

Factors Determining Vulnerability of Automated Teller Machines to Insecurity Against Commercial Banks in Nairobi County Kenya

Ocharo Becky Osebe¹ | Samson Wokabi Mwangi² | Panuel Mwaeke³

¹Student, Department of Peace Security Social Sciences, Egerton University Kenya

²Department of Peace Security Social Sciences, Egerton University, Kenya

³Department of Peace Security Social Sciences, Egerton University, Kenya.

Received 05-04-2024

Revised 07-04-2024

Accepted 23-04-2024

Published 24-04-2024



Copyright: ©2024 The Authors. Published by Publisher. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

Abstract:

This paper uses data collected for an MA Thesis on assessing the factors determining vulnerability of ATMs to insecurity among commercial banks in Nairobi County, Kenya. The study was conducted in three commercial banks located in the Nairobi City County. Specifically, the study established the various types of ATM crimes among commercial banks, examined the impact of bank internal control mechanisms, established the effect of ATM location on vulnerability of ATMs to insecurity, and evaluated the influence of ATM user competence on vulnerability of ATMs to insecurity. The study was guided by Fraud triangle theory and crime prevention through environmental design theory. Descriptive research design was adopted. The study targeted 2391 employees in the commercial banks in the study area. The study utilized proportionate stratified to select a sample of 96 respondents while purposive sampling techniques in selecting key informants for interviews. Questionnaire and key informant interviews were the methods of data collection. Descriptive statistics and content analysis were the methods of data analysis. Main types of ATM crimes established among commercial banks in Nairobi County include; theft by fraudulent electronic transactions (31%), theft by electronic data interception (24%), vandalism of ATMs (18%), and robbery of couriers who fill ATMs with cash (5%). According to this study, commercial banks have formulated and adopted information security policy, implemented audit policy which allows for regular auditing in identifying possible irregularities related to ATM crimes, and inadequate employee trainings on fraud detection, response and reporting that was observed to have an effect on curbing the ATM related insecurity. Thirdly, although the commercial banks have done much to curb ATM related crime, there are gaps that need to be addressed. According to the last objective, commercial banks have not adequately educated their customers on risks associated with using ATM use and related frauds that led to vulnerability of the users. Amongst other recommendations the study recommended target hardening of ATMs clients by investing in innovations that enhance security of electronic transactions and related crimes. Further the study recommends beefed up user education, increased regular ATM audits, embrace the ergonomic designs of ATMs to assist in recessing the monitor display more deeply within the terminal to provide adequate security against shoulder surfing.

Key Words: Security Vulnerability, Automated Teller Machine Security.

Introduction:

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions either within the bank building or in a convenient public space (Snellman, 2006). With the use of an ATM, customers can access their bank accounts for cash withdrawals and check their account balances either inside the premises of banks, or in ATMs placed in different locations such as shopping centers/malls, airports or restaurants. The emerging global trend however is that the security of ATMs and that of users against criminal attacks is still a challenge. (Scott, 2001). In a recent study in the US, Shinde, Chingale, Dhane and Vader (2017) argued that although the ATM technology has simplified and increased the banking activity in many countries, it has also tremendously increased crimes such as robberies, ATM vandalism, ATM frauds amongst other ATM related crimes to the detriment of the financial institutions. Given their impact to impoverish the society and inculcate fear or scare the investors, rise of ATM crimes may affect the economic activity of a place. Rise of such crimes indicate that there is still more that needs to be done to manage ATM crimes more so in Nairobi County, Kenya.

Globally, several other types of ATM crimes were reported. For example, the year 2016 alone more than \$2 billion with respect to ATM skimming all around the world was lost. Additionally, the skimming frauds amounted to 33% of all the fraudulent activities that occur globally and the losses that occurred or took place are 98% because of the skimming crime (FFA UK, 2017). Further, statistics of the European ATM Security Team (EAST) show that around 18,738 incidents have been reported against the ATM crimes in Europe since 2015. According to Financial Fraud Action (FFA) in the UK, these rounds up to around 51 attacks for every 1000 ATMs attack over a certain period of time which means that there is a 19% increase since the previous year that is 2014 (FFA UK, 2015). Reports of EAST say that in 2015 around 327.48 million euros were lost. This was a

total of 17% increase when compared to the loss incurred or that took place in 2014, which was around 279.86 million euros. These losses amount to a loss of around 884,069 euros for every ATM (FFA UK, 2015).

In the East Africa Region, ATM related crimes present a significant challenge for financial institutions with card frauds, phishing attacks on customer accounts, and physical attacks reported as the most significant forms of ATM crimes (PWC, 2019; Mgaya, 2015). In Tanzania, physical security of ATM and protection of cardholder's PIN from theft and attack from criminals have been and still is a challenge to most of banks in Tanzania particularly because security is often overlooked. A banking institution may have purchased the best security technologies to protect ATM and trained their employees and customers so well that they lock up all their secrets before initiating any ATM transaction, and hired building guards from the best security firm in the business. However, if the environment in which the ATM is located is not well assessed from security viewpoint, that institution is still unsecured (Mgaya, 2015). In Kenya, there are more intricate and distinct ATM robbery patterns, each of which presents unique challenges in responding. The most common pattern of robbery at an ATM is for the offender to rob the ATM user immediately after the victim makes a withdrawal or the offender forces the victim to go to an ATM to withdraw cash after he robs the victim of his or her ATM card (Murigu, 2008). Despite the banks adopting some security measures, to target harden and insulate ATMs against criminal attacks, ATM crimes have continued to rise in Nairobi County, apparently causing irreparable damages, hence the rationale for this study. This study therefore seeks to investigate the factors that contribute to ATM vulnerability to various forms of insecurity with a focus on security systems, organizational management culture, ATM location and customer competence.

Problem Analysis:

Security of automated teller machine (ATM) is one of the emerging global challenges threatening

many states, more so in Kenya. Despite the fluidity of the problem, the National Police Service Crime Reports have categorized ATM insecurity under other major categories of crime, hence silent about the escalation of ATM insecurity. This study however, attempted to bring such crimes to the limelight because of the irreparable damage that these crimes have done to society albeit unnoticed by many scholars. For example, in Kenya, banks are increasingly finding it difficult to cope with huge requests to compensate hundreds of millions of shillings in ATM card skimming and their customers are worried on the fate of their deposits. There is very little that has been done through research to address this issue. Besides, there has never been any systematic and detailed inquiry that has been done on ATMs security and safety. This study assumed that security measures to prevent ATM robberies, Securing PIN and preventing cardholders from attack at ATM site are amongst other measures still inadequate given the rising trends of ATM crimes especially in the NCBK in Nairobi County, Kenya, hence the rationale for this study.

Methodology:

The study used a Descriptive Research Survey Design to investigate the problem under the study because it allows subjects to be observed and described without any manipulation (Obwatho, 2014). The study used proportionate stratified sampling and purposive sampling techniques to enlist 96 respondents into the study. This technique was suitable because the target population was subdivided into strata (Kothari, 2012). On the other hand, purposive sampling technique was appropriate because it helped the researcher acquire privileged information (Kothari, 2012). Questionnaire and key informant interviews were used to collect data. Descriptive statistics and content analysis were used to analyze data. Quantitative data was analyzed using Statistical Package for Social Sciences (SPSS Version 23) and presented using frequency distribution tables, graphs and pie charts.

Results and Discussion:

The researcher reached 95 out of the 96 targeted respondents which translated to 99% response rate. This is because some of the respondents were out on duty during the entire period of the data collection exercise. According to Mugenda and Mugenda (2003), a response rate of more than 70% is very good, a 60% response rate is considered good while 50% of the response is considered adequate for analysis. Thus the 99% response rate was considered very good and ideal for this research.

Types of ATM Crimes Among Commercial Banks in the Study Area:

The study sought to investigate the types of ATM crimes among the commercial banks in Nairobi County. The study established that a number of ATM crimes affect the banks. The most profound ones according to the study findings are: theft of money from ATMs by bank /ATM service employees (3 % response), robbery of couriers who fill ATMs with cash (5% response), theft of customer Personal Identification Numbers (14% response), vandalism of ATMs (18% response), theft by electronic data interception (24% response), theft by fraudulent electronic transactions (31% response), and fraudulent use of ATM card obtained from customers (5% response).

From the findings, majority of ATM crimes include the theft by fraudulent electronic transactions (31% response). This was associated with the adoption of money transactions using Apps and other money transfer avenues that banks have embraced due to advancement in banking technology. The finding was confirmed during key informant interviews held. The findings agrees with Gyamfi & Katsriku (2016) who argued that criminals use innovative techniques that are designed to go unnoticed one of them being that of keyboard overlays. The technique which involves overlaying the genuine ATM keyboard with a dummy keyboard allows the keyboard underneath to function properly, allowing usage of the ATM keyboard without any issue. The advent of banking and money transfer technologies have revolutionized banks

transactions to the extent of fostering ATM crimes in the study area. In addition, the study established that the major factor contributing to ATM insecurity among commercial banks in Nairobi is poor pay among employees in banks and courier companies. That poor pay influence employees' deviant behavior of engaging in ATM related crime in order to get money. The same was echoed during key informant interviews in which the informants argued that the main factor contributing to ATM insecurity among the commercial banks in Nairobi is the poor remuneration among employees of banks and those of security companies involved in cash transit. The finding is in line with Jain (2017) who argued that bank employees responsible for ATM operations collude with criminals outside the bank to commit ATM fraud or worse, employees with access to ATM and related customer information use those access rights to commit crimes. Although poor pay (31%) response emerged as the significant factor in ATM related crime among the commercial banks in Nairobi County, other factors that contribute to the same according to the study findings include inadequate internal control (27%), weak employment policies and procedures (19%) and low motivation (20%) among other factors.

Influence of Bank Internal Control Measures on the Vulnerability of ATMs to Insecurity Among Commercial Banks in the Study Area

This was the second objective in this study. From the analyzed data, it was established that majority of the respondents had high opinion on the influence of bank internal control measures on the vulnerability of ATMs to insecurity among commercial banks in the study area. For instance, the respondents had a high opinion that the commercial banks in the study area have information security policy to which the employees have consented to, commercial banks have an ATM audit policy which allows for regular auditing in identifying possible irregularities related to ATM crimes, and that respondents regularly undergo training on fraud detection, response and reporting that have a far-reaching positive implication on curbing the ATM related

crimes among the commercial banks in the study area. The findings were in line with Peprah (2018) who argued that effective supervision is the way to control or minimize the impact of employees using their capabilities to commit fraud. The finding is also in line with Hamberg (2013) who averred that auditing highlights financial controls, supervision checks, employees' competence, quality operations, and clients' results all need to be considered.

On the contrary, the study established that majority of respondents had a low perception on the influence of bank internal control measures on the vulnerability of ATMs to insecurity among commercial banks investigated. This was informed by the low opinion on the influence on information security policy informing employees of what is expected as well as the consequences for any breaches can deter insider related ATM frauds, conducting ATM audits such as reconciliation of settlement account deposits with actual ATM balances can deter cases of operational fraud, and low opinion on the training of branch personnel/ATM service providers/technicians on ATM fraud recognition to deter ATM fraud. The findings supported studies by Albrecht, Hill & Albrecht (2006) and Maina (2019) which revealed that financial need and personal issues coupled with inadequate internal controls create good opportunities for ATM fraud among commercial banks. The inadequate control make ATM technicians and security guards entrusted with providing security at ATM locations to collude with criminals to defraud banks in what is commonly regarded as insider job that foster ATM related crime among banks.

The findings of this study were also in line with studies by Fenlon (2010), Hannah *et al* (2016), Rabi'u and Noorhayati (2015), and Ruankaew (2016) which established that insincerity of bank employees has created opportunities for ATM fraud. The insincerity, according to the study, make them exploit breakdowns in internal controls to engage in fraud in cooperation with criminal networks outside the banks and having access to confidential customer information is perceived as

an opportunity to commit fraudulent actions. The acts have to high extent contributed to the ATM related crimes among the commercial banks.

Effect of ATM Location on Vulnerability of ATMS to Insecurity Among Commercial Banks in Nairobi County

The fourth objective of this study was to investigate the effect of ATM location on vulnerability of ATMs to insecurity among commercial banks in Nairobi County. The study established that majority of respondents had a high opinion that the location of ATMs had an effect on the vulnerability of ATMS to Insecurity Among Commercial Banks in the study area. The measures that the commercial banks have put in place in terms of the location of their ATMs have curbed the vulnerability of ATMs to insecurity. The reason for this argument is that the commercial banks in the study area have located ATMs in a high traffic area with adequate lighting and signage which can deter ATM robberies and burglaries and that the commercial banks have perfected in ATM installation where they use free-stand ATMs or through-the-wall ATMs that play an important role in preventing ATM fraud. According to the study findings, the measures the commercial banks put in place have greatly helped in minimizing ATM-related crimes among the commercial banks in the study area. The data from respondents was confirmed by key informants during interviews.

The key informants argued that commercial banks in the study area have formulated and put in place strategies to curb ATM-related crimes. The key informants gave illustrations to justify their claims by arguing that commercial banks have situated their ATMs in a high traffic area with adequate lighting and signage that can deter ATM robberies and burglaries and that they have installed ATMs using free stand or by use of walls that have helped to control ATMs related crimes among the commercial banks in Nairobi.

From the information from key informants, it was clear that commercial banks in Nairobi County have had spirited effort to curb ATMs robberies and fraud. The measures that banks have put in

including locating their ATMs in a high traffic area with adequate lighting and installation of ATMs using free stand or by use of walls have assisted in preventing crimes associated with ATMs. The findings concur with Brunner, Decressin and Kudela (2004) who argued that the location of an ATM is a high determinant of fraud or crime carried out at an ATM point. The findings are also in agreement with Adepoju and Alhassan (2010) that the location of ATM in secluded places contributes to fraud perpetuated at ATM points. ATMs within premises and in high-traffic areas have been found to be more secure compared to those located outside bank premises given the increased robbery incidents against the clients.

Conversely, some respondents felt that ATM location among commercial banks in the study area had not had any effect on protecting vulnerability of ATMs to insecurity. The low opinion of the respondents was based on the banks' ineffective ergonomic design of ATMs in which the ATMs don't recess the monitor display more deeply within the terminal to provide adequate security against shoulder surfing and that some ATMs are not well designed to prevent shoulder surfing. According to the study findings, this is a setback in the fight against ATMs insecurity among the commercial banks in Nairobi County. The finding was confirmed by some key informants who asserted that some commercial banks have not done much to curb ATMs related crimes. This is because some banks have not embraced the ergonomic design of an ATM to provide adequate security against shoulder surfing.

The finding is consistent with Doyle (2004) who listed out environmental features that can contribute to increase of robberies around ATM deployments. The features include un-kept landscapes, solid structures near ATM deployments acting as hiding spots, having telephone kiosks, inadequate lighting, bench seats near ATMs and/or having wide footpaths near ATM deployment. The findings also agree with Jain (2017) and Gyamfi et al., (2016) who recommended designing of ATMs in a manner that the positioning of the keyboard is centered directly

below the monitor, allowing for the body to naturally cover the area of PIN entry and recessing the display and positioning the PIN entry device in such a manner that will allow the genuine ATM user to block direct viewing to their transaction details by others thus preventing cases of shoulder surfing which affects the banks' efforts to tackle ATMs related crimes.

Influence of ATM User Competence on The Vulnerability of ATMs to Insecurity Among Commercial Banks in Nairobi County

Influence of ATM User Competence on The Vulnerability of ATMs to Insecurity Among Commercial Banks in Nairobi County was the fourth and last objective in this study. From the data collected and analyzed, it was established that majority of the respondents had high opinion on the influence of ATM user competence on the vulnerability of ATMs to insecurity among commercial banks in Nairobi County. The study finding was informed by the commercial banks' ability to train their customers on proper usage & safety of credit/ATM card, ability to make ATM Safety and security educational materials available to customers, and the banks' efforts to make customers well educated on the ATMs crimes and how to avert such crimes.

The findings were found to be consistent with Choplin (2011) who reported that factors such as education and demographic had an effect on consumer vulnerability to fraud. The findings also agree with those of Rizzardi (2008) who emphasized on the need for consumer education to prevent credit/debit card fraud. However, the findings contradicted Jain (2017) who established that that many banks in India have not sufficiently educated their customers on basic usage of cards, resulting to loss of ATM cards at ATM placements by ignorant customers who influence ATM related crimes in banks.

On contrary, according to this study, some respondents were of the low opinion that commercial banks in the study area have not done much on the ATM user competence on the vulnerability of ATMs to insecurity. This is

because there have been minimal efforts by the banks to educate ATM users/customers on proper ATM card usage and PIN management to prevent them from falling victims of fraudulent activities, the banks have not adequately educated their customers on risks associated with using ATM and how to avoid the risks can deter ATM related frauds, and that the commercial banks in Nairobi County have not educated ATM users about the look and location of ATM components such as PIN pads, card readers, monitor and cash dispensers and how to use them can deter ATM fraud crimes among the commercial banks.

The study found the findings concurring with Mgaya (2015) who reported that most ATM users in CRDB bank branches in Dar Es Salaam assume that they will not be deceived by others, based upon a belief that the probability of being deceived is very low. The study argued that attackers having understood this common belief, make their requests sound so reasonable that no suspicion is raised, all the while exploiting the victim's trust. The study also agrees with Russell (2018) who argued that advising customers about the types of real-life ATM scams that occur can help them recognize when something is suspicious and decrease their chances of falling victim. This decreases the vulnerability of customers to ATM related crimes.

Conclusions and Recommendations:

The study established vulnerability of ATMs to insecurity among commercial banks in Nairobi County, Kenya. Amongst other recommendations the study recommended target hardening of ATMs clients by investing in innovations that enhance security of electronic transactions and related crimes. Further the study recommends beefed up user education, increased regular ATM audits, embrace the ergonomic designs of ATMs to assist in recessing the monitor display more deeply within the terminal to provide adequate security against shoulder surfing.

References:

1. Adepoju, S. A., & Alhassan, M. (2010). Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria—A Case Study of Selected Banks in Minna Metropolis. *Journal of Internet Banking and Commerce*, 15(2), 3–10.
2. Albrecht, W. S., Hill, N. C., & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. *Australian Accounting Review*, 16(1), 30-40.
3. Brunner, A., Decressin, J. & Kudela, B. (2004): Germany's Three-Pillar Banking System – Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC.
4. Choplin, J., Stark, D., & Ahmad, N. (2011). A Psychological Investigation of Consumer Vulnerability to Fraud: Legal and Policy Implications. *Law & Psychology Review*, 35, 61-108.
5. Fenlon, W. (2010). *How does ATM skimming work?* <https://money.howstuffworks.com/atm-skimming.htm>. Accessed 31 December 2017.
6. Financial Fraud Action (FFA, 2015). *Annual Review. Working together to Prevent Fraud*. Retrieved from: http://www.theukcardsassociation.org.uk/wm_documents/FFA%20UK%20Annual%20Review%202015%20Final.pdf
7. Financial Fraud Action (FFA, 2017). *Annual Review. Working together to Prevent Fraud*. Retrieved from: http://www.theukcardsassociation.org.uk/wm_documents/FFA%20UK%20Annual%20Review%202015%20Final.pdf
8. Gyamfi, N. K., Katsriku, F., Adamu, M., Kwaku, N., & Abdulah, J.-D. (2016). Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective. *International Journal of Applied Science and Technology*. 6(1), 102–111
9. Hamberg, E. (2013), Supervision as control system: the design of supervision as a regulatory instrument in the social services sector in Sweden. *Scandinavian Journal of Public Administration*. 17(3), 45- 64.
10. Hannah, C., Srinivas, T., & Subbaiyan, G. (2016). The Impact of Design and Placement of ATM Deployments on Perceived Safety in India. *International Journal of Criminal Justice Services*. 11(1), 1–16.
11. Jain, S. (2017). ATM Frauds – Detection & Prevention. *International Journal of Advances in Electronics and Computer Science*. 4(10), 82–89
12. Kothari, C.R. (2012). *Research methodology: Methods and techniques*. (2nd Ed.). New Age International Publishers: New Delhi
13. Maina, K. (2019, April 24). How Absa ATM heist was executed. *The Star*. Retrieved from <https://www.the-star.co.ke/news/2019-04-24-how-absa-atm-heist-was-executed>
14. Mgaya, G. (2015). Analysis Of Atm Premise Security Aspects On Preventing Cardholder 's Pin
15. Theft And Attack. A Case Of Crdb Branches In Dar Es Salaam , Tanzania. *Journal of Multidisciplinary Engineering Science and Technology*, 2(8), 2075–2082
17. Murigu, A. H. (2008). *The Usage of Automated Teller Machines Case Study: Absa Bank of Kenya*. University of Nairobi.
18. Obwatho, S. (2014). *Academic Research: The Logical Sequence*. Nairobi, Kenya: Starbright Services.
19. Peparah, W. K. (2018). Predictive Relationships among the Elements of the Fraud Diamond Theory: The Perspective of Accountants. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 8(3), 141–148. <https://doi.org/10.6007/IJARAFMS/v8-i3/4547>
20. Rabi'u, A., & Noorhayati, M. (2015). Fraud Triangle Theory and Fraud Diamond Theory . Understanding the Convergent and Divergent For Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*. 5(4), 38–45. <https://doi.org/10.6007/IJARAFMS/v5-3/1823>
21. Rizzardi, R. (2008). Financial Management -- Payment Card Fraud Can Happen to You. *Optometry & Vision Development*. 39, (2) 64-65
22. Ruankaew, T. (2016). Beyond the Fraud Diamond. *International Journal of Business Management & Economic Research*. 7(1), 474–476.
23. Russell, D. (2018). *Best Practices for Customer Security Education. International Minimum Security Guidelines and Best Practices for Protecting ATM Systems*. ATM Industry Association.
24. Scott, W.R. (2001) *Institutions and Organizations*. Sage Publications

25. Shinde, S.P., Chingale, R. R., Dhane, D.C., & Vader, P.B (2017). ATM Security Using GSM And Mems Sensor
26. Snellman, H. (2006). Automated Teller

Machine network market structure and cash usage. Scientific monographs ISBN 952-462-318-8.