pacini, 2005)

Placing enough staff to face planning problems and assign duties Increase experience Selection of staff is efficient. This situation can be easily exploited to deal with these frauds at the bank on the day. Compensation of customers Adequate compensation of benefits and additional salaries owed to employees of the Bank.

Where he discovered the most important ways to prevent fraud is to understand the cause and identify gaps in the procedures and then assessed in terms of possibility, where the effective monitoring of the prevention of fraud where it requires no effort and time. The organization begins by identifying weaknesses in the system, followed by improving vulnerability with a good system and better controls, where the implementation of these controls and education, training and awareness programs will reduce fraud.) (Newsletter, 2001).

Developing appropriate record keeping programs and accounts with inconsistencies between the different accounts of the bank monthly, weekly or daily often do not find fraudulent talk can exploit this gap by the staff of the bank.

Figure 2. *Figure 2 Products vis Digital Platforms*

The Bank's management is taking new security measures to eliminate fraud in e-banking services. Security measures need to be taken to ensure identity regardless of traditional methods. It is no longer sufficient. Biotechnology has been identified as one of the potential technologies to improve security.) (Vandommele, 2010)

Increased training and retraining is appropriate on the theoretical aspects of banking activities, process and operations, more often resulting in increased production and performance. These gaps can be easily exploited by the fraudster.

Hosted files are downloaded Check for viruses and spyware viruses before you save the file on the system. Most of the files are only found to be unclean as soon as the user falls prey to one of them.

There are some precautions that consumers should use to prevent identity theft and simple ways to avoid falling victim to scam. Be stingy in giving personal information to others. Check financial information regularly and know when something

Figure 3. *Fraud Risk Owners*

strange happens. It is also often necessary to keep accurate financial records in case they are used at a critical time.

It is possible to conspire among the agents who are charged with protecting the interest and other assets of the bank.

Bad working conditions.

Betrayal and poverty of employees.

Fraud operation model, the effectiveness and cost of fraud risk management. The survey posed questions to understand fraud risk management by banks to improve investment decision-making processes. The total cost of fraud risk management is not monitored by the 52 percent surveyed, which reduces the visibility of the board and risk committees responsible for providing resources regarding the effectiveness of fraud functions.

Figure 4. *Fraud Navigator*

KPMG's Fraud navigator, fraud Risk Management Operational Model It is important in the risk assessment to have strong banking lists to reduce the risk of external and internal fraud in the bank. Diagram (2)

External Fraud Studies have shown in 2018 that the total number of external fraud has increased by 61%, including various types of fraud from 2015 to 2018 including identity theft, fraudulent access to the account and card that does not provide fraud

Internal fraud (employee) where the total answers were that the total cost of the global fraud scale remained the same in 2017 and 2018, many incidents occur to external clients with the help of experienced internal sources with detailed experience of operations and controls.

Through the questionnaire, respondents selected digital channels as one of the first challenges, as the use of digital channels by banks increases. Non-cash transactions are expected to increase by 12.7% as of 2021 through the 2018 World Payments report, 78 respondents said a quarter of the products were delivered through digital channels, with many banks competing to showcase their products through digital channels.

Articles

Banks advised to stay a step ahead of fraudsters

"MUSCAT: Bankers should stay one step ahead of fraudsters, V N Sethuraman, Executive, and Banking Development Department at Central Bank of Oman (CBO), said. He then, enumerated the measures that should be taken to insulate banks from fraudsters as successfully carried out frauds could chip away the condence of the consumers. Sethuraman made the remarks in his speech on Fraud Risk Management (FRM) at an event organized by the Oman chapter of Association of Carried Fraud Examiners (ACFE). The CBO executive said that the need of the hour was to have a system in place that could prevent frauds from taking place, adding that the master circular on FRM issued by CBO oared a stellar framework with regard to the same. To address FRM for all licensed nancial leasing companies," he said. And added that if we they collected enough information from aliased banks, and then big data would help them predict behavior of fraudsters. "I think we need to be pro-active, rather than reactive in dealing with banking frauds," he added.

Tahir bin Salim Al Mamri, the Executive President of CBO, pointed out that banking frauds were not merely operational problems, but rather dierent issue, altogether. "This article shows that the bank must be one or two steps ahead of the fraudsters in order to keep them away from danger. There are procedures that were mentioned by Sethuraman at an event organized by a branch in Oman by the Accredited Fraud Society (ACFE).It has been reported that some big data helps predict predators' behavior. Also, there must be activity so that there is no dealings with bank fraud. Taher bin Salim Al Maamari, executive director of the Central Bank of Oman (CBO), said fraud is a fairly severe problem, not an operational one.

Major seminar to be held on fraud risk management

“The ACFE is the world’s largest anti-fraud organization and premier provider of antifraud training and education. Together with more than 80,000 members, the ACFE is reducing business fraud worldwide and inspiring public condenses in the integrity and objectivity within the profession " (cfes) this article talks about the unique experience you are talking about in the area of fraud prevention and detection. Which can be all over the world of fields, sizes, sectors and industries? CFE is run by proven expertise in preventing, deterring and detecting fraud.

Banks advised to stay a step ahead of fraudsters

"MUSCAT: Bankers should stay one step ahead of fraudsters, V N Sethuraman, Executive, and Banking Development Department at Central Bank of Oman (CBO), said. He then, enumerated the measures that should be taken to insulate banks from fraudsters as successfully carried out frauds could chip away the condence of the consumers. Sethuraman made the remarks in his speech on Fraud Risk Management (FRM) at an event organized by the Oman chapter of Association of Carried Fraud Examiners (ACFE). The CBO executive said that the need of the hour was to have a system in place that could prevent frauds from taking place, adding that the master circular on FRM issued by CBO oared a stellar framework with regard to the same. To address FRM for all licensed nancial leasing companies,” he said. And added that if we they collected enough information from aliased banks, and then big data would help them predict behavior of fraudsters. “I think we need to be pro-active, rather than reactive in dealing with banking frauds,” he added. Tahir bin Salim Al Mamri, the Executive President of CBO, pointed out that banking frauds were not merely operational problems, but rather dierent issue, altogether. "This article shows that the bank must be one or two steps ahead of the fraudsters in order to keep them away from danger. There are procedures that were mentioned by Sethuraman at an event organized by a branch in Oman by the Accredited Fraud Society (ACFE).It has been reported that some big data helps predict predators' behavior. Also, there must be activity so that there is no dealings with bank fraud. Taher bin Salim Al Maamari, executive director of the Central Bank of Oman (CBO), said fraud is a fairly severe problem, not an operational one. Figure 5 explains how the risk can be assessed and controlled.

Figure 5. *Effect on brand due to fraud*

Figure 6. *Fraud Assessment Framework.*

Major seminar to be held on fraud risk management

“The ACFE is the world’s largest anti-fraud organization and premier provider of antifraud training and education. Together with more than 80,000 members, the ACFE is reducing business fraud worldwide and inspiring public condenses in the integrity and objectivity within the profession "(cfes) this article talks about the unique experience you are talking about in the area of fraud

prevention and detection. Which can be all over the world of fields, sizes, sectors and industries? CFE is run by proven expertise in preventing, deterring and detecting fraud.

Conclusion

In conclusion, this article included many of the problems faced by banks through electronic thefts and there are internal and external factors, internal factors, which are unfaithful employees who can penetrate and access to the system in cases of weakness through the bank and theft and all weak internal controls and strict laws, while external factors such as penetrations By people stealing money or by dealing with the bank employee to cooperate on theft. Banks have developed several solutions to eliminate or minimize this phenomenon, such as highlighting new and stringent controls and laws, strong management to prevent thefts and robber accounting, developing technology in the bank to emphasize the system and non-penetration, providing training for employees to take sufficient knowledge to maintain the security of the bank and understand banking practices and principles. Banks deal with this phenomenon in various ways.

Acknowledgements

I offer all the pride and gratitude to Mr. Jitendra Pandey for his assistance and accomplishment throughout the work of this article, and that I value all the useful and exerted efforts that he has given, his suggestions and experiences have helped us throughout our career in this article. Today, I am pleased to thank Mr. Jitendra for the concerted efforts made, which contributed to the advancement of the work to provide the best possible, although this indicates the painstaking efforts that did not wait for them, thank you and praise, So I am pleased to thank you for all you deserve.

References

E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT,(Mr. Rupesh. D. Dubey and Dr. Anita Manna)2019, available at < http://oldtm.lbp.world/SeminarPdf/167.pdf>.

reserve banks of India, India central bank , 2019 , available at,<https://www.rbi.org.in/scripts/otherlinks.aspx>

MBA Knowledge Base , Kate ,August 22, 2010, available at <https://www.mbaknol.com/business-finance/recent-trends-in-indian-banking-sector/ >

Digital banking fraud: Best practice for technology-based prevention ,2019, available at <https://netguardians.ch/digital-banking-fraud/>

Bank fraud, From Wikipedia,2019, available at <https://en.wikipedia.org/wiki/Bank_fraud> Five examples of user-centered bank fraud, Andre Machado,2019, available at <https://www.helpnetsecurity.com/2019/08/02/user-centered-bank-fraud/ >

Fraud risk management A guide to good practice, January 2009, available at < https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf >

Iyer, N. and Samociuk, M., (2006), Fraud and Corruption: Prevention and Detection.

CIMA and the IBE, (2008), Managing responsible business

Collier, P.M. and Agyei-Ampomah, S., (2007), CIMA Offi cial Learning System Management

Accounting Risk and Control Strategy.

The Institute of internal auditors, The Association of certifi ed public accountants, The Association of certifi ed public examiners, (2008), Managing the business risk of fraud: A practical guide.

Fraud Advisory Panel, (2006), Fighting Fraud: A guide for SME’s 2nd Edition.

Fraud poses serious risks to banks, Oman Daily Observer, · 12 Jul 2018 , available at <https://www.pressreader.com/oman/oman-daily-observer/20180712/281917363845980>