Northumbria Research Link

Citation: Shah, Mahmood (2013) Critical success factors for preventing E-banking fraud. Journal of Internet Banking and Commerce, 18 (2). p. 14. ISSN 1204-5357

Published by: OMICS International

URL: http://www.icommercecentral.com/open-access/critic... <http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196>

Northumbria
University
NEWCASTLE

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2013, vol. 18, no.2
(*http://www.arraydev.com/commerce/jibc/*)

Critical Success Factors for Preventing e-Banking Fraud

AHMAD KABIR USMAN, MSc
Researcher, Lancashire Business School, University of Central Lancashire, UK
Postal Address: **Lancashire Business School, University of Central Lancashire, Greenbank Building, Preston, Lancashire, PR1 2HE**
Email: ***ausman2@uclan.ac.uk***
Ahmad Usman is a research student at the University of Central Lancashire. His areas of interest are E-Banking Security and Biometric Technologies.

MAHMOOD HUSSAIN SHAH, PhD
Senior Lecturer, Lancashire Business School, University of Central Lancashire, UK
Postal Address: **Lancashire Business School, University of Central Lancashire, Greenbank Building, Preston, Lancashire, PR1 2HE**
Email: ***mhshah@uclan.ac.uk***
Dr. Mahmood Shah is a Senior Lecturer in Business Systems and Cyber Security at the University of Central Lancashire. His research interests are in the areas of cyber security, e-banking, identity theft prevention in e-retailing, e-business and Information Systems.

Abstract

E-Banking fraud is an issue being experienced globally and is continuing to prove costly to both banks and customers. Frauds in e-banking services occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls. Lack of research in this area is problematic for practitioners so there is need to conduct research to help improve security and prevent stakeholders from losing confidence in the system. The purpose of this paper is to understand factors that could be critical in strengthening fraud prevention systems in electronic banking. The paper reviews relevant literatures to help identify potential critical success factors of frauds

prevention in e-banking. Our findings show that beyond technology, there are other factors that need to be considered such as internal controls, customer education and staff education etc. These findings will help assist banks and regulators with information on specific areas that should be addressed to build on their existing fraud prevention systems.

Keywords: E-Banking; E-banking Frauds Prevention; Internet Banking Security; Fraud Prevention; Critical Success Factors

INTRODUCTION

Electronic banking services are the banking class of services that can be offered by a bank to individuals and companies through electronic means via a fixed or mobile telephone, and Internet (RATIU, 2011). Given that internet technology has evolved considerably over the years, newly developed e-banking services now differ considerably from older systems (Khan and Mahapatra, 2009). Some of the more common types of E-Banking services today are Online Banking, Automated Teller Machines (ATM), Electronic Funds Transfer, Electronic Cheque Conversion, Direct Payment and Web ATM services. There are many security issues related to all of these services and this paper aims to highlight factors that could be critical to the prevention of fraud in the e-banking space by reviewing relevant literature.

The online banking channel is the cheapest delivery channel for delivering banking products once established (Sathye, 1999 and (Tero Pikkarainen, 2004). Therefore it is no surprise that the banks globally are continuing to shift towards e-banking services. With the growing patronage of e-banking services and its anticipated dominance in the near future, some of the known factors that contribute to addressing the acute problem of security must be addressed. This paper identifies and synthesises a number of that factors such as the availability of funds, change management, timely access to information and strict internal controls could all prove vital for reducing e-banking fraud. Exposure to such factors provides regulators and bank management teams an insight into areas that may require increased emphasis and improvement.

Systematic Literature Review

The research makes use of a systematic literature review taking into consideration e-banking fraud and other electronic fraud or security related literature. A systematic literature review "is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest" (Kitchenham, 2007). Therefore ensuring thorough coverage of pertinent literature using a systematic approach. This was done using an iterative search strategy as the review evolved rather than predetermined linear search strategies as recommended by (Finfgeld-Connett, 2013).

The literature review was carried out in 3 phases inline with the guidelines of (Kitchenham, 2007).

These are:

1. Planning the review. This includes identifying the need for a review, specifying the research question and then developing & evaluating the review protocol
2. Conducting the review. This phase involves identification of the research, selection of the primary studies, study quality assessment, data extraction and synthesis.
3. Reporting the review. This is where the dissemination mechanisms are specified and then formatting and evaluation of the main report.

In order to perform searches for relevant literature, a selection of data sources was made. The databases that were used are:

- Academic Search Complete
- E-Journals
- Web of Knowledge

A number of keywords were used for searching databases to find relevant literature for the review. They are given below:

- Fraud Prevention Critical Success Factors
- E-Banking Fraud Prevention Technology/Security/Measures/Software
- E-Banking Fraud
- Fraud Prevention
- E-Banking Security

While searching, advanced search features such as applying related words and searching within the full text of articles were utilised. After each search had been completed, the results were reviewed and the most relevant literature was selected for use.

E-BANKING SECURITY CHALLENGES

The introduction of E-Banking has come with its challenges. These range from technology adoption, financial limitations, and technology acceptance of new systems. Other factors experienced globally are the increase in security fears, cultural barriers, limited internet access and legislation (Masocha, 2010). Auta (2010) found that security, user friendly, queue management, accessibility, time factor and fund transfer are major factors in the adoption of e-banking and that security is rated as the most important issue of online banking services. Research conducted by Agboola and Salawu (2008) is in agreement with this. Security concerns are of greatest importance for the adoption of e-banking services (Angelakopoulos, 2011 4). Hence, the desire to understand these challenges in more detail and adopt initiatives to address them.

Security is a factor that is constantly highlighted as a CSF for the success of E-Banking. The inadequacy of security potentially leads to financial losses, punitive measures by regulators and negative media publicity (Shah et al, 2012) therefore its importance cannot be over emphasised. In E-banking, fraud is a major contributory factor to the term security and needs to me managed closely. “Incentives for fraud increase when transactions are made in large amounts, when transactions are made anonymously or at the point of sale, when claims cannot be effectively verified at the point of sale, and when issuers of payment claims bear the costs of fraudulent transactions” (Roberds

1998). E-Banking offers most if not all these incentives, hence the need for adequate fraud prevention strategies.

In 2010, most of the fraud cases were perpetuated via electronic banking systems therefore reflecting weaknesses in the internal control systems (CBN Annual Report, 2010). Financial services and organisations suffer yearly losses through crimes such as online banking, cheque and card fraud (Adams, 2010). These clearly indicate that criminals are exploiting e-banking mediums. Hence the need for improved continuous improvement in security to prevent fraud (Giles, 2010) and mitigate the risk of customers' losing confidence in e-banking services. More recently, there has been some improvement in preventing fraud over electronic banking mediums. Financial Fraud Action, 2011 reported that in the UK, Fraud losses on credit/debit cards were at a 10 year low while online banking fraud losses fell by 24%. This has been attributed to improved e-banking security through both technological and non-technological approaches. Research aimed at minimizing fraud has proved popular extending beyond the banking industry to online auctions (Cecil Eng et al. 2007;Chang and Chang 2011), healthcare (May 2010), Insurance (Ormerod et al. 2012) to fraud prevention in the telecommunications industry (Estavez et al. 2006) where 56.2% of fraudsters were able to be identified by testing a fraud prediction module. However, research into factors critical to e-banking fraud prevention is limited.

E-Banking Fraud

Although there is no single accepted definition of fraud (The Legal Practitioner, 2013), it relates to wrongful or criminal deception that results in financial or personal gains. Bank Fraud is the use of deliberate misrepresentation (which usually requires some technical expertise) in order to fraudulently obtain money or other assets from a bank (wiseGeek, 2013). The types of fraud that are commonly experienced by financial institution include sales fraud, purchase fraud, cheque payment fraud and ATM fraud (Benjamin, 2011). Other strategies employed include collaborating with security agents and bank officials as well as local and international networking (Aransiola, 2011). Worryingly, results show that internal personnel of banks had been collaborating with fraudsters. This presents a real threat as internal personnel have direct access to banking systems and access to customers' personal information and records. According to the FBI, the majority of fraud is committed by employees who exploit breakdowns in organisations (Sidden, 2005). Research to understand why internal staff opts to engage in such activities exists. (Benjamin, 2011) found that perceived inequality and perceived job insecurity had significant effect on employee fraudulent intent. Such findings help highlight that beyond technology, there are other factors capable of impacting fraud that come into play.

Phishing is one of the mechanisms that fraudsters use to obtain customers personal details leading to its use for fraudulent activities. Amtul (2011) states that such challenges presented by phishing results in companies loosing thousands of dollars, and emphasises the need for biometrics to help checkmate such activities. In addition, statistics show that 35.9% of the financial sector is the target for phishing. A Javelin Identity Theft Report (2010) stated that there was a 12% and 12.5% increase in identity theft victims and fraud respectively. This not only highlights the fact that fraud and identity theft is on the rise, but that current security measures in place are insufficient.

Critical Success Factors

Rockart (1979) defines CSFs as the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organisation. CSFs are imperative in concept yet highly practical and as such readily understood and accepted by managers and practitioners (Butler and Fitzgerald, 1999). CSFs have been used for a variety of purposes ranging from manufacturing to IT System Implementations and are useful for planning and decision making purposes.

In contrast to this, Critical Failure Factors (CFFs) is a different approach that can be used to identify factors that tend to cause failure. Research shows that this approach is used less often and is suited to scenarios such as the work of Amid et al (2012) where frequent failures have occurred leading to the need 'to identify such factors and classify them' to help prevent failures in the future (Amid, 2012 11). However, Aziz and Salleh (2011) contradict this by arguing "identifying the critical success factors (CSFs) has become the main agenda for researchers, academicians and practitioners due to the wide number of failures reported". Therefore CSFs can still be applicable in such scenarios.

Identifying CSFs

Both quantitative and qualitative research methods can be used to identify CSFs. Methods previously employed include literature reviews (Umble and Umble, 2001), case studies (Holland and Light, 1999), surveys and interviews interviews (Rockart and Van Bullen, 1986) just to name a few. Shah and Siddiqui (2006) concluded that the survey approach is the most commonly used method for the identification of CSFs. However, this does not imply that this is the most effective approach. This study used the systematic literature review methodology to synthesise existing relevant literature and identify factors that affect e-banking fraud globally spanning both the developed and developing nations.

Critical Factors for Fraud Prevention

Bank stakeholders are constantly introducing new security measures with the aim of eradicating e-banking fraud, however existing measures have not been able to achieve this (Roberds 1998). Consequently, there is still need for research to narrow down on specific areas for improvement. Personally, I believe that improved authentication systems is the way forward and can play a significant role in e-banking fraud prevention. The common use of the same passwords for authentication increases the vulnerability whenever such information is stolen. Thus, an additional security measure is required to confirm the identity (Robert Moskovitch et al, 2009). Given that conventional methods of authentication via usernames and passwords are no longer sufficient (Vandommele, 2010), biometric technology has been identified as one of the potential technologies to improving security.

	Fraud Prevention Measure	**Reference to literature**
1	Biometric Authentication	(Bhattacharyya et al, 2009), (Akinyemi Ibidapo, 2010)
2	Fraud Prevention Software	(Sherman, 2002)(Sharer, 2004)
3	One Time Passwords (OTPs)	(Johnson 2007), (Annon 2005)
4	Smart Card Authentication	(INFORM, 2004)
5	Password	(Moskovitch, 2009)
6	Multi Layer Passwords	(Herzberg, 2003)

Table 1: Summary of Existing Fraud Prevention Measures

Given the information above, two critical success factors can be derived from the review of existing fraud prevention measures. These are:

- *Appropriate Technical Fraud Prevention Measures*
- *Innovative use of Fraud Prevention Technologies*

The table above summarises some of the existing fraud prevention measures and shows how some of the more recent literature is shifting its attention to biometric technologies. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security (Bhattacharyya, 2009). Hence, this type of technology can potentially play a pivotal role in minimising e-banking fraud. Biometric technology is seen as a way forward due to every individual's unique features that can be used for identification. Although advances in biometric technologies such as fingerprint and keystroke dynamics appear promising, (Murdoch, 2010) highlighted that secure authentication solutions need to be both technologically sound and economically viable.

Technological Factors	**Reference to Previous Research**
Strengthening of Authentication Systems using Biometrics	(Jain et al 1997) (Walker and Shearer 2009) (Clarke and Furnell 2007) (Revett et al 2005) (Bleha et al 1990)
Data Encryption	(Shah et al, 2012), (Ganesan & Vivekanandan 2009), (Roberds 1998)
Scalability of Security System	(Moskovitch, 2009)
Authentication solutions being economically viable	(Murdoch, 2010)

Table 2: Summary of Possible Factors Affecting E-Banking Fraud Prevention Systems

The table above highlights factors that researchers have placed emphasis on as a means of improving fraud prevention. Again, biometric authentication appears as a frontrunner and is covered in a number of papers. Research has proved that biometric technology can significantly decrease e-banking fraud and has already been implemented in some banks such as the biometric ATMs by First Bank in Nigeria. However instances of such deployments remain rare. Interestingly, Murdoch & Anderson, (2010) emphasised that authentication solutions need be both technological and economically viable. Therefore beyond looking at the accuracy of biometrics, their false rejection and acceptance rates, the cost of deploying such a technology comes into play. Fingerprint technology isn't the only biometric technology available today with some banks opting to use Keystroke dynamics a behavioural biometric to improve their security.

'Keystroke Dynamics is the process of analyzing the way a users type at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type' (Monrose, 1999). Ecuador bank deployed an Authenware solution to measure online behaviour and keystroke patterns chosen because of its convenience and ability to improve online banking security (PRWEB, 2010). The Bank of Utah also backs this up as they deployed keystroke dynamic technology in a bid to strengthen the scecurity of their internet banking service (Hosseini and Mohammadi 2012). In addition to this, low costs of deployment and minimal changes to the users' modus operandi may make this technology an attractive investment for banks.

Looking beyond technology, there are other factors that affect fraud prevention. Top Management Support has commonly been identified as a CSF for the success of E-Banking and is likely to be applicable as a CSF for Fraud Prevention too. This is because to secure e-banking services, a variety of security measures such as encryption (Shah et al, 2012), passwords (Johnson 2007) and One Time Passwords (OTPs) are used. Therefore changes to the modus operandi will be necessary and this wouldn't be possible without support from the top management. Social and community factors are equally important influencers on the perpetration and prevention of crime (Cecil Eng, 2007). Results from research performed by (Igwe, 2011) agree with this as Socio-Economic factors such as unemployment and poverty both being contributory factors to fraud. Therefore, it is essential that their importance is not underestimated to ensure adequate consideration and emphasis is given.

Banking customers' vulnerability to fraud is another area that has been looked into. (Choplin, 2011) conducted a psychological investigation and found that factors such as education and demographics both had an effect on consumers' vulnerability. This ties closely to the work of Rizzardi (2008) where emphasis is placed on consumer education to protect their personal information to prevent payment card fraud. Similarly Roberds (1998) reaffirms this by highlighting privacy as a factor that affects the risk of fraud. In addition to this, employees who exploit breakdowns in internal controls commit a large proportion of fraud; strict internal controls have been identified as an effective defence measure for fraud (Sidden, 2005). Similarly, Sidden (2005) reiterated where he states that internal controls are the first and best defence against fraud. This therefore places emphasis on the role that internal audits are required to play to ensure compliance.

Given the importance of strict internal controls, it is paramount that not only internal controls exist, but that they are strictly adhered to and policed by internal audits. The importance of internal audits on minimising fraud are highlighted by Coram et al (2008) which concluded that organisations with internal audit functions are more likely to detect and self report fraud than those that don't have internal audit function. In addition to this, the research also found that organisations that have some in-house internal audit function are more effective in detecting and reporting fraud than those that completely outsource the internal audit function. However, it has been argued that internal auditors' are more costly in comparison to outsourced auditors and that some auditors fear from "retaliation" when reporting fraud related to management and seem less independent (Salameh, 2011).

Another likely CSF is organisational learning in the context of fraud vulnerabilities through access to historical lessons learnt. Ganesan (2009) stated, "the open nature of the Internet, transaction security is likely to emerge as the biggest concern among the e-bank's account holders". Signs agreeing with this argument already exist as Roberds (1998) exposes factors from historical lessons learnt where inadequate security measures had led to fraud in retail payment methods. An example was given where cloning that resulted in losses of at least $600 million could beat a store's value cards encryption. Research by Ganesan (2009) reiterates the importance of protecting customer data via encryption and recommends a hybrid model with a hyperelliptic curve cryptosystem to perform the encryption and decryption processes.

An additional security measure that builds on encryption is encouraging the use of agencies that become intermediaries between the customer and banks. Such scenarios help support confidentiality, integrity, and authentication interactions (Tan, 2003) as transactions are not directly linked to the banks systems.

The tables below summarise the factors along with their sources and have been categorised into strategic, managerial, operational and technical factors.

Strategic Factors

Factor	**Reference to Previous Research**
Communication & Timely access to information to empower management decision making	(Shah et al, 2012), (Koskosas 2011), (Sidden, 2005)
Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education	(Somers and Nelson, 2001); (Summer, 1999) (Choplin, 2011)
Awareness of Socio-Economic climate	Igwe (2011) (Cecil Eng et al. 2007)
Engaging Consultants/Specialists	(Somers and Nelson, 2001;)
Organisation learning for fraud prevention	(Roberds 1998)
Adaptive Policies, Procedures and Controls	(Titrade, Ciolacu, & Pavel 2000)
Use of specialist third parties for online transactions to enhance confidentiality.	(Tan, 2003 24)
Using historical data to determine probability of fraud during each transaction	(Fedrizzi, 2004)

Table 3: Summary of Strategic Factors for E-Banking Fraud Prevention

Managerial Factors

Factor	**Reference to Previous Research**
Financial Resources	(Gargeya and Brady, 2005); (AbuAli and Abu-Addose, 2010), (Koskosas 2011)
Management and Employees Readiness to Change	(Somers and Nelson, 2001); (Shah et al, 2012); (AbuAli and Abu-Addose, 2010), (Koskosas 2011)
Top Management Support	(Sommers and Nelson, 2001), (Koskosas 2011)
Change Management as above	(Shah et al, 2012); (Somers and Nelson, 2001);
Ensure Adequate Resources	(Shah et al, 2012), (Koskosas 2011)
Careful Organisational Change	(Shah et al, 2012);

Table 4: Summary of Managerial Factors for E-Banking Fraud Prevention

Operational Factors

Factor	**Reference to Previous Research**
Internal Audit in Banks	(Salameh, 2011)
Strict Customer Data Protection	(Rizzardi, 2008)
Security Specialist Team	(Shah et al, 2012)
Strict Internal Controls	(Sidden, 2005)
Responsive customer service	(Shah et al, 2012)
Regular internal audits	Coram et al (2008)

Table 5: Summary of Operational Factors for E-Banking Fraud Prevention

Technical Factors

Factor	Reference to Previous Research
Strengthening of Authentication Systems using Biometrics	(Lin et al 1997) (Walker and Shearer 2009) (Clarke and Furnell 2007) (Revett et al 2005) (Bleha et al 1990)
Data Encryption	(Shah et al, 2012), (Ganesan & Vivekanandan 2009), (Roberds 1998)
Scalability of Security System	(Moskovitch, 2009)
Low System Administration	(Vandommele, 2010)
Authentication solutions being economically viable	(Murdoch, 2010)
User Friendliness	(Vandommele, 2010)
Integration of Solutions	(Shah et al, 2012)

Table 6: Summary of Technical Factors for E-Banking Fraud Prevention

Although there are similarities in factors relating to securing electronic services across industries, inevitably there will also be factors specific to e-banking. Gibson (2011) argued that CSFs for the banking industry are different, particularly in the case of security. Although the review of various literature has exposed factors that could prove critical in improving fraud prevention systems, additional work needs to be done to understand whether the factors are critical to e-banking fraud prevention.

CONCLUSION

Security issues are major barriers to internet banking and e-commerce activities among consumers (Khasawneh, 2009) with fraud highlighted as an important risk associated with payments systems (Roberds, 1998). To secure an e-banking system, IBM placed emphasis on defining clear objectives. This is achieved by understanding the business goals, objectives and critical success factors when planning the security strategy, as well as the impact on the business if they are not achieved (International Business Machines (IBM), 2001). There has been minimal research related to organisations experience on fraud prevention and the critical success factors for e-banking fraud prevention measures. Hence the factors that have been identified require further investigation to understand their criticality.

Beyond technology, other effective ways to control security risks need to be administered. This can be achieved by having adaptive policies, procedures and controls (Titrade, 2000). The issue of communication was found to play an important role in e-banking security in addition to organizational flexibility, availability of resources, e-banking project alignment, support from top management, information transparency and security knowledge and awareness (Koskosas, 2011). This compliments results from the work of Akindele (2011) where it was found that lack of adequate training, inadequate communication, and weak leadership styles of supervisors and managers as all causes of fraud. In the UK, online banking has witnessed upto a 32% decline in fraud and this has been attributed to increased customer awareness and fraud detection software in banks (UK Fraud Action, 2010). Therefore indicating that beyond the technological aspects, there is significant impact from customer awareness and exposure to fraud precautionary measures.

REFERENCES

Ratiu, C., Craciun., M.D., & Bucerzan, D. (2011). Statistical Model Of The People Confidence In E-Business Services. Analele Universitatii Maritime Constanta, 51, (14) 237-240 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=59564746&site=ehost-live

Khan, M. S., and Mahapatra, S. S. (2009). Service quality evaluation in internet banking: an empirical study in India. Int. J. Indian Culture and Business Management, 2(1), pp.30-46

Sathye, M. (1999). Adoption of internet banking by Australian consumers: an empirical investigation. International Journal of Bank Marketing, 17(7), 324-334.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., Pahnila, S. (2004) "Consumer acceptance of online banking: an extension of the technology acceptance model", Emerald 14,

Kitchenham, (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering.

Finfgeld-Connett, D. & Johnson, E.D. (2013). Literature search strategies for conducting knowledge-building and theory-generating qualitative systematic reviews. Journal of Advanced Nursing, 69, (1) 194-204 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=84385897&site=ehost-live

Masocha, R., Chiliya, N. and Zindiye S, (2010). 'E-banking adoption by customers in the rural milieus of South Africa: A case of Alice, Eastern Cape, South Africa'. [online] Available at: <http://www.academicjournals.org/AJBM/PDF/pdf2011/4Mar/Masocha%20et%20al.pdf> [Accessed 29 March 2012]

Auta. (2010). E-BANKING IN DEVELOPING ECONOMY: EMPIRICAL EVIDENCE FROM NIGERIA. Journal of applied quantitative methods, 5(2)

Agboola, A. Salawu, O. (2008). Optimizing the Use of Information and Communication Technology (ICT) in Nigerian Banks. Journal of Internet Banking and Commerce, 13(1)

Angelakopoulos, G. & Mihiotis, A. (2011). E-banking: challenges and opportunities in the Greek banking sector. Electronic Commerce Research, 11, (3) 297-319 available from:http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=23362267&site=ehost-live

Shah, M.H., (2012). Critical Success Factors in e-Banking: A Study of Two UK Retail Banks

Roberds, W. 1998. The impact of fraud on new methods of retail payment. Economic Review (07321813), 83, (1) 42 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=632409&site=ehost-live

Central Bank of Nigeria, (2012). CBN Annual Report 2010. [online] Available at: <http://www.cenbank.org/Out/2011/publications/reports/rsd/AR2010/Annual%20Report%202010.html> [Accessed 15 January 2012]

Adams, R. (2010). Prevent, protect, pursue preventing fraud. Computer Fraud & Security, 2010, (7) 5-11 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=52878189&site=ehost-live

Giles, J. (2010). The problem with online banking. New Scientist, 205, (2745) 18-19 available from: http://www.sciencedirect.com/science/article/pii/S0262407910602242

Cecil Eng, H.C., Wareham, J., & Robey, D. (2007). THE ROLE OF ONLINE TRADING COMMUNITIES IN MANAGING INTERNET AUCTION FRAUD. MIS Quarterly, 31, (4) 759-781 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=27391969&site=ehost-live

Chang, W.H. & Chang, J.S. (2012). An effective early fraud detection method for online auctions. Electronic Commerce Research and Applications, 11, (4) 346-360 available from: http://www.sciencedirect.com/science/article/pii/S1567422312000191 Accessed August 2012.

May, D. (2010). The new fraud offensive. Modern Healthcare, 40, (26) 26 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51928564&site=ehost-live

Ormerod, T.C., Ball, L.J., & Morley, N.J. (2012). Informing the development of a fraud prevention toolset through a situated analysis of fraud investigation expertise. Behaviour & Information Technology, 31, (4) 371-381 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=74188608&site=ehost-live

Estavez, P.A., Held, C.M., & Perez, C.A. (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. Expert Systems with Applications, 31, (2) 337-344 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=20622472&site=ehost-live

Legal Practitioner, (2013). An Introduction To Corporate Regulation and Standardization [Online] Available at: url:http://legal.practitioner.com/regulation/standards_9_2.htm [Accessed 15 March 2013]

wiseGeek. (2013). What is Bank Fraud?. [Online] Available at:<url: http://www.wisegeek.com/what-is-bank-fraud.htm> [Accessed on 13 March 2013]

Aransiola, J.O. & Asindemade, S.O. (2011). Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. Cyberpsychology, Behavior, and Social Networking, 14, (12) 759-763 available from: http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=26521700&site=ehost-live

Sidden, K. & Simmons, D. (2005). Banking on security. American City & County, 120, (11) 30 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=18651183&site=ehost-live

Benjamin, O.A. & Samson, B.S. (2011). Effect of perceived inequality and perceived job insecurity on fraudulent intent of bank employees in Nigeria. Europe's Journal of Psychology 99-111 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=60039658&site=ehost-live

Amtul, F. (2011). E-Banking Security Issues – Is There A Solution in Biometrics? Journal of Internet Banking and Commerce, 16(2).

Rockart, J. (1979). "Chief executives define their own information needs". Harvard

Business Review, 81-92.

Butler, T. & Fitzgerald, B. (1999). Unpacking the systems development process: an empirical application of the CSF concept in a research context. The Journal of Strategic Information Systems, 8, (4) 351-371 available from: http://www.sciencedirect.com/science/article/pii/S0963868700000275

Amid, A., Moalagh, M., & Zare Ravasan, A. (2012). Identification and classification of ERP critical failure factors in Iranian industries. Information Systems, 37, (3) 227-237 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=70262427&site=ehost-live

Aziz, N. Saleh, H (2011). People Critical Success Factors of IT/IS Implementation: Malaysian Perspectives. World Academy of Science, Engineering and Technology, 56

Umble, E. and Umble, M. (2001). Enterprise Resource Planning Systems: A Review of Implementation Issues and Critical Success Factors. Paper presented at the 32nd Decision Sciences Institute Annual Meeting, San Francisco, USA.

Rockart, J. and Van Bullen, C (1986). A Primer on Critical Success Factors. The Rise of Management Computing. Homewood: Irwin.

Shah, M.H. & Siddiqui, F.A. (2006). Organisational critical success factors in adoption of e-banking at the Woolwich bank. International Journal of Information Management, 26, (6) 442-456 available from: http://www.sciencedirect.com/science/article/pii/S0268401206001101

Roberds, W. (1998). The impact of fraud on new methods of retail payment. Economic Review (07321813), 83, (1) 42 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=632409&site=ehost-live

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Lohlein, B., Heister, U., Moller, S., Rokach, L., and Elovici, Y., (2009). Identity Theft, Computers and Behavioral Biometrics. [Online] Available at: < http://dl.acm.org/citation.cfm?id=1706455 > [Accessed 20 March 2012]

Vandommele, T (2010). Biometric Authentication Today. [Online] Available at: < http://www.cse.hut.fi/en/publications/B/11/papers/vandommele.pdf> [Accessed 15 April 2013]

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric Authentication - A Review. International Journal of u- and e- Service, Science and Technology, 2, (3)

Akinyemi Ibidapo, O., Omogbadegun, Z.O., & Oyelami, O.M. (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. International Journal of Electrical & Computer Sciences, 10, (6) 68-73 available from: http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=62093371&site=ehost-live

Sherman, E (2002). Fighting Web Fraud. Newsweek June 10. [online] Available at: < http://www.tlsi.net/articles/Newsweek%20_061002.pdf> [Accessed 15 April 2013]

Johnson, M., and Moore S., (2007). A New Approach to E-Banking, University of Cambridge. [online] Available at: < http://www.matthew.ath.cx/publications/2007-Johnson-ebanking.pdf > [Accessed 20 March 2012]

INFORM, (2004). How can a Bank prevent Online Banking Fraud? [online] Available

at:<http://internetbankingfraud.com/> [Accessed 26 November 2011]

Herzberg, A. (2003). P**ayments and banking with mobile personal devices.** Communications of the ACM - Wireless networking security, 46(5)

Murdoch, S. & Anderson, R. (2010), "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication," In Financial Cryptography and Data Security, 6052 ed. R. Sion, ed., Springer Berlin Heidelberg, pp. 336-342.

PRWEB,. (2010). AuthenWare Expands Financial Services Clientele by Nearly a Half-million Portals. [Online] Available at: < http://www.prweb.com/releases/2010/02/prweb3525574.htm> [Accessed 18 March 2013]

Hosseini, S., Mohammadi, S. (2012). Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System. Journal of Basic and Applied Scientific Research, 2(9)

Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 19, (4) 302-314

Revett, K. (2009). A Bioinformatics Based Approach to user Authentication via Keystroke Dynamics, International Journal of Control, Automation, and Systems, 7(1)

Bleha, S., Slivinsky, C., Hussain, B.(1990). "Computer-Access Security Systems Using Keystroke Dynamics". IEEE Trans.Pattern Anal. Machine Intelligence., 12(12)

Ganesan, R. & Vivekanandan, K. (2009). A Secured Hybrid Architecture Model for Internet Banking (e-Banking). Journal of Internet Banking and Commerce, 14, (1) available from: http://www.arraydev.com/commerce/JIBC/2009-04/JIBC-Ganesan%20R.pdf

Murdoch, S. & Anderson, R. (2010), "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication," In Financial Cryptography and Data Security, 6052 ed. R. Sion, ed., Springer Berlin Heidelberg, pp. 336-342.

Monrose, F., and Rubin, AD., (1999), 'Keystroke Dynamic as a biometric authentication'. [Online] Available at:< http://avirubin.com/fgcs.pdf> [Accessed 7 March 2012]

Igwe, C.N. (2011). Socio-Economic Developments and the Rise of 419 Advance-Fee Fraud in Nigeria. European Journal of Social Science, 20, (1) 184-193 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=67493593&site=ehost-live

Choplin, J.M., Stark, D.P., & Ahmad, J.N. (2011). A PSYCHOLOGICAL INVESTIGATION OF CONSUMER VULNERABILITY TO FRAUD: LEGAL AND POLICY IMPLICATIONS. Law & Psychology Review, 35, 61-108 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=67026670&site=ehost-live

Rizzardi, R. (2008). Financial Management -- Payment Card Fraud Can Happen to You. Optometry & Vision Development, 39, (2) 64-65 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=32871069&site=ehost-live

Sidden, K. & Simmons, D. (2005). Banking on security. American City & County, 120, (11) 30 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=18651183&site=ehost-live

Coram, P., Ferguson, C. & Moroney, R. (2008). Intemal Audit, Altemative Intemal Audit Structures and the Level of Misappropriation of Assets Fraud. Accounting & Finance, 48(4), 543-559.

Salameh, R., Al-Weshah, G., Al-Nsour, M., & Al-Hiyari, A. (2011). Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention: Evidence from Jordanian Banking Industry. Canadian Social Science, 7, (3) 40-50 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=79201535&site=ehost-live

Tan, J., Titkov, L., & Poslad, S. (2003), "Securing Agent-Based e-Banking Services," In Trust, Reputation, and Security: Theories and Practice, 2631 ed. R. Falcone et al., eds., Springer Berlin Heidelberg, pp. 148-162.

Koskosas, I. (2011). E-banking security: A communication perspective. Risk Management, 13, (1-2) 81-99 available from: http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=24754949&site=ehost-live

Titrade, C., Ciolacu, B., & Pavel, F. E-Banking: Impact, Risks, Security. (2000). Ref Type: Online Source

Fedrizzi, M., Molinari, A., & Ventre, V. (2004) A model for evaluating the transaction risk in e-banking. e-society International conference, e-society; 172-178

Vidyaranya B. Gargeya, Cydnee Brady, (2005) "Success and failure factors of adopting SAP in ERP system implementation", Business Process Management Journal, 11(5)

AbuAli, A.N. & Abu-Addose, H.Y. (2010). Data Warehouse Critical Success Factors. European Journal of Scientific Research, 42, (2) 326-335 available from: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=50994847&site=ehost-live

Khasawneh, A., Al Azzam, I., & Bsoul, M. (2009). A study on e-commerce security in Jordan. International Journal of Electronic Finance, 3, (2) 166-176 available from: http://dx.doi.org/10.1504/IJEF.2009.026358

International Business Machines (IBM). (2001), A Security Strategy for Mobile E-Business. [Online] Available from: http://www-935.ibm.com/services/in/bcs/pdf/gsoee213-a-security-strategy-for-mobile-e-business.pdf

Akindele, R. I. (2011). Fraud as a Negative Catalyst in the Nigerian banking Industry. Journal of Emerging Trends in Economics and Management Sciences, 2(5), 357-363.

Williams, J. J. and Ramaprasad, A. (1996) A taxonomy of critical success factors, European Journal of Information Systems, 5