Original Research Article

Assessment of Mobile Money Transaction Frauds and Consequences

Confronting Zanzibar Telecom Service Providers

Abstract

This study investigates Mobile Money Transaction Frauds and consequences stimulating Telecom Service Providers in Zanzibar, Tanzania. It provides a clear understanding and assessment of precise level of phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar and evaluates the consequences and solution of the same. Purposive sampling was used among managers, staffs & agents in the telephone service providers explicitly Zantel, Tigo and Airtel companies. These selected operators are giants and widely used by the majority in Zanzibar. The qualitative analysis had been recorded and coded. The data gained from the descriptive survey design were themed for the purpose of the analysis. The study revealed that phishing (handset hacking, unauthorized SIM swap and PIN reset), spoofing (Fraudulent SMS, Whatsapp messages, phone calls for money transfer) and fake call from operator call center which include receive call from call center are common and committed frequently in mobile money transactions fraud. The common consequences of mobile money transaction are originated in marketing consequences, financial consequences and legal consequences which indeed affect the companies in operations and therefore, awareness program concerning with precaution of using mobile money transaction should be initiated besides establishment of clear mandate on mobile money issues between Communication Regulatory Authorities such as TCRA, Police Unit and Service providers in improving performance outcomes.

Keywords: *Mobile-Money, Consequences, Transaction Frauds, Telecommunication, service providers*

1. BACKGROUND AND INTRODUCTION

Digital Frauds in businesses today have become a global economic risk which threatens not only the survival of individuals, firms, industries, economies but the telecommunication industry and the mobile money service in particular. Mobile payment service is exploding at an impressive rate as the global mobile payment revenue almost tripled over the last five years (Lu, 2019). Mobile money transaction is a new payment systems phenomenon especially in the developing

world. Mobile money (M-money) is the process where products with monetary value are transferred electronically between one or more recipients, the sender and the receiver. Mobile cash is just but one of the examples of M-money.(Malady et al: 2014).

Mobile money is there used loosely to refer to money stored using the SIM (subscriber identity module) in a mobile phone as an identifier as opposed to an account number in conventional banking. Notational equivalent is in value issued by an entity (an MNO in this case) and is kept in a value account on the SIM within the mobile phone that is also used to transmit transfer or payment instructions, while corresponding cash value is safely held elsewhere, normally in a bank for the case of EAC. The balance on the value account can be accessed via the mobile phone, which is also used to transmit instant transfer or payment instructions (UNCTAD, 2012).

A mobile money account can be best described as a checking account associated with a mobile phone number. Users can cash-in and cash-out money from the account using a dense network of local agents serving as ATMs. Additionally, users can perform cash-free transactions, such as peer-to-peer transfers, using a mobile phone with mere support of legacy SMS technology. Mobile money networks differ from traditional banking by having significantly lower capital and institutional barriers to create and operate because, they leverage the existing dense cell phone network, the only capital requirement to become an agent, who facilitates deposits and withdrawals, is to have a mobile phone, and therefore the networks do not need to invest in costly banking branches. Consequently, mobile money networks can offer a viable alternative to traditional banking. (Tobbin, 2011).

Mobile money has been a fast growing phenomenon in developing countries around the world but particularly in East Africa. The East African countries of Kenya, Uganda and Tanzania have shown remarkable growth and are three of the 16 countries globally where mobile money accounts outnumber bank accounts. The sector has now evolved to provide mobile financial services such as savings, loans and even insurance, providing greater opportunities for increased financial inclusion (Paelo, 2017)

Kenya sets world first with mobile money transfer by Safaricom M-PESA in 2006. Specifically, in Tanzania, Zantel was the first to launch mobile money transaction by offering Z-Pesa to the Tanzanian market, shortly thereafter, Vodacom introduced M-Pesa in 2008. In 2009, Bharti Airtel introduced Airtel Money service, and a year later a fourth provider, Tigo entered the market with Tigo Pesa (CGAP, 2018). M-PESA was launched in Tanzania by Vodacom Tanzania Limited (VTL) in April 2008. Since then, M-PESA has grown to more than a million customers transferring $12.8 million per month at 2,000 agent locations from May

2009 when M-PESA had 280,000 customers, transferring $5.5 million per month at 930 agent locations (Hoope, 2013).

In Tanzania, mobile banking has significant adoption, that is, almost thirty-five percent of households have at least one m-money account. Thirty two percent of the population use exclusively m-money as a provider of financial services and only 2% have an active traditional bank account. There are three major m-banking networks: Vodacom (Vodafone) with 40% market share in m-money, Tigo with 33% share, and Airtel with 16% market share. (TCRA Jan-March 2019 communications statistics report)

Coupled with a large number of population not having bank accounts, Africa has seen a tremendous growth in adoption and embracing of M-money. M-money services sometimes called Digital money has in it some risks just like other electronic platforms (e-platforms). The e-Platforms have become a playground of cyber-criminal, phishing and other financial crimes(Boorman, J., Ingves, 2001).

A study about cyber security showed that, the fear of mobile money transaction crimes cost the world community a large amount of money in establishing security protocols. In 2008 the worldwide cost of cybercrime was approximately USD 8 billion (Intersecurity Magazine, 2013). Some of the recently characterized cyber crimes include e-Platforms cyber-criminal, mobile transaction crime and other financial crimes (Singer & Friedman, 2014).

Many countries face difficulties in addressing issues arising from mobile transaction crimes, because they lack a concrete definition of online transaction fraud and how such crimes differ from traditional crimes (Aslam, 2006; Mayunga, 2013). Aslan (2006) defined online transaction crimes as a violation of criminal laws that involves the knowledge of computer technology for its penetration, investigation, or prosecution. Unfortunately, Africa has become the target of online transaction crimes than the rest of the world where more internet users are victimized by these crimes than before.

In the Tanzanian context, a significant percent of the population is connected to the internet (Lubua E. , 2014; IPP Media, 2014). As the result the government established a unit within the Police Force to address challenges of online transaction crimes. However, the impact of crimes is still threatening the security of financial transaction. In 2012, about 620 cases were reported to the cybercrime unit (Mayunga, 2013). The most reported crime was online stealing of money. Other reported crimes include obscene communications, computer forgery and life threatening messages. It is evident that the increase of cybercrimes affects transactions which are conducted online in the Tanzanian community.

Nevertheless a number of controls have been introduced to address the challenge. Such controls include the use of authentication methods, establishment of sim card registration by using biometric system and enhance awareness campaigns about online safety, vivid example is the strategic technique established by Police force in collaboration with TCRA and Telecom service providers of sending precaution text messages to every valid sim card.

Together with all these considered efforts to control the existing mobile money transaction fraud, still the challenge seems to grown and continue to effects the community, government and telecom service providers have no exception.

The introduction of mobile money transaction services has transformed the lives of Tanzanians and Zanzibar specifically. In a country where only a section of the population can afford, or have enough balances to open and manage bank accounts, mobile money services have made it easy to send and receive money, to pay bills and obligations and for some, to save their money. Out of the 43,918,502 mobile phone subscriptions in Tanzania including Zanzibar, 22,796,830 have been registered for mobile money services. Consequently, 243,522,841 Mobile Money Transactions with the worth Tsh 7,823,673,367,061/- were transacted (TCRA, March, 2019). The statistics show that, Zanzibar has been reported a total of 197 cases concerning with mobile money transaction fraud to the cyber-crime unit of the Police Force for the period of seven months from 1st January to 24th July, 2019. Those complaints are from various mobile operators including Tigo, Zantel, Airtel, Vodacom and Halotel.

Zanzibar, like other developing countries has employed different strategies against the problem of mobile money transaction fraud. Such strategies include the use of authentication methods during the transaction, establishment of sim card registration by using biometric system and enhance awareness campaigns about online safety (i.e sms from Police force to every subscriber identification module).

However, during the implementation of these strategies, varieties of challenges have also been raised. Some of these challenges are; the mobile money transaction fraud seen to increase due to the different reasons such as advancement of Science and technology, the desire of people to earn money so easily, poor information on the uses of mobile money services as well as low knowledge to the users of mobile money services (TCRA National report 2015 – 2016).The failure of these strategies may cause a reputation and financial problems to Telecom service providers who offer mobile money transaction service in Zanzibar. The researcher considers marketing, financial and legal negative impact to be consequences of mobile money transaction fraud Telecom service providers in Zanzibar.

Until recently, there has been no reliable evidence that addresses relationship between mobile money transaction fraud and consequences to Telecom service providers in Zanzibar. This indicates a need to understand such relationship if any.

Therefore, this study is primarily proposed to focus on mobile money transaction frauds and consequences to Zanzibar Telecom Service Providers. The study specifically assesses the level of phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar and evaluates the consequences of phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar. This will provide suggestions on in overwhelming the existing challenges of mobile transaction fraud in the country which have been affecting the public in general. The result of the study also will help the policy makers and Telecom service providers to reform their policies and laws which will be resulted to generate more income.

2. LITERATURE PERSPECTIVE

2.1 Application of Technology in Service Theory

Many theories have been developed on Information Technology (IT) adoption, such as Davis' (1989) Technology Acceptance Model (TAM), Roger's (1995), Application of Technology in Service Theory etc.

Developed by Davis, 1989, Technology Acceptance Model is an information systems theory that connects users' acceptance of a technology. The model suggests that when users are presented with a new technology, two specific factors influence their decision about, how and when they will use it. These are 'perceived usefulness', which refers to the degree to which a person believes that using a particular application system would enhance his or her job performance; and 'perceived ease-of-use', which is the degree to which a person believes that using a particular system would be free from effort (Davis, 1989).

Banking industry technology has got positive competition which has resulted to positive impact on mobile money transfer services (Morawczynski and Pickens (2009)).This theory explains so far how the technology has contributed to improve mobile money transaction services. The theory has a number of advantages to society as it explain in details how so far this new technology has improved the service delivery as banking business has increased(Leow, Hock Bee, 1999). The theory explain in details it availability and expansion to rural areas where other technology were not available hence effect a number of advantages through effecting transactions and payments systems.

Chapman and Holtham (1994) argued that application of new technologies creates potential for improvement in delivery of services as it is in recent developments in mobile phone technologies which has resulted in a rise in volume of banking business performed through the mobile phone such as mobile money transfers (Leow,Hock Bee, 1999). TigoPesa as the positive effect towards new technology as the theory suggest it has brought a number of positive impacts as to make easy transactions on matters which were not easy (Sirken, (2009) Financial Access.

This theory has its weakness as it does not explain how so far it brought changes to areas where are unbanked (BoT report on Balancing Act Africa, issue 541

February 2011, accessed on 17th June 22, https://www.balancingact-africa.com/news/issue/telecoms-en/541). The technology theory has been new to society such that it reveals no positive effect as it is new to society. Technological developments have brought many changes to society as transactions have been possible at every stage with no any limit. (BoT report on Balancing Act Africa, issue 541 February 2011, accessed on 17th June 22, https://www.balancingact-africa.com/news/issue/telecoms-en/541). This is another weakness resulted by technological theory as it tries to excel mobile money transfer services with no boarder of control hence reveal shortfalls to users of this services.

2.2. Mobile Money Transfer services and keeping balance theory

Zhdanova et al. 2014, cited by Adeyinka, A,2018 defined Mobile Money Transfer (MMT) as a financial service provided by a Mobile Network Operator (MNO) that enables transfer of funds (mMoney) between service subscribers through the use of mobile channels. In MMT service, mobile subscribers can add electronic money called mMoney to his or her virtual mobile account (mWallet) and store for later use, transfer to other mobile subscribers or purchase goods via mobile phone. The receiver can inexpensively convert this credit back into cash through a retailer such as local corner shops to act as bank branches.

Mobile money transfer service allows users to send cash using SMS technology thereby avoiding inconvenient and costly transfer methods such as physical travel, the mail, or traditional wire transfer services like Western Union and Post-pay which are often done in banks. For example, payments for services like electricity and water where people need to travel long distances and may end up meeting huge queues at the bank.

Morawczynski and Pickens (2009) found out that M-Pesa users often keep a balance on their M-Pesa accounts, thereby using the system as a rudimentary bank account. M-Pesa users also send smaller but more frequent remittances, suggesting that the use of M-Pesa system might someday allow informal insurance networks to function more efficiently and effectively.

The rapid uptake of M-money services is not surprising when one considers the level of financial development in Tanzania and in sub-Saharan Africa. Less than 30 percent of the population in East and Southern African has a formal bank account, ranging from 9 percent in Tanzania. These findings are according to a study conducted by FinMark Trust in 2008. In 2006, Tanzania had only 450 bank branches and 600 automatic teller machines, or less than two bank branches per 100,000 people (Vaughan, 2007). Tanzanians primarily sent money by one of three mechanisms: via Western Union or post office, via intermediaries (such as bus drivers), or via friends or relatives. Wire transfers via Western Union are secure but expensive and not always available in remote rural areas.

2.3. Adoption of Mobile Money Transfer services theory

Since 2005, Mobile Money transaction services have been used in a number of ways in developing countries. It is the theory which explains the adoption of money transfer services and its effect to developing countries. A study conducted by Porteous (2006) on the adoption of Mobile Money transaction services in Africa found out that Mobile Money Transfer s in Africa are in the following forms; transmitting airtime, paying bills and transferring money. The forms which has been explains in this theory base much on the activities being conducted by the society such as paying bills, as it is for water bills, electricity (LUKU), DSTV, Star times etc. There are also a few m-money systems in developing countries that allow international money transfers.

In this theory it is much explaining its impact to developing countries for transacting e money while the matter of mobile money transfer services is wider than it has been stated in this theory. The positive effect of this theory is it explaining the actual situation being performed on adoption to mobile money transaction services as it explaining it effect in developing countries. Although this adoption theory has positive effect there are other negative effect whereby it does not explain how so far it has benefited the society and its impact to development of the society at large particularly in developing country and focusing on the society living in rural areas.

2.4. Usage and impact of Mobile Money transaction services theory

Usage theory explains the impacts resulted by mobile money transfer services(Tigo-Pesa) the impacts to individuals through personal savings and timing amount of transfers. Jack and Suri (2009) suggest that that the inconspicuous nature of M-money transfers could allow individuals to increase their personal savings, because friends and relatives would be less likely to know about the timing or amount of transfers. Wilson, Harper and Griffith (2010) find that members of informal savings groups in Nairobi are using M-money to deposit individual savings into their group account.

A variety of qualitative studies provide some insights into the characteristics, patterns and potential impacts of Mobile Money Transfer usage. For example, a study by Morawczynski and Pickens (2009) on usage and impact of mobile financial services in Kenya found out that users often keep a balance on their M-money accounts, thereby using the system as a rudimentary bank account. This theory is much used for financial transactions and keeping of funds and their usage. The theory fails to reveal the impact to users as it does not recognize its impacts to society hence further study has to be applied.

***Phishing*:** The term phishing is broadly used with lots of definitions in literatures In some publications, the phenomenon of phishing is explicitly defined; in some, it is described by means of an example, while others assume that the reader already

knows what phishing is. Numerous writers suggest their definition of phishing, leading to a large number of different definitions in the scientific literature

Chris et al.2016 defined Phishing as tricking individuals into disclosing sensitive personal information through deceptive computer-based means. It is also a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person (Michael, et al 2017)

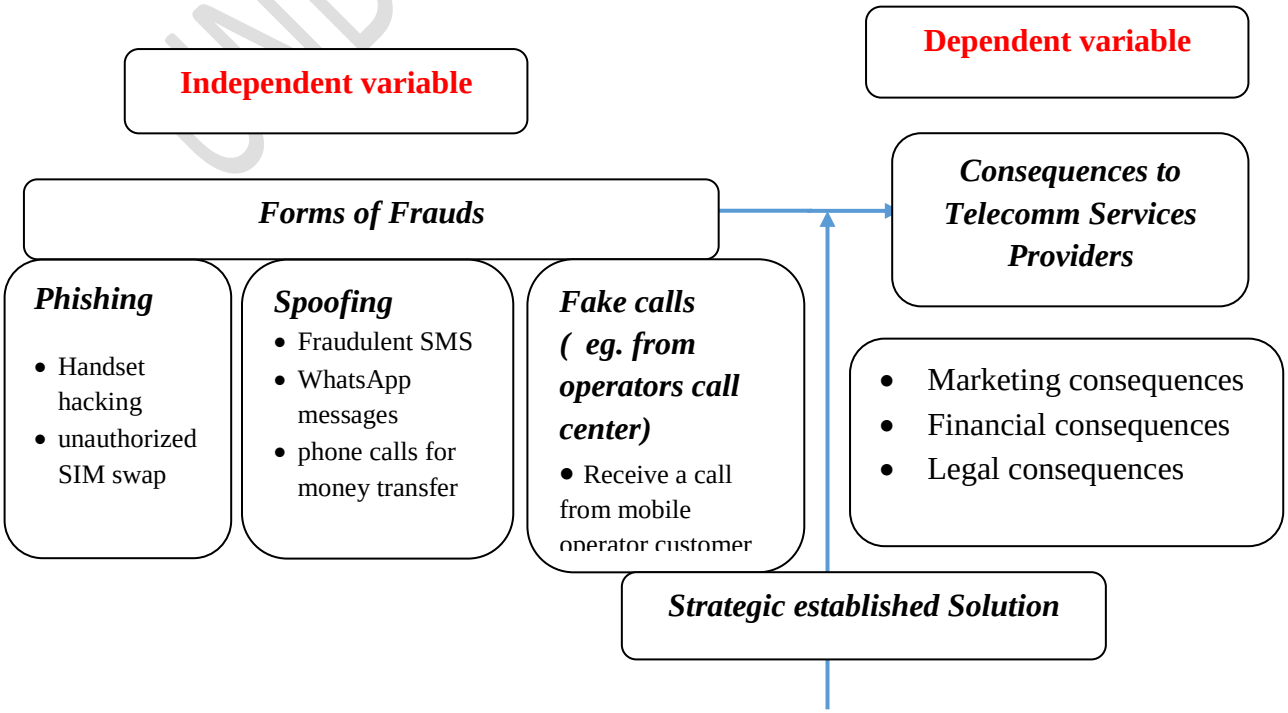
Spoofing: Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing also refers to a type of cheat in which a criminal disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source. Spoofing often involves changing just one letter, number, or symbol of the communication so that it looks valid at a quick glance. A ***fake call*** is a telephone call in which the caller lies to or tricks the person they called.

2.5 Conceptual Frame Work

This section viewed the conceptual frame and contained three variables which are two independent variables and one dependent variable; the dependent variable concerns about consequences to Telecom service providers in Zanzibar and independent variables are diverse forms of mobile money transaction frauds that include spoofing, phishing and fake calls. So the researcher presumes that the dependent variable will be a result of independent variables.

Figure 1: Conceptual framework of the study



- Online patrol within Cybercrime unit
- Biometric sim card registration
- Transaction authentication method
- Precaution message from police force

3. METHODOLOGY

3.1 The Study Design

A Descriptive Survey design for the major purpose of providing description on the consequences of mobile money transaction fraud to Telecom service providers in Zanzibar was used it also assessed the effectiveness of the solution taken by the communications stakeholders to resolve the challenge. The design adapts sequential mixed methods of quantitative and qualitative techniques; these two methods were used to attain the answers to the specific objectives of the study.

3.2. Population and Sample

Kombo (2014) defined population as a group of individuals, objects or items from which samples are taken for measurements. This study, the uses six Telecom service providers namely; Zantel, Tigo, Airtel, Vodacom, Halotel and TTCL who offer mobile money transaction service in Zanzibar. Respondents include operator's management, operator's staffs and operator's agents. This study uses Purposive sampling to select three telecom service providers namely; Tigo, Zantel and Airtel. The selection was regarded operators who are giants and widely used by the majority in Zanzibar. The sample size of the study is determined by taking into consideration the suggestions given by Hair et al. (2013) in multiple regression which recommended that a minimum sample of 50 and preferably 100 respondents is normally required for most research situations, however the minimum ratio of respondents to predictors is 15:1 or 20:1. This implies that 15 or 20 respondents are required for a single predictor. On the other hand, Wilson Van Voorhis and Morgan (2007) propose that for regression equations with three or more independent variables considered, an absolute number of 10 respondents per predictor are appropriate. Based on the above recommendations, the sample size of the current study shall be at least 30 or 45 respondents as suggested by Van Voorhis and Morgan (2007) and Hair et al. (2013) respectively, resulted by the study having 3 predictors. The study was regarded to have a sample size of 45

respondents 15 from every provider. The respondents will include Management, staffs and agents from the earmarked operators; this selection was due to a limited number of staffs to telecom service operators particularly in Zanzibar.

Table 1: The Study sample

Categories	**Sample size**
Managers, staffs & agents from TIGO Company	15
Managers, staffs & agents from ZANTEL Company	15
Managers, staffs & agents from AIRTEL Company	15
TOTAL SAMPLE	**45**

3.3. Data **Collection Methods and Analysis**

The data has been collected using both primary and secondary means in both qualitative data as complemented with quantitative ones. Questionnaires and interviews were used for collection of primary data; these techniques were used for the objective of attaining the answers of the study. The questionnaire designed and administered moderately and distributed to three telecom service provider's management, staffs and agents, it was in English language. Researcher considered questionnaire research instrument which enabled getting the required information from respondents which provided insight of the current status of problem facing Telecom service providers from existing challenge of mobile money transaction frauds. The questionnaires were also provided a window to respondents to assess the effectiveness of the existing solution provided by communication stakeholders to deal with the fraud, if not effective to suggest proper mechanism on how the fraud will be mitigated.

The Interview has been administered to purposive sample; Operator's staffs and agents were interviewed, operator's management was not involved due to limited time they have. The Information obtained through the interview guide was critically analyzed. Data collected from the field was analyzed and regression technique used to explore the effect between one continuous dependent variable and the independent variables or predictors.

4. RESULTS AND ANALYSIS

4.1 General Information of the Respondents

For level of Education, the study's findings revealed that majority of respondents were attained secondary education by accounting about 31% of all respondents, followed by certificate level which accounted 27%. Undergraduate level was in third position by accounting 20% and the last position was taken by two groups of level of education which were post graduate and primary education each took 11%. Secondary education level leads by scoring 31% resulted by researcher earmarked higher number of agents against operator's management and staffs, this means many agents have secondary education. Post graduate was scored only 11%, who were mobile operator's management and staff positions.

For working position, the study's results show that most of the respondents were agents who were 31, thereafter, followed by operator's staffs that were 6 staffs. Other involved positions were legal officer, marketing manager and customer service center manager who were 2, 2 and 3 respectively. This indicates that some telecom service providers in Zanzibar have a vacant in management position particularly marketing and legal positions. This is due to mobile operators to outsource companies operations in Zanzibar and concentrate only in customer's service operations known as mobile shops which significance management position is customer's service managers only and centralized the remaining management positions. The researcher learn that majority of respondent particularly agents have limited capability and experienced on addressing mobile transaction fraud issues.

In working experience, the study's findings indicated that larger group of respondent were in the field for a period of 1-5 years, the percentage of the same was 85, the second group represented by 11% were in the field within 6-10 years and two last groups represented by 2% each were lasting in the industry for 16-20year. The study also revealed that many agents were in the post as temporary employment while they are waiting for permanent employment that is why 85% were counted in the field within the range of 1 – 5 years. All who have experienced from 6 – 10 years and above were from mobile operator's managements and staffs group. This interpretation means that majority of agents have limited working experience that causes to be conducted frauds or being victim unknowingly.

4.1. Check for Normality

In assessing the normality of data, the most popular used approaches are by measuring Skewness and Kurtosis (Hair et al., 2014, Pallant, 2016). Based on the reference, to assess the normality the tests of Skewness and Kurtosis were used. According to Hair et al. (2010), if the calculated z value for Skewness and Kurtosis exceeds the mostly common used threshold of ± 2.58, then the distribution will not be normal. However, Kline (2016) recommends that to achieve normality of data the z value for Skewness be ≤ 3 and the value for Kurtosis ≤ 7. Based on this

statement, the results of Skewness for the study as displayed in table 2 below show that all variables are normally distributed since they did not exceed the threshold set by Hair et al. (2014).

Table 2: Test of Normality

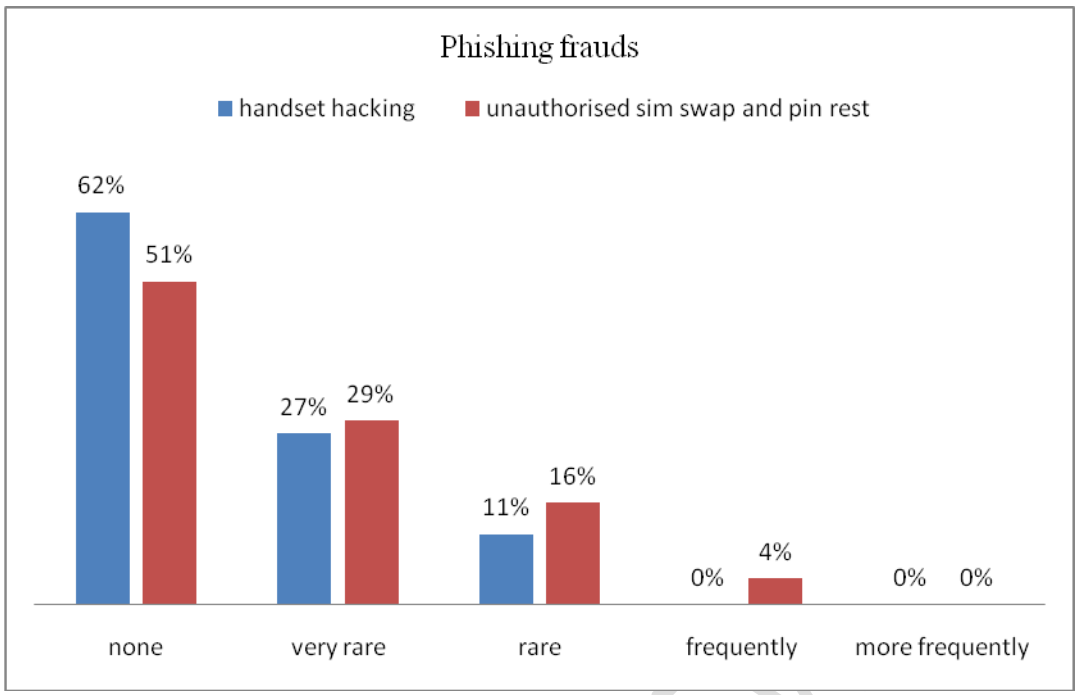
	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
Phishing	45	-1.274	.354	2.189	.695
Spoofing		-.104	.354	-.323	.695
Fake-call		-.269	.354	-.548	.695
Valid N (listwise)					

The results found in Skewness and Kurtosis column as seen in the table 2 above show that all variables are normally distributed as they are within the range of the threshold of ± 2.58 for skewness and ± 7 for kurtosis (Hair et al., 2014), and with the exception of phishing fraud shows that Skewness statistic value is -1.274 and kurtosis statistic value is 2.189 all are under acceptance range, therefore this study assumes that all study variables are normally distributed.

4.2 Results for Phishing

Specifically the interest was to know whether the phishing fraud is available and at what extent. For achieving of the same the respondents were asked the following question "how frequently phishing frauds reported to your office?" The results of this question are charted hereunder.

Figure 2: Phishing Frauds



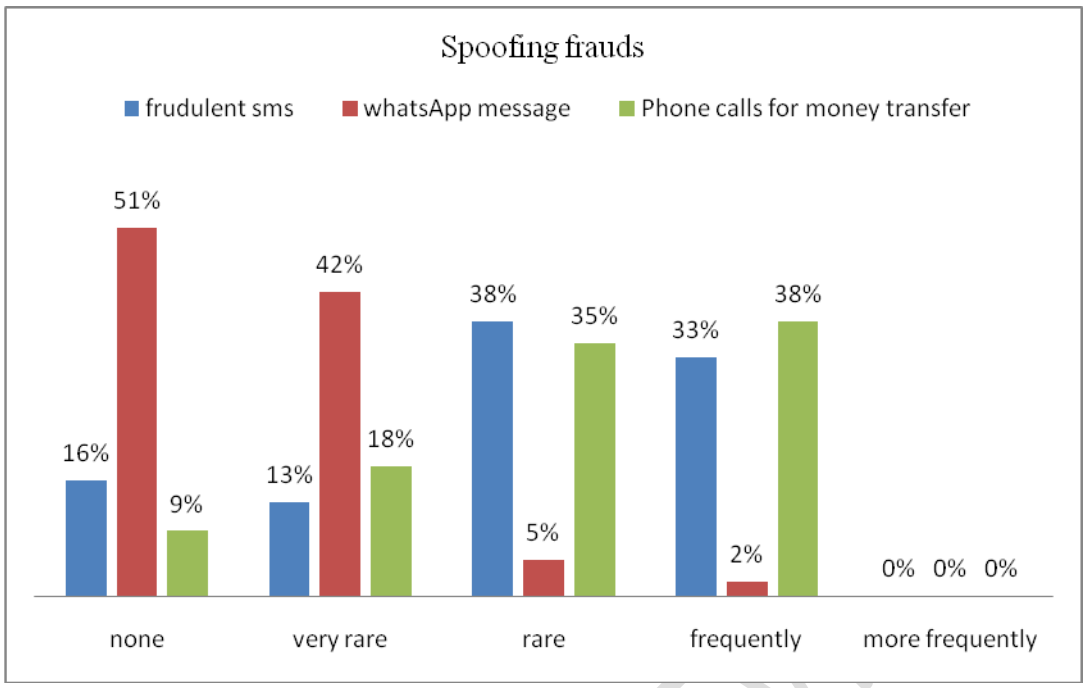
Source: (Field data, 2022)

The results from the findings indicated that most of the respondents said handset hacking and unauthorized sim swap and pin reset frauds do not exist, that was the results rated by 28 and 23 respondents out of 45 which are equivalent to 62% and 51% respectively as shown in figure number 2. The second rating was very rare which was selected by 27% and 29% of respondents for handset hacking and unauthorized sim swap and pin reset frauds respectively, while 5% and 7% of respondents ranked the frauds happened rarely. The last two ratings for spoofing frauds which are frequently and more frequently were rated by 0% and 4%, and 0% and 0% for handset hacking and unauthorized sim swap and pin reset respectively. The interpretation of the findings revealed that phishing frauds reported to telecom service provider's and agent's offices were very few.

4.3. Spoofing Frauds

Here the researcher was interested to find out about the reported spoofing fraud, the respondents were asked "how frequently spoofing frauds reported to your office?" The results of this question are interpreted hereunder;

Figure 3: Spoofing frauds



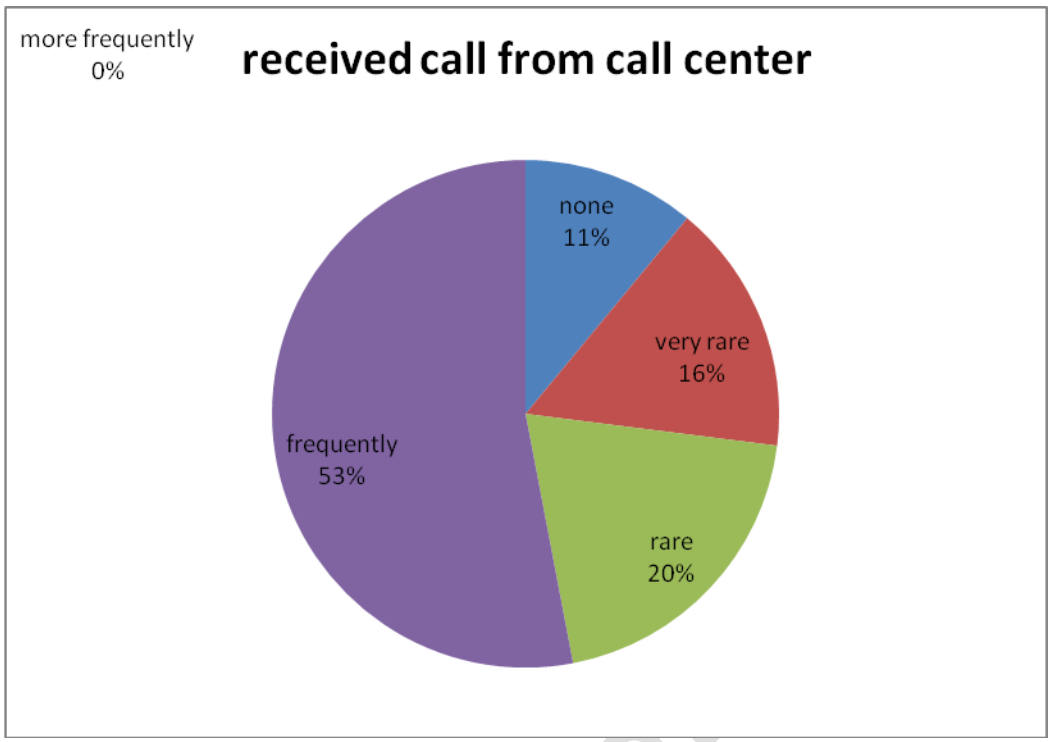
Source: (Field Data, 2022)

The results from findings revealed that fraudulent sms and phone call for money transfer frauds reported frequently to operator's and agent's offices, whereby phone calls for money transfer fraud lead by being rated 38% followed by 33% of fraudulent sms as shown in figure 3 above. The results also indicated that whatsApp sms fraud was ranked in none position by 51%, and rare position by 42%. The positions of rare, frequently and more frequently were ranked with 5%, 2% and 0% respectively. This means that fraudulent sms and phone calls for money transfer is a great challenge to telecom service providers and agents, while whatsapp sms was not available.

4.4. Fake call from call centre

This was another type of fraud which researcher was interested with. The respondents were asked the following question "how frequently spoofing frauds reported to your office?" The results of this question are shown here below

Figure 4: Fake calls from call centre



Source: (Field Data, 2022)

The study's findings indicated that majority of respondents which were 53% said fake call from call centre fraud complains reported frequently to their offices. The Second selection was rare which was ranked by 20%, and then followed by very rare and none which were ranked by 16% and 11% respectively as shown in the figure 4 above. These findings means that operator's and agent's offices have received many complaints against fake call from call centre.

4.5. Consequences of Mobile Money Transaction Frauds

Here the researcher was intended to find out if the existing frauds resulted impact to telecom service providers in Zanzibar, the researcher considered marketing, financial and legal consequences as impact to telecom service providers from the frauds explained in 4.2 above. The standard multiple regression statistical technique was used to answer this objective by exploring the relationship between impacts to telecom service providers with mobile money transaction frauds

The results from the findings of the standard multiple regression as tabulated in Table 3 below indicated that three independent variables namely phishing, spoofing and fake call accounted for 58.0% of the variability in consequences of mobile money transaction frauds to telecom service providers in Zanzibar (R^2 = 0.580). The adjusted R square value was 0.550. Therefore, these results verify that only 58% of variability in consequences of mobile money transaction frauds to telecom service provider in Zanzibar could be explained by the frauds factors of

phishing, spoofing and fake call from call centre. The remaining 42% of variability depends on other unexplained factors.

Table 3Findings from standards multiple regression for the testing of mobile money transaction frauds factors and its consequences to telecom service providers in Zanzibar.

Table 3: Model summary

R	R Square	Adjusted R Square	R Square Change	F Change	Sig. F Change
.762[a]	.580	.550	.580	18.909	.000[b]

a. Predictors: (Constant), fake call, phishing and spoofing frauds

b. Dependent Variable: consequences of frauds to MNO

Table 4: Dependent mobile operators' consequences

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-1.603	.699		-2.294	.027
	Phishing	-.012	.105	-.012	-.116	.908
	Spoofing	1.335	.181	.762	7.391	.000
	Fake Calls	.210	.085	.254	2.476	.018

According to the coefficients in Table 4 above, at the 0.05 level of confidence, the results has revealed that only two independent variables or predictors which were spoofing and fake call have a significant effect or impact on the outcome or dependent variable which was mobile operators consequences, the results were as follow:- for spoofing side $\beta = 0.762$, $t = 7.391$, $p < 0.05$ and for fake call side $\beta = 0.254$, $t = 2.476$, $p < 0.05$. On other hand, one independent variable which was phishing has shown no significant effect on the dependent variable which was mobile operators' consequences as per accordance with the output observed of $\beta = -0.012$, $t = -0.116$, $p > 0.05$.

Basically, the impact or effect of spoofing and fake call mobile money transaction frauds with consequences to telecom service providers was in a positive direction.

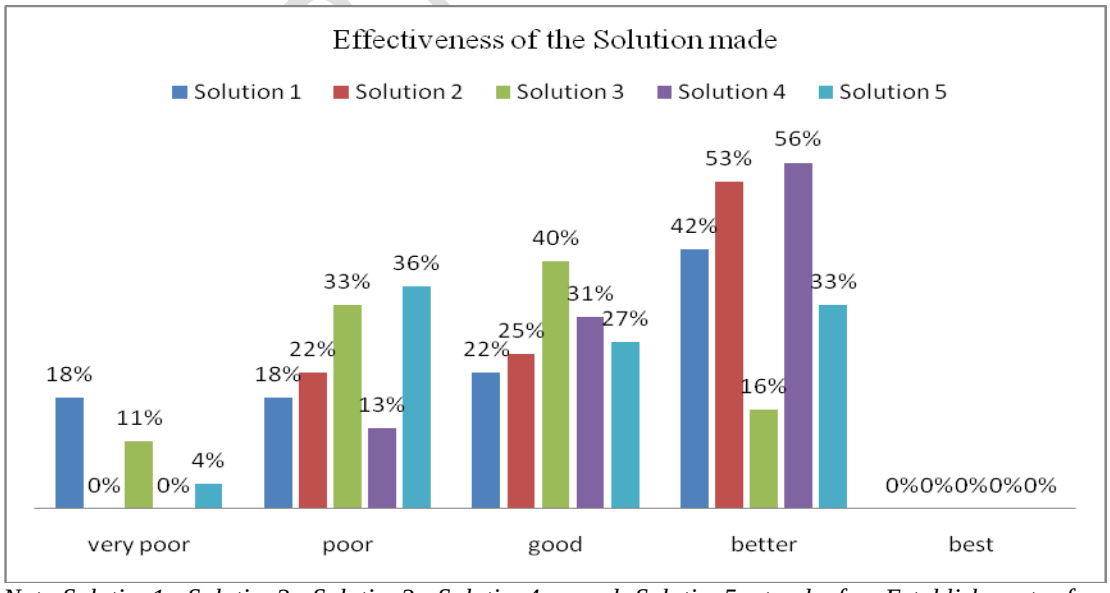
This situation indicates that the increase of these frauds (spoofing and fake call) results in the increase of consequences to telecom service providers (Hair et al., 2010, Pallant, 2016).

4.5.1. Effectiveness of the solution taken

In this target, the purpose was to examine whether the solution established by communications stakeholders including Regulator, Police force, Mobile operators and others to overcome emerged mobile money transaction frauds fulfill the expectation or not. Five solutions were considered in the study; the first one was Establishment of cybercrime unit within Police force, followed by Establishment of biometric sim card registration system, and then Establishment of clear mandates on mobile money transaction issues between the Police, TCRA, BOT and service providers go after. The study was also involved provision of fraud precaution messages to every active simcard from the Police force as a solution made, and finally ends up with establishment of mobile money transaction authentication method during the transaction process. Descriptive statistical technique was used to attain the answer of this objective.

The output from findings is illustrated in figures 5 and 6 hereunder;

Figure 5: Effectiveness of the Solution made

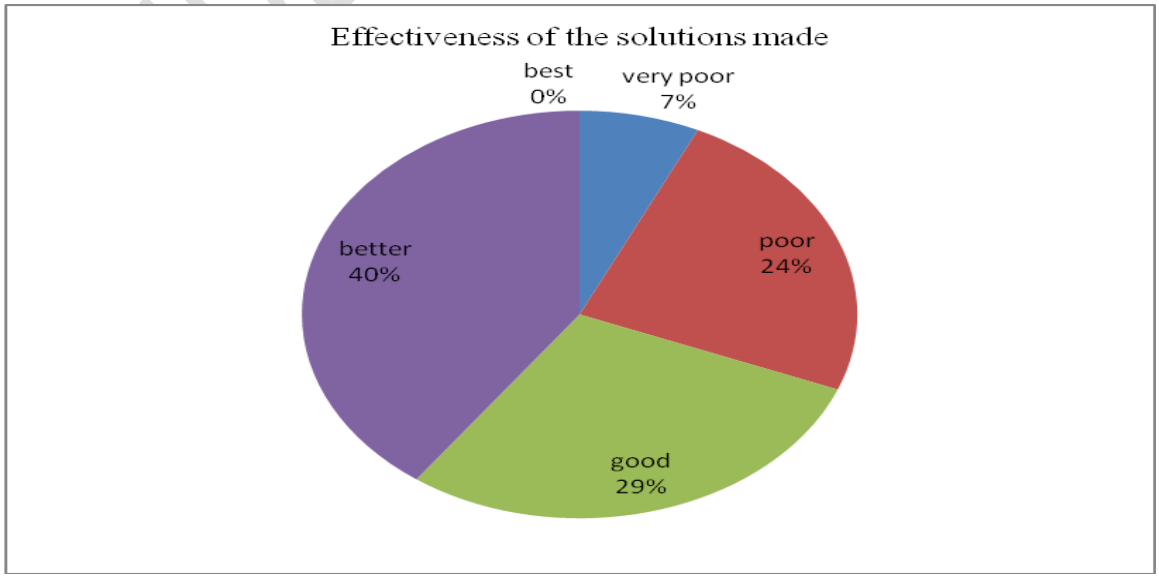


Note:Solution1, Solution2, Solution3, Solution4, and Solution5 stands for Establishment of cybercrime unit within Police force, Establishment of biometric sim card registration to secure mobile money transaction process, Establishment of clear mandates on mobile money transaction issues between the Police, TCRA, BOT and service providers. Provision of fraud precaution message to every active sim card from Police force and Establishment of mobile money transaction authentication method respectively.

Source: (Field Data 2022)

Based on the above Figure 5 revealed that solution 4 is lead on effectiveness on mitigating mobile money transaction frauds by counted 56%. Afterwards solution 2 was the second on being better frauds controller by counted 53%, thereafter solution 1 and solution 5 followed by counted 42% and 33% respectively. The least was counted 16% which was solution 3, that was for better grade. For good grade, solution three was lead by counted 40%. The solution which lead in worse condition to overcome mobile money transaction frauds was solution 1 counted by 18%. There was no any solution which was selected to be best on resolving mobile money transaction frauds.Moreover, the researcher manipulated effectiveness of the solutions made in generalization form and came out with the following output; best was lead by ranked with 40% followed by good, poor and very poor, their ranks were 29%, 24% and 7% respectively. Best position was ranked by none, counted 0%. The interpretation of the outputs means that 40% of respondents said that the solutions made by communications stakeholders are better in effectiveness on mitigating emerged mobile money transaction frauds, 29% said the solutions made were good, 24% and 7% said the solutions made were poor and very poor respectively. Besides, there was no any respondent said the solution made by communications stakeholders is best in effectiveness on mitigating emerged mobile money transaction frauds. According to the above observations there is a need for communications stakeholders to introduce and enforce a strong solution which will be a permanent remedy to confront emerged mobile transaction frauds which will result to countdown the impact faced by telecom service providers in Zanzibar in terms of marketing, financial and legal impact**.**

Figure 6: Effectiveness of the general solution made



Source: (Field Data, 2022)

5. CONCLUSION AND RECOMMENDATION

The study aimed at investigating consequences and solutions of the mobile money transaction frauds to Telecom service providers in Zanzibar, the study specifically sought to assess the level of phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar, to evaluate consequences of phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar and finally and moreover, the study intended to evaluate effectiveness of solution taken to overcome phishing, spoofing and fake call transaction frauds to Telecom service providers in Zanzibar.

This study revealed that phishing (handset hacking, unauthorized SIM swap and PIN reset), spoofing (Fraudulent SMS, WatsApp messages, phone calls for money transfer) and fake call from operator call centre which include receive call from call center are common and committed frequently in mobile money transactions fraud. In the consequences of mobile money transaction fraud, the study found marketing consequences (The company loss reputation and trust to its customers, the company loss customers by switching to another company), financial consequences (the company loss revenue due to customer being disappointed on using the services, the company increase cost of handling customer claims, the company increase cost of establishing a smart tools and process for security purpose, the company to be bankrupt), and finally is the legal consequence which include the company may be legal responsible and fined a lot of money as well as the company loss license due to noncompliance with licence condition are the most consequences of mobile money transaction to mobile operator, agents and government as well. the solution made include establishment of cybercrime unit within police force, establishment of biometric sim card registration system to secure mobile money transaction process, establishment of clear mandates on mobile money transaction issues between Police, TCRA, BOT and service providers, provision of fraud precaution message to carry live sim card from Police force and finally establishment of mobile money transaction authentication method are useful to combat the problem of mobile money transaction but still there is need for new strategies and solution to be done to combat the problem completely.

The problem of mobile money transaction fraud indeed affect the business system and life standard of people in the community as shown in the figure which shows the consequences of mobile money transaction fraud, this problem cannot be combated by the efforts from one side only, there must be joint of efforts from government institutions, mobile money operators, agents of mobile money as well as customers in fighting and removing the problem of mobile money transaction fraud and by enhancing establishment of awareness program on precaution of

using mobile money transaction services, enactment of the rules and regulation which commend the customers the customer to show their recognized indemnity during the transaction process of receiving money, establishment of clear mandates on mobile money transaction issues between mobile money stakeholders could relief to a very great extent.

Mobile Money operators should enhance awareness program on precaution of using mobile money transaction services to the users, the problem of mobile money transaction could be combat when awareness program on precaution of using mobile money transaction services provide to the users. The Agents should be very carefully during the transaction process, they should consider all rules and regulation of transaction process so as to overcome the problem of mobile money transaction fraud.

The mobile operator should come with the best alternative of producing very secure sim card such as wireless sim card system and other alternative which are conducive, reliable and affordable to the customers. The Government through its Institution (TCRA) should organize seminar and workshop aimed and improving conscious on how to overcome the problem of mobile transaction fraud and build good working relation between mobile money operator, agent of mobile money and customers. It also should organize the workshop for Police Force and mobile money operator to enable them acquire or improve their working relationship so as to improve the effectiveness and achieved to overcome the problem of mobile money transaction fraud.

Also government should include the safety use of mobile and mobile money services as part of the curriculum to secondary education in Tanzania so as to enable people to understand the best ways to use their mobile and mobile services without being hacked by mobile money hackers. A Part from that, TCRA should introduce new rules and regulation which commend the customers to show their recognized identity during the transaction process (receiving money from mobile money agent) Government to enact mandates on mobile money issues between the Police, TCRA and services providers as well as customer so as to overcome the problem of mobile money transaction.

REFERENCES:

1. Adeyinka, A; (2018), predicting fraud in mobile money transfer, University of Brighton
2. Aslan, Y. (2006). Global Nature of Computer Crimes and the Convention on Cyber Security.Ankara Law Review, Vol. 3 No. 2, 129-142
3. Boorman, J., Ingves, S., (2001), Financial system abuse, financial crime and money laundering-background paper. Wash. IMF.
4. Chris, J.; Lee, B.; David, W.; (2016) Computer Security Division Information Technology Laboratory, NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing.
5. CGAP. (2018, June). Building Inclusive Payment Ecosystems in Tanzania and Ghana. Retrieved August 1, 2019, from www.cgap.org: http://documents.worldbank.org/curated/en/663171533185481164/pdf/129139-WP-PUBLIC-Focus-Note-Building-Inclusive-Payment-Ecosystems-June-2018.pdf
6. Chapman, J. and Holtham, C, (1994), "Technology in Service Delivery", Alfred Walter Limited. World, 3rd Ed., Cincinnati, Ohio, South Western Publishing Co. Ltd.
7. Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," Management Science (35:8), August 1989, pp. 982-1003.
8. HAIR, J. F., RINGLE, C. M., & SARSTEDT, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. Long Range Planning, 46, 1-12
9. Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM). London: SAGE Publications, Incorporated.
10. Hoope, S. (2013). The role of mobile money services in improving microfinance services in rural. Retrieved July 2019, from scholar.mzumbe.ac.tz: http://scholar.mzumbe.ac.tz/bitstream/handle/11192/378/MBA%20%20Dissertation-%20Saskia%20Hoope-.2013.pdf?sequence=1

11. IPP Media. (2014, February 2). Number of Internet users still low in Tanzania, says global report.

12. Intersecurity Magazine. (2013). Global Cybercrimes Costs.

13. Jack, William and Tavneet Suri. 2009 “Mobile Money: The Economics of M-Pesa” MIT Sloan School of Management Working Paper

14. Kline, R. B. (2016). Principles and practice of structural equation modeling (4th ed.). New York, NY: Guilford Press.

15. Kombo, D. K. (2014). Proposal and thesis writing. Nairobi: Paulines Publications Africa.

16. Lu, L. (2019) Mobile Payments—Why They Are So Successful?. *Open Journal of Business and Management*, **7**, 1131-1143. doi: 10.4236/ojbm.2019.73078.

17. Leow, Hock Bee (1999), "New Distribution Channels in banking Services." Banker’s Journal Malaysia,No.110, June 1999, p.48-56.

18. Lubua, E. (2014). Adoption of E-transparency in the Tanzanian Public Sector. Durban: University of KwaZulu Natal.

19. Mayunga, J. (2013). Cybercrimes Investigation in Tanzania. Morogoro: Mzumbe University

20. Maria Zhdanova, Jurgen Repp, Roland Rieke, Chrystel Gaber, and Baptiste Hemery. “No smurfs: Revealing fraud chains in mobile money transfers”. In: 9th International Conference on Availability, Reliability and Security, ARES 2014. IEEE, 2014, pp. 11–20.

21. Morawczynski, O., & Pickens, M. (2009). Poor people using mobile financial services: Observations on customer usage and impact from M-PESA. Washington, DC: CGAP.

22. Michael, N.; Kelley, D.; Victoria, Y.; (2017) An Introduction to Information Security, NIST Special Publication 800-12 Revision 1

23. Porteous, D. (2006).The Enabling Environment for Mobile Banking in Africa, Report Commissioned by Department for International Development – DFID, Vol. 3.1.

24. Pallant, J. (2016). SPSS survival manual : a step by step guide to data analysis using SPSS. (6 edn). Maidenhead :Open University Press/McGraw-Hill,

25. Paelo, A. (2017). A Comparison of the Mobile Financial Services Sector in Kenya, Tanzania and Uganda. Annual Competition and Economic Regulation (ACER) Conference. Dar es Salaam, Tanzania.

26. Rogers, E. M. (1995). Diffusion of innovation. The Free Press, New York (1995)

27. Sirken. (2009). Ministry of finance audit findings on M-Pesa money transfer services.

28. Singer, P.W., Friedman, Allan. (2014). Cybersecurity and Cyberwar : What Everyone Needs to Know . Oxford: Oxford University Press.

29. Tanzania Communications Regulatory Authority Paper, 2015; "Know your Rights: Rights and Obligations of communications consumer's services" www.tcra.go.tz

30. Tanzania Communications Regulatory Authority Regulator (March, April – June, 2019). Mobile Money Fraud in Dar es Salaam, Dar es Salaam TCRA, pp.17 – 19

31. Tobbin, P. (2011). Adoption of Mobile Money Transfer Technology: Structural Equation Modeling Approach. European Jounal of Business and Management, 72-74.

32. UNCTAD. (2012). Mobile Money for Business Development in the East African Community. United Nations Conference on Trade and Development (p. 1). Switzerland: United Nations Publication.

33. Vaughan, Pauline. 2007. "Early lessons from the deployment of M-PESA, Vodafone's own mobile transactions service" In The Transformational Potential of M-transactions, Vodaphone Policy Paper Series, No.6. Online http://www.vodaphone.com/m-transactions

34. Wilson, K., M. Harper, and M. Griffith (eds). 2010. Financial Promise for the Poor: How Groups Build Microsavings. Kumarian Press.

35. Wilson Van Voorhis, C. R., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. Tutorials in Quantitative Methods for Psychology, 3, 43–50. doi:http://dx.doi.org/10.20982/tqmp.03.2.p043