Journal of Educational Policy and Entrepreneurial Research (JEPER)
ISSN: 2408-770X (Print), ISSN: 2408-6231 (Online)
Vol.2, N0.3, March 2015. Pp 1-7

Factors Affecting the Online Transactions in the Developing Countries: A Case of E-Commerce Businesses in Nairobi County, Kenya

Paul Muriku Kanyaru[1] and Josphat K. Kyalo[2]

[1] BSC [Computer Science], MBA [MIS] candidate, P.O BOX, 25923-00100, Nairobi, Kenya
murikuh@gmail.com

[2] BSC, MSC [IS], PhD (Candidate), P.O. Box 222 – 00519; Mlolongo, Kenya
joskyalo@gmail.com

Abstract
The growth in online transactions is accompanied with an increase in the incidences of fraud. In the online marketplace, fraudsters are using sophisticated malware to take over accounts and commit fraud related activities. At the global level, online fraud is rampant with high financial losses for customers and online merchants. In Kenya, the scope of online fraud is still small, however, the increasing adoption of e-commerce is anticipated to increase fraud related incidences. Based on this, this study reviewed literature on challenges associated with internet fraud and best practices that can be adopted by online merchants. It was shown that the challenges are related to the use of improper theft and security measures by online merchants, the increase of mobile devices and lack of customer awareness of security risks in online transactions. To prevent internet fraud, organizational, consumer, and technical measures have to be adopted by online merchants in Kenya.

Keywords: E-Commerce, Internet Fraud, E-Merchants, Online Transactions, Security Risks, Security Measures, Customer Awareness

Introduction

The advancement of the internet and the consequent development of electronic commerce have result in a dynamic operating environment where business transactions are conducted over the internet. Internet transactions are a critical element of e-commerce as business transactions such as buying and selling of products and services and communication are conducted over the internet (Janita & Chong, 2013). According to Lawrence & Tar (2010), internet transactions provide great opportunities for businesses in terms of gaining access to markets across the globe and a driver of the economy a developing country such as Kenya.

Ghobakhloo, Arias-Aranda and Benitez-Amado (2011) contended that the adoption of internet transactions has significantly supported the growth of businesses and holds a promise in the reduction of costs and improvements in the operational efficiency. Businesses have migrated to online transactions in order to benefit from increased efficiency, reduced costs,

and the ability to operate across the various platforms in real time. One of the major reasons as to why there has been a rapid growth in online transactions is that it has a considerable effect on the productivity and costs of the business. Specifically, they have assisted businesses and organizations to reduce the costs associated with marketing, advertising, sales, and other transactions. In addition, online transactions have been useful in terms of assisting businesses to reach markets across the globe irrespective of the time zones (Terzi, 2011).

The adoption of internet transactions is expected to enhance business performance through reduced transaction costs and improved coordination of economic activity among partners in business (Olatukun & Bankole, 2011). The real effect of online transactions on the economy is that they reduce the costs and prices and make doing business more efficient. Increased productivity comes about as a result of reduced costs of production, lower costs of holding inventory, and reduced costs of inputs for the business. This has a considerable influence on the interactions between businesses (Suryani & Subagyo, 2011). Abou-Shouk (2011) summarized the benefits of internet transactions in the economy as; expansion of the marketplace to national as well as international markets, reduced costs of information creation, storage, processing and distribution, minimization of delivery delays, and its ability to allow businesses to closely interact with their customers.

MacGregor (2011) argued that some of the economic benefits that can be reaped from online transactions include; increased sales, increased productivity, and economies of scale across the operational processes of the business. Online transactions allow businesses to expand the customer base through the penetration into global markets due to enhanced access to information on an international scale. Through online transactions, small businesses can improve most aspects of their operations and in turn improve their internal efficiency. This in turn results in improved performance of the business while enhancing efficiency in the supply chain.

The Organization for Economic Cooperation and Development (OECD) identifies a number of benefits that can be reaped from adopting internet transactions by businesses (2013). First, they transform the marketplace by changing the manner in which business is carried out. Particularly, they replace the traditional intermediary transactions and results in the growth of new markets as well as products. Due to internet transactions, relationships between the business and its customers have become closer. Second, electronic commerce has significantly increased interactivity within the economy and this extends even to small firms that hope to reach out to the entire world. Online transactions have increased the ability of people to communicate as well as to carry out business in virtually any location and at any time and this has eroded the geographic as well as economic boundaries. Third, internet transactions have a catalytic effect as they accelerate as well as diffuse the changes that are already taking place in the economy such as the globalization of economic activity and the establishment of electronic links between businesses. Various business trends have largely been accelerated due to the evolution of online transactions such as direct booking of transport and electronic banking (OECD, 2013). Finally, e-commerce has altered the relative significance of time as it has speeded up the cycles of production and enabled the businesses to operate in close coordination and the consumers to conduct commercial transactions across the clock (OECD, 2013).

However, the benefits of online transactions are negatively affected by fraud. Indeed, there has been an increase in internet fraud cases in Kenya. For instance, it is reported that in the

initial six months of 2014, $9.4 million was stolen by fraudsters from commercial banks through the exploitation of gaps found in online banking solutions (Olingo, 2014). Further statistics indicate that $2.6 million was lost via electronic transfer crime, while $13,403 was lost through internet scams, and computer fraud accounted for $138, 683 in financial losses in commercial banks (Olingo, 2014). Recently, 7 Chinese nationals were arrested for suspicion of being involved in internet fraud (Smith, 2014).Given the prevalence of internet fraud, it is important to examine best practices in preventing fraud and the challenges faced in dealing with fraud associated with online transactions. Therefore, this case study addresses two questions: what are the challenges faced in preventing internet fraud; what are the best practices for dealing with fraud in online transactions?

Literature Review

According to Schneider (2011), the level of fraud in online transactions is higher than telephone or in-person transactions of the same nature. Although less than 10% of credit card transactions occur in the online environment, they still account for nearly 70% of fraud associated with credit cards (Schneider, 2011). The internet is a perfect medium for fraudsters as it provides them with anonymity of committing this crime to a large victim pool in various remote locations (Excell, 2012). Online transaction fraud is of various dimensions including stealing personal identification information such as bank account number or credit number and using it repeatedly for completing transactions in the actual individual's name (Fernandes, 2013). Another form of fraud associated with online transactions is account hacking that is characterized by unauthorized access to an organization's or customer's account and then engaging in fraudulent activities.

Finally, phishing involves the acquisition of confidential data from a user where the fraudulent hacker poses as a trusted party. In this type of fraud, the attacker sends malware in hyperlinks or attachments in emails which appear to have been sent by a legitimate organization (Fernandes, 2013). When the user clicks on the hyperlink or attachment, his or her system gets infected with a malware. In the next online transaction, the malware is activated and used in stealing personal and private financial information such as personal identification number or credit card number that the fraudster utilizes in stealing money from the users account.

Various measures are currently being used to prevent fraud in online transactions. These are proactive measures that focus on identifying the potentiality of internet fraud occurring and preventing it based on the risk level associated with it (Excell, 2012). For instance, Secured Socket Layer (SSL) is used by e-commerce platforms to ensure the confidentiality of the customer's personal data through encryption of such information (Fernandes, 2013). In addition, fraud detection tools are available for preventing fraudulent activities in online transactions. For instance, the Universal Payment Identification Code enables online merchants to receive electronic payment devoid of disclosing any confidential information (Fernandes, 2013). Similarly, fraud detection software is utilized for detecting fraud by providing fraud results that enables the online merchant in making decisions related to acceptance, rejection and review of the transaction (Fernandes, 2013).

Conversely, there are various challenges related to preventing fraud in online transactions. In a white paper titled ``*Five Trends to Track in E-Commerce Fraud''*, ThreatMatrix identified important challenges. One of the challenges identified is that online transactions are increasingly being conducted over mobile devices that lack anti-malware and anti-virus

defenses that have been developed for desktop systems (ThreatMatrix, 2013). In this regard, mobile devices provide fraudsters with unprotected platforms for the delivery of malicious code and this increases opportunities for fraudsters to execute attacks during online transactions. Another challenge is that fraudsters are using refined techniques for initiating fraud-related attacks in internet transactions as online merchants lack robust theft and fraud protection systems (ThreatMatrix, 2013). According to Fernandes (2013), consumers' awareness in terms of potential risks is important for ensuring that they adopt cautious and active attitudes when performing internet transactions. Therefore, lack of consumer awareness is another challenge to preventing online transaction fraud.

Literature Summary

The review of literature has indicated that fraud in online transactions is very high due to the anonymity provided by the internet. Such fraud takes various forms including phishing, account hacking and stealing of personal information all of which reduce trust in e-commerce transactions. It has been shown that online fraud can be dealt with using fraud detection tools and software as well as through encryption. Conversely, there is need to consider the challenges associated with the prevention of online fraud including lack of consumer awareness, poor fraud detection systems, and lack of malware protection on mobile devices.

Methodology

The research methods used include a review of secondary data. Secondary data analysis involves using data that already exists or which has been collected by a different researcher with a different research question or for other studies. The approach used in collecting the secondary data for this research was obtained from various external sources including scholarly journals, books and credible publications. The information from these data sources was used for writing this report.

Discussion

Globally, internet fraud is increasing at a rapid rate. Although the development of digital and internet technologies have transformed businesses and provided tools for daily communication in the UK, they have also provided opportunities for cyber crime to be committed including fraud (McGuire & Dowling, 2013a). In a review of evidence on cyber fraud, it was found that different types of fraud were reported in the UK. For instance, 3% of 8,373 internet users reported that they had money when using the internet (McGuire & Dowling, 2013b). Furthermore, it was reported that 5% of 1518 internet users experienced financial losses when their debit or credit cards was misused online(McGuire & Dowling, 2013b). Another finding is that 12% of internet users were victims of identity fraud where their personal data was used by someone else for impersonating the actual owners (McGuire & Dowling, 2013b).

Online fraud is also reported in Australia, especially fraud associated with card not present transactions that refers to online shopping. Credit not present fraud in the online market place is a major challenge to online merchants as physical verification aspects found in the brick and mortar organizations are non-existent in e-commerce platforms (Prabowo, 2011). In the online market place, neither the cardholder nor the card is present and the merchant cannot authenticate the cardholder. Statistics show that online fraud in Australia increased to $219.7 million in 2013 from $183.1 million in 2012 and accounted for 72% of overall card fraud in 2013 (Australian Payments Clearing Association, 2014). In the USA, card not

present fraud accounted for the largest category of $1.92 billion in financial losses faced by online merchants (Smart Card Alliance, 2014).

A comparison of internet fraud in Kenya and other countries such as the USA, Australia, and UK indicate critical differences in terms of scope. Specifically, amount of financial losses associated with internet fraud in Kenya is low at only $9.4 million. However, cases of internet fraud are expected to rise in Kenya due to the growing adoption of e-commerce platforms. Due to such expectations, there are various critical success factors that have to be considered to minimize online fraud in Kenya. First, online merchants need to adopt new security measures as traditional techniques of authenticating individuals via passwords and usernames are no longer adequate (Usman & Shah, 2013).

Consequently, advanced techniques such as random knowledge based authentication where users are used randomly chosen secret questions for confirming their identity as well as end-point methods for identifying the device used by the users in accessing a specific online merchant(Smart Card Alliance, 2014). Second, online merchants need to put in place stringent internal controls to prevent online fraud by employees exploiting vulnerabilities in the e-commerce platform (Usman & Shah, 2013). It is noted that internal security audits assist the organization in detecting and dealing with fraud committed by its employees. According to Akindele (2011), weak leadership by organizational managers and supervisors, poor communication and inadequate training of employees on security policies associated with the online marketplace were major causes of fraud. Such issues highlight the importance of having robust internal controls to promote security and prevent fraud in online transactions.

Third, there is need for consumer awareness of security in the online marketplace is another effective mechanism for preventing online transaction fraud (Aleem & Anti-Boasiako, 2011). In this regard, consumers are educated on suspicious activities during online transactions to ensure that they are well informed to prevent unauthorized access to credit card information or accounts.

Finally, using intermediaries is another approach that online merchants should consider using to increase integrity and confidentiality in authentication of online transactions (Usman & Shah, 2013). For instance, online merchants in Kenya should consider using intermediaries who are involved in performing risk assessment of every online transaction to enable the implementation of varied security approaches (Smart Card Alliance, 2014). Such assessments examine different information sources including the browsing history, visits from a specific internet protocol address, and recent activity on a credit card to score risks and detect any signs of fraud (Smart Card Alliance, 2014). Therefore, outsourcing the function of authentication of the identity of users to an intermediary safeguards both the customers and online merchant from fraud related activities (Usman & Shah, 2013).

Conclusion

This article has examined the issue of internet transaction in the context of Kenya by focusing on the issue of online transaction fraud. It has examined the issues surrounding fraud in e-commerce transactions. Specifically, this is associated with the challenges in the online market place including lack of customer awareness on the security risks found in online transactions, increased use of mobile devices with high vulnerabilities, and the increasing sophistication of fraudsters' attacks. The results also identified the best practices that can be

used in the context of Kenya to prevent online transaction fraud. These included robust security systems for detection and prevention of fraud related attacks, continuous detection and conventional protection measures, incident management plans, and regular security assessments.

Therefore, the implementation of these best practices will enable online merchants to continue enjoying the benefits brought about by online transactions while preventing fraud. Furthermore, online merchants should consider using intermediaries to enhance authentication in online transactions and also perform internal audits to prevent fraud carried out by employees. Similarly, prevention of internet fraud should extend to customers by educating them on risks associated with online transactions to ensure they are well informed to deal with this issue. Therefore, implementation of the identified strategies at the organizational, technical, and consumer level will ensure that online merchants benefit from online transactions while preventing online fraud.

Recommendations

Given that e-commerce platforms are rapidly increasing in Kenya, it is important that appropriate security measures are put in place to ensure confidentiality and integrity of sensitive information. Based on this, the following recommendations are suggested for organizations operating e-commerce platforms in Nairobi. First, there is need for enterprise risk management and governance for e-commerce platforms. Concerning governance, organizations need to identify and address threats related to protecting sensitive data in e-commerce transactions. Furthermore, organizations should focus on governing, assessing and managing enterprise risks related to confidential data in e-commerce transactions.

The various organizations need to perform internal and external audits to establish assurance that the risk management activities associated with the security of information in e-commerce transactions is guided by best practices. There is need for robust data security and information management in e-commerce transactions. In this regard, information management includes the processes and policies used by e-commerce firms in the creation, storage, use, sharing and destroying of information used in online transactions. Similarly, robust data security through encryption is necessary for ensuring the integrity of sensitive information utilized in e-commerce transactions.

References

Abou-Shouk, M. (2011). Factor Analysis of E-commerce Adoption Benefits: A Case of Egyptian Travel Agents. *Information and Communication Technologies in Tourism,* 305-317.

Akindele, R. (2011). Fraud as a negative catalyst in the Nigerian banking industry. *Journal of Emerging Trends in Economics and Management Sciences, 2*(5), 357-63

Aleem, A., & Antwi-Boasiako, A. (2011). Internet auction fraud: the evolving nature of online auctions criminality and the mitigating framework to address the threat. *International Journal of Law, Crime and Justice, 39*, 140-60

Australian Payments Clearing Association (2014). Australian payments fraud: details and data. Retrieved from http://apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2014.pdf

Excell, D. (2012). Bayesian inference-the future of online fraud protection. *Computer Fraud & Security*, 8-11

Fernandes, L. (2013). Fraud in electronic payment transactions: threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review*, *2*(3), 23-32

Ghobakhloo, M, Arias-Aranda, D, & Benitez-Amado, J. (2011). Adoption of e-commerce applications in SMEs. *Industrial Management and Data Systems*, 111, 1238 – 1269.

Janita, I., & Chong, W. (2013). Barriers to B2B E-business adoption in Indonesian SMEs: a literature analysis. *Procedia Computer Science, 17*, 571-78

Lawrence, J. & Tar, U. (2010). Barriers to ecommerce in developing countries. *Information, Society and Justice,* 3(1), 23-35

MacGregor, R. (2011). Perception of Barriers to e-Commerce adoption in SMEs in a Developed and Developing Country: a Comparison between Australia and Indonesia. *Journal of Electronic Commerce in Organizations,* 8(1), 61-82

McGuire, M., & Dowling, S. (2013b). *Chapter 2: cyber-enabled crimes-fraud and theft*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

McGuire, M., & Dowling, S. (2013a). *Cyber crime: a review of the evidence: summary of key findings and implications*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

OECD (2013). *Electronic and mobile commerce*. Retrieved from http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE/IIS%282012%291/FINAL&docLanguage=En

Olatokun, W. & Bankole, B. (2011). Factors Influencing Electronic Business Technologies Adoption and Use by Small and Medium Scale Enterprises (SMES) in a Nigerian Municipality. *Journal of Internet Banking and Commerce,* 16(3), 1-26

Olingo, A. (2014). *Kenya's commercial banks lose $9.4m to fraud in just six months*. Retrieved from http://www.theeastafrican.co.ke/news/Kenyan-commercial-banks-lose--9-4m-to-fraud-in-just-six-months/-/2558/2523802/-/rd9jyuz/-/index.html

Prabowo, H. (2011). Building our defense against credit card fraud: a strategic view. *Journal of Money Laundering Control*, *14*(4), 371-86

Schneider, H. (2011). *E-business*. India: engage learning

Smart Card Alliance (2014). *Card not present fraud: a primer on trends and authentication processes*. Retrieved from http://www.smartcardalliance.org/resources/pdf/CNP-WP-FINAL-022114.pdf

Smith, A. (2014). *77 Chinese nationals arrested in Kenya for cybercrimes*. Retrieved from http://www.newsweek.com/77-chinese-nationals-arrested-kenya-cybercrimes-289539

Suryani, T, & Subagyo, I. (2011). Adoption Intention and Benefits of E-Commerce Usage in Business: An Exploratory Study. *SSRN Working Paper Series*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1882247

Terzi, N. (2011). The impact of e-commerce on international trade and Employment. *Procedia Social and Behavioral Sciences,* 24,745–753

ThreatMatrix (2013). *Five Trends to track in E-commerce fraud*. Retrieved from http://info.threatmetrix.com/rs/threatmetrix/images/Five_Trends_eCommerce_Fraud_WP

Usman, A., & Shah, M. (2013).Critical success factors for preventing e-banking fraud. *Journal of Internet Backing and Commerce*, *18*(2), 1-15