I. J. Computer Network and Information Security, **2018, 12, 21-33**
Published Online December 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.12.03

Security Risk Analysis and Management in mobile wallet transaction: A Case study of Pagatech Nigeria Limited

Musbau D. Abdulrahaman, John K. Alhassan
Federal University of Technology, Minna, Minna, Niger state, Ngeria.
E-mail: abdulrahaman.pg7186@st.futminna.edu.ng, jkalhassan@futminna.edu.ng

Joseph A. Ojeniyi and Shafii M. Abdulhamid
Federal University of Technology, Minna, Minna, Niger state, Nigeria.
E-mail: ojeniyija@futminna.edu.ng and shafii.abdulhamid@futminna.edu.ng

Received: 16 June 2018; Accepted: 28 October 2018; Published: 08 December 2018

***Abstract*—**Mobile wallet is a payment platform that stores money as a value in a digital account on mobile device which can then be used for payments with or without the need for the use credit/debit cards. The cases of cyber-attacks are on the rise, posing threats to the confidentiality, integrity and availability of information systems including the mobile wallet transactions. Due to the adverse impacts of cyber-attacks on the mobile payment service providers and the users, as well as the risks associated with the use of information systems, performing risk management becomes imperative for business organizations. This research work focuses on the assessment of the vulnerabilities associated with mobile wallet transactions and performs an empirical risk management in order to derive the security priority level needed to ensure the security and privacy of the users of mobile wallet platforms. Based on the extensive literature review, a structured questionnaire was designed and administered to the mobile wallet users who are Paga student customers via the internet. A total number of 52 respondents participated in the research and their responses were analyzed using descriptive statistics. The results of the analysis show that mobile wallet Login details are the most important part of customer information that need to be highly protected as their compromise is likely to affect others. Also, customers' information such as Mobile Wallet Account Number, Registered Phone Number, Linked ATM Card details, and Linked ATM Card PIN among others are also plausible to attacks. Hence, different security priority levels were derived to safeguard each of the components and possible security tools and mechanisms are recommended. The study also revealed that there are vulnerabilities from the mobile wallet users end that also pose threat to the security of the payment system and customers' transaction which need to be properly addressed. This research work will enable the mobile payment service providers focus on their services and prioritize the security solutions for each user's information types or components base on the risks associated with their system and help in taking an inform security related decisions.

***Index Terms*—**Security Risk Analysis, Electronic Payment, Mobile Payment, Mobile Wallet transaction, Risk Management, Information System Security.

I. Introduction

Over the years, payment has always been an integral part of human commercial activities mostly through paper currency and face to face method. Owing to the development in computing and technology which has transformed the mode of transacting businesses, thereby making payments flexible and convenient through electronic commerce (e-commerce). Electronic commerce was designed to eliminate or reduce some of the problems in physical payment characterized by many problems and given individuals, organizations as well as banking sectors financial transactions headache [1]. Some of the problems of the traditional physical payment systems including experience of long queue at banks while making deposit or withdrawal, making a stressful and very long distance journey in order to settle payment for goods and services, and paying utility bills. With electronic payment system, customers now have access to their bank information anywhere at any time, and making financial transactions possible without paying a physical visit to banks. Mobile payment is one of the numerous payment platforms in electronic payment system operates under financial guideline for financial transactions from or through mobile phone. Reference [2] defined mobile payment as any transaction which involves the use of a mobile device such as mobile phone, Smartphone, tablet, Personal Digital Assistant (PDA) to initiate, authorize or confirm an exchange of financial value in return for goods and services. The growth in the mobile technology has made it spreads across the nations including the rural areas, and continuously improving the way people gets

closer and making payments for goods and services in an efficient, faster and easier manner. Mobile payment solution has been long anticipated for since early 2000s, but recently gained much needed attention and adoption especially in the US, Europe, Asia, including some developing countries such as Kenya, Tanzania, South Africa and Nigeria. This is as a result of its benefit to improving the payment infrastructure with the ability to reduce the usage of non-cash in circulation.

With respect to the importance of payment in our lives, coupled with the increasing demands for the adoption of mobile payment by many organizations and clients, mobile wallet has emerged as one of the mobile payment solutions that leverage on the ubiquity and mobility of mobile devices and seeks to replace the use of traditional credit/debit cards with mobile phones. Mobile wallet is a digital account with the combination of hardware and software in smartphone that stores money as virtual value which can be used to perform financial transactions and payments [3]. The mobile wallet is continuing to grow due to its enormous benefits such as needless for carrying credit/debit cards around, ability to provide additional value offerings such as location based services to be delivered near the Point of Sale (POS) and the financial inclusion which makes payment to be convenient, faster and economical. With mobile wallet, people can pay money to any account using smartphone application, social media or website, and text messages. The world wide mobile payment volume is also increasing and leading to the launching of several new solutions such as Samsung Pay, Google Pay and Apple Pay digital wallet.

Pagatech Nigeria Limited is a financial service firm licensed by central bank of Nigeria, to leverage on the ubiquity of mobile phones and internet technologies and provide online payment system. Paga acts like a mobile wallet whereby users can conduct financial transactions via mobile phones or internet enabled computers or devices [4]. The essence of Paga is to ensure financial inclusiveness to all Africa irrespective of where they are at any time through seeking to include the unbanked and underbanked population in the digital banking era [5]. With Paga, customers can perform several financial services such as deposit, purchase pre-paid phone credit, pay utility and cable bills, and make payments to retailers. Interestingly, the partnership between Paga and Western Union has also added the benefit where Western Money transfers sent to users can be deposited into the users' Paga accounts. The firm works in partnership with selected Banks, Microfinance institutions, and all Mobile Network Operators. Paga was founded in the early 2009 by Tayo Oviosu but launched publicly in the year 2011. It currently has four people as members of its board of directors with Tani as the Managing Director of Resource Plc, Tayo Oviosu as the founder and Chief Executive Officer (CEO), Tokunboh Ishmael and Yemi Lalude. Paga mission is to continue transforming lives through providing innovative and universal access to financial services [6]. Some of the Paga mobile payment (wallet) platform competitors in Nigeria including e-Transact, Pay Pal, Quick Teller, Pay U, Eazy Money, Airtel Money, Vogue and Global Pay.

Globally, cyber-attacks have cost companies in excess of several millions of dollars in term of security breach claims and also reduced the customer confidence in organizations and patronage. Despite the enormous benefits provided by the mobile wallet platforms, there are a lot of security challenges associated with which has raised concerns among the financial and academic communities due to the networking environment through which the mobile payment system works and the risks associated with the use of information systems for various financial transactions. These security challenges are posing threats to the confidentiality, integrity and availability of the information, information system as well as mobile wallet transactions which have adverse impacts on both the service providers and the users [3].

A business organization like mobile wallet service provider who deploys technologies for the provision of financial services needs to ensure the security and privacy of their information, systems and network. Failure of a business organization to safeguard its information resources from any information or cyber security incidents may have high adverse impact on the business, employees, customers and the business associates. It is actually believed that no business can be completely secure, but it is reasonable to implement a program that balances the security with the needs and capability of the business. Therefore, it becomes imperative for businesses such as mobile wallet providers to analyze the vulnerabilities in its system through risk management process in order to minimize or reduce the impact of the security incidents [7].

The mobile payment system stakeholders can be broadly categorized into two, service providers and service customers. The extensive literature review shows that there are few research works that focus on investigating the vulnerabilities in the mobile wallet system that pose threat to the security and privacy of mobile payment customers' information and the likelihood of attacks on the payment platforms based on the security measures currently put in place by the mobile wallet service providers in Nigeria. The aim of this research work is to analyze the security risks in mobile wallet transactions using Pagatech Nigeria Limited customers as a case study for the purpose of understanding the most important information used by users for financial transactions and the likelihood of attacks on those information types. The outcome of the research furnishes the mobile wallet service providers with the knowledge of the impact of each customer's information components and the risks associated with the platform in order to prioritize their information or cyber security efforts.

The remaining chapter is organized thus: section 2 provides a review of related works while chapter 3 describes the method used for this paper. Chapter 4 presents the data analysis and results of the finding, chapter 5 concludes the work, while chapter 6 presents some recommendation and acknowledgement.

II. Literature Review

Mobile technology has been described as the best innovation ever for mankind, due to the way it is influencing lives of ordinary people and still continue to create opportunities with different dimensions to businesses and individuals [8]. The trend in the mobile technology has witnessed the emergence of mobile device as an inevitable component in the payment system. Mobile device can now be used to initiate or complete financial transactions in a manner that do not requires physical presence of individual at banks or moving about with paper currency as they can now make payment for goods and services through mobile payment platform [9]. Mobile payment can be defined as any transaction which involves the use of a mobile device such as mobile phone, Smartphone, tablet, Personal Digital Assistant (PDA) to initiate, authorize or confirm an exchange of financial value in return for goods and services [2]. In other words, it is a payment for products as services between parties for which a mobile device plays a key role in the realization of the payment.

The recent studies show that there is tremendous improvement in the acceptance of mobile payment method in both advanced and emerging economies. This has led to the emergence of different mobile payment methods especially mobile wallet [3]. Reference [3] defines mobile wallet as virtual platform that stores digital value in form of wallet out of which you can make money transactions and pay for goods and services just like traditional paper money. The recent trend in the mobile payment including Apple Pay, Google Pay, Pay Pal, Airtel Money, Quick Teller, e-transact, easy money, Paga, Pay U, Global Pay. This mobile payment technology has a combination of software and hardware on a certain device and seek to replace the use of traditional credit/debit cards with mobile phones.

Mobile payment can be categorized into two based on the technologies used to deliver them which are either remote or proximity payment [10]. In a remote mobile payment system customers are required to register for a service usually involves downloading of application and then use it on their mobile devices to pay for items. Customers may have some values stored in a prepaid account (digital wallet) or draw funds directly from a linked banked account. For instance, payment service provides like Google, Pay Pal, and Go Pago use a cloud-based remote payment to for their services. On the other hand, Proximity payment system requires customers to present a credit/debit card, mobile phone, or tablet at the point of payment in order to complete the transaction. This payment method is facilitated by Near Field Communication (NFC) which is often referred to as "Contactless Payment" [2].

Many stakeholders are involving in the mobile payment ecosystem such as "merchants", "customers", "mobile network operators", "payment service providers", "device manufacturers" and "financial institutions", but can be broadly categorized as mobile payment customers and mobile payment service providers. Basically, there are different stakeholders that play active role in mobile payment (wallet) ecosystem [11]. Mobile payment business model can be categorized as; (1) operator centric model, which is coordinated by network operator to customers with NFC enabled mobile devices; Bank centric model is usually overseen by banks (2) peer-to-peer model enables providers to take advantage of the existing online applications to complete transaction without POS infrastructure required (3) Collaboration model is a n ideal model that allows several stakeholders focus on their core competencies. It involves mobile operators, banks, trusted third-party who are responsible for the management of mobile payment system.

The review of related works shows that despite the enormous benefits of information system in ensuring works are performed faster, efficiently and convenient, there exist lot of security risks that affect both business and its customers which usually leads to huge loss.

Reference [12] investigated methods for the identification of potentials losses in the user organization. the paper reviewed some prior literature on various methods for the analysis and reporting of losses in organization. It understudies a business process analysis method that involves a systematic analysis of potential losses in different phases of organization's core business process, using action research to examine to associate the information system available risk with potential losses in business. The analysis was based on two different companies, one from paper industry and in financial sector. Data was collected through direct observations, interviews of the company's employees using tape recorder and the review of company documents. The study revealed some risks in the use of information systems for business processes and identify the potential business losses the IS risks can cause to the company.

Reference [3] reviewed several literatures in order to obtain high level understanding of various threat types that are likely to affect mobile wallet applications with its possible countermeasures. It identified and analyzed different threats and vulnerabilities of a typical mobile wallet application. The study shows that most of the mobile wallet service providers have been implementing most of the security solutions due to the fast development of mobile technology and digital wallet. The research findings also indicated that if new payment solution is identified, it will increase the trust boundaries within the mobile wallet payment system. Similarly, Reference [2] reviewed some academic literature to generate discussion about the vulnerabilities generated by mobile technology in retail in order to provide platform for the investigation of potential risks associated with it. The author harnesses learning from the implementation of self –checkout which is combined with the available information relating to mobile scanning (m-scan) as well as mobile point of sale (MPOS). Aside from searching online journals, industry publications and web resources, the study also interviewed some retail security professionals who are working within asset protection, loss prevention, and business development while focusing on fast-moving consumer goods (FMCGs) in the food and grocery sector

predominantly. The study found that mobile payment market is flooded with software products which exposes retailers to many payment platforms, but they are not cognizant of enormous potential risks therein. However, the study recommended further research to study the permutation of mobile POS and it impacts on the customers when it comes to internal and external theft.

A research to test the functional relationship between adoption reediness (AR), perceived risk (PR) and usage intention for mobile payments in India was carried out by [9] to investigate the stability of proposed structural relationships across different customer groups. A mixed method research was employed for the development and validation of the proposed research method which involves literature review and extensive interviews with experts from industry and academia. A systematic literature review was conducted to review major attributes of technology acceptance in order to develop construct for AR. The model was later tested empirically using structural equation modelling. Three steps were adopted for the analysis. The first confirms the factor structure of measurement items of antecedents of mobile payment services. The second investigates the relative importance of each dimension in the customer's usage intention, while the third explores invariance between respondent sub-groups based on usage. It was reported the proposed model supported five out of six hypotheses whereas one hypothesis was supported partially, while the test of invariance showed significant variance among users and non-users.

In [1], the authors studied the user acceptability as well as the payment problems encountered by Nigerians while using electronic banking system. It also examined the contribution of e-payment to the elimination or reduction of problems in the traditional payment system. A qualitative research method was used to collect data from primary and secondary sources. A total number of 500 questionnaires were sent to First Bank Plc, United Bank for Africa Plc and Guarantee Trust Bank Plc employees, customers and some corporate bodies in Nigeria of which only 484 responses were received given a response rate of 96.8%. The study revealed that cash usage is still very high in Nigeria despite the efforts of Central Bank of Nigeria towards the adoption of electronic payment system. The finding posed that this is caused by the problems of inadequate power supply, shortage of critical technological infrastructures, lack of sociocultural support and absence of regulatory framework that are required to operate seamless and effective electronic payment system in Nigeria. The need for government to remove barriers innovation which includes those challenges earlier mentioned and the regulatory barriers to pave way for rapid development of the electronic payment systems in the country was recommended.

According to [8], the paper investigated extent of the adoption and usage of the mobile phone banking services among banking customers in Nigeria as well as ascertain associated problems. The paper also studies the levels of usage and no usage of these financial services by customers within Nigeria. The study sampled staff, student customers who are in higher institutions of 10 out of 21 commercial banks in Nigeria. The data was gathered for two months using unstructured set of interview questions and the analysis was done through the thematic evidences that arose from the data analyzed. Their findings revealed that despite the fact that phone banking was more established than internet banking and ATM services, ATM services had a wider reach and adoption due to some hindering factors such as educational level of customers, poverty and infrastructure deficit and cost and maintenance involved. Awareness creation on mobile banking, security improvement from service providers, and proper regulation to curb excesses and misuse both from the service providers, customers and malicious users were advocated.

III. Research Method

A Qualitative research method was used to survey some undergraduate and postgraduate students who are mobile wallet users and Paga customers. The choice of the two categories of the respondents is to be sure that the participants are literate since the mobile payment services are provided in English language by most of the mobile platforms in Nigeria. Based on the literature reviewed and an in-depth study of the mobile payment system using Paga as a case study, the researcher was able to understand the mode of operation of mobile wallet, its major components and information types use, store and process including some vulnerabilities, threats and possible attacks on the system. A structured questionnaire was constructed based on the information security program procedure provided in [7] using google form and administered via some social media groups belonging to undergraduate and postgraduate students. A total number of 52 valid responses were received and analyzed using descriptive statistics.

IV. Data Analysis and Results

After the responses of the questionnaire were received and thoroughly investigated, a descriptive statistic was used as a method for data analysis. The result of the demographic profile of the respondents in table 1 shows that 76% (40) of respondents are male while 23.1% (12) of the respondents are female. Age wise, the results shows that majority of the respondents who are mobile wallet users based on the age bracket tested are within 21 years and 30 with 50%, while those within the age bracket of 41 years above who are using mobile wallet are less than those below them. This shows that the mobile wallet system is popular between the younger age. The table also shows that most of the respondents are postgraduate students with 29 (55.8%) compare to undergraduate which is 23 (44.2%). Most of the respondents have claimed to have been using the mobile payment for more than 2 years which is good for the reliability of the research as who have had more experience of the platform. The result also indicates that

most of the respondents use mobile wallet for financial transaction regularly.

A. Demographic Profile of the Respondents

Table 1. Demographic Profile of the Participants

Alternative	Respondents	Percentage
Gender		
Male	40	76.9
Female	12	23.1
Total	**52**	**100**
Age		
Less than 20 years	5	9.6
21 – 30 years	26	50
31 – 40 years	18	34.6
41 above	3	5.8
Total	**52**	**100**
Program		
Postgraduate	29	55.8
Undergraduate	23	44.2
Total	**52**	**100**
Experience with mobile wallet (payment)		
0 - 1 year	12	23.1
2 - 4 years	21	40.4
5 years above	19	36.5
Total	**52**	**100**
Mobile wallet usage intensity in a month		
I use it Rarely	15	28.8
I use it Occasionally	21	40.4
I use it frequently	16	30.8
Total	**52**	**100**

B. Identification and Ranking of Customer Information

According to the risk management framework provided by [7], information security program begins with the identification of the information stores and uses for a business. Since, the research focuses on identifying the risks associated with the mobile wallet information used the customers during financial transaction. In order to identify various information used by mobile wallet customers, an extensive literature review was done including a case study of Pagatech Nigeria limited which is one of the leading mobile wallet providers in Nigeria. After the important users' information were identified, the respondents were asked to rank them based on the level of the importance of each information components to the success of the payment as well as the impact of the information on them. A five point Likert was adopted for ranking, ranging from (Not important "1" to very important "5"). Table 2 shows the rating of the important information components used by mobile wallet users. The customer information column represents all the identified information needed by users to perform financial transactions on the mobile wallet application platform. The ranking options gives the various ranking possibilities of the information based on their importance to the users. The response and percentage columns give the distribution of the respondents in term of number (frequency) and percentage according to the ranking options. For ease of analysis, the ranking option was further categorized into three point Likert option where "Not important "represents "Low impact", "Less important" and "Important" represent "Medium impact", and "More Important" and "Very Important" represent "High impact" respectively. In selecting the overall impact, the impact with the highest number of responses for each information component is selected as either Low, Medium, or High depending on the nature of the distribution.

Table 2. Ranking of the Mobile Wallet Customers' Information

Customer Information Component	Ranking Options	Response	Percentage	Impact	Overall Impact
Mobile wallet account Username	Not important	0	0	Low (0)	High
	Less important	3	5.8	Medium (24)	
	Important	21	40.4		
	More important	8	15.4	**High (28)**	
	Very important	20	38.5		
Mobile wallet account PIN	Not important	0	0	Low (0)	High
	Less Important	0	0	Medium (12)	
	Important	12	23.1		
	More Important	5	9.6	High (40)	
	Very Important	35	67.3		
Mobile wallet account Number	Not important	0	0	Low (0)	High
	Less Important	4	7.7	Medium (22)	
	Important	18	34.6		
	More Important	9	17.3	**High (30)**	
	Very Important	21	40.4		
Registered Phone Number	Not important	1	1.9	Low (1)	High
	Less Important	2	3.8	Medium (18)	
	Important	16	30.8		
	More Important	13	25	**High (33)**	
	Very Important	20	38.5		
Registered E-mail Address	Not important	2	3.8	Low (2)	Medium
	Less Important	10	19.2	**Medium (34)**	
	Important	24	46.2		
	More Important	4	7.7	High (16)	
	Very Important	12	23.1		

Supply E-mail Address Password	Not important	10	19.2	Low (10)	High
	Less Important	8	15.4	Medium (20)	
	Important	12	23.1		
	More Important	3	5.8	**High (22)**	
	Very Important	19	36.5		
Linked Bank Account Number	Not important	4	7.7	Low (4)	Medium
	Less Important	8	15.4	**Medium (25)**	
	Important	17	32.7		
	More Important	4	7.7	High (23)	
	Very Important	19	36.5		
Linked Bank Account Name	Not important	4	7.7	Low (4)	Medium
	Less Important	17	32.5	**Medium (30)**	
	Important	13	25		
	More Important	7	13.5	High (18)	
	Very Important	11	21.2		
Linked ATM card details	Not important	8	15.4	Low (8)	High
	Less Important	4	7.7	Medium (18)	
	Important	14	26.9		
	More Important	11	21.2	**High (26)**	
	Very Important	15	28.8		
Linked ATM card PIN	Not important	10	19.2	Low (10)	High
	Less Important	7	13.5	Medium (16)	
	Important	9	17.3		
	More Important	5	9.6	**High (26)**	
	Very Important	21	40.4		
Transaction OTP	Not important	10	19.2	Low (10)	Medium
	Less Important	7	13.5	Medium (16)	
	Important	9	17.3		
	More Important	5	9.6	**High (24)**	
	Very Important	21	40.4		
Transaction e-receipt	Not Important	2	3.8	Low (2)	Medium
	Less Important	8	15.4	Medium **(29)**	
	Important	21	40.4		
	More important	8	15.4	High (21)	
	Very Important	13	25		

From table 2 it was observed that the Mobile wallet account Username, Mobile wallet account PIN, Mobile wallet account Number, registered Phone Number, Supply Email Address Password, Linked ATM card details, Linked ATM Card PIN are the most important of the customers' information with "High" value or impact, while the Registered Email Address, Linked Bank Account, Linked Bank Account Name, Transaction OTP and Transaction e-receipt are considered less important to the mobile payment transaction. The distribution of the impact of the mobile wallet customers' information is summarized in table 3.

Table 3. Summary of the Impact of the Mobile Wallet user Information

S/N	Mobile wallet Customer Information	Impact
1	Mobile Wallet Account Username	High
2	Mobile Wallet Account Pin	High
3	Mobile Wallet Account No	High
4	Registered Phone No	High
5	Registered EMail Address	Medium
6	Supply EMail Address Password	High
7	Linked Bank Account No	Medium
8	Linked Bank Account Name	Medium
9	Linked ATM Card details	High
10	Linked ATM Card Pin	High
11	Transaction OTP	Medium
12	Transaction e-receipt	Medium

C. Inventory of Technology

Inventory development process is an important stage when it comes to the information security program. This phase enables the security professional to identify the technologies that come in contact with the information uses, stores, processes and transmitted by the mobile payment system during financial transaction. To do this, the respondents were asked to select the technologies (hardware/software) used for financial transactions with mobile wallet (payment) from those that have been pre-identified by the author. Table 4 and Fig. 1 represent the distribution of the responses from the participants. The results show that majority of respondents mostly use mobile phone for payment transaction (78.8%) followed by Internet with 53.8%. It also shows that customers use Laptop/Desktop and Unstructured Supplementary Service Data (USSD) for transaction by recording 36.5% and 25% respectively, while only 19.5% of the respondents use Short Message Service (SMS) and recorded the least used technology according to the survey.

Table 4. Inventory of Technologies used by Mobile Wallet Customers

S/N	Technology	Response	Percentage
1	Mobile phone	41	78.8
2	Laptop/Desktop Computer	19	36.5
3	USSD	13	25
4	SMS	10	19.2
5	Internet	28	53.8

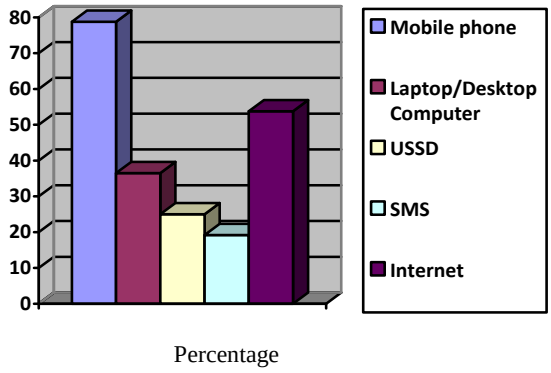

Fig.1. Inventory of Technologies used by Mobile Wallet Customers

D. Vulnerability and Threat from Mobile Wallet Users

Human are usually regarded as the weakest link in the information security chain. Therefore, to ensure the security risk management efforts put in place by the mobile wallet service providers are not jeopardized, the vulnerabilities from the side of the service users that can also contribute to the threat to the business and users' information must be identified and considered. This research work asked some information security related questions from the participants in order to assess the vulnerabilities and threats to the security of their information and mobile payment services. Table 5 and Fig. 2 show the distribution of responses of mobile wallet users to the vulnerability and threat related issues from their end. According to the customers' responses, the probability of the user's information comprises as a result of lost/stolen mobile phone is high with respect to 76.9% responses, 40.4% of the users believed they are not likely to installed malicious programs on their devices whether intentionally or accidentally, 50% of respondents believed they are likely to disclose their information to third party, while 46.2% believed it is possible to give OS legitimate permission which may likely be used by hackers to attack them. Finally, about 53.8 of users believed that their mobile devices may also contribute to inability to access mobile payment services due to issues such as power failure. In essence, the distribution of the users' responses show that the vulnerabilities also exist from the mobile wallet customers end and need to be addressed in order to ensure safe mobile payment transaction.

Table 5. Vulnerabilities and Threats to Mobile Wallet System from Customers

S/N	Security related Questions	Response	Percentage
1	My mobile phone/device can be get stolen or lost, I may grant my device's Operating System permission to modify my data legitimately, which may also be hijacked by hackers	40	76.9
2	I may install a malicious application on my devices accidentally	21	40.4
3	I may disclose my mobile wallet information to a relative accidentally/intentionally	26	50
4	I may grant my device's Operating System permission to modify my data legitimately, which may also be hijacked by hackers	24	46.2
5	My mobile phone/device can be get stolen or lost, My mobile devices may not be reached due to power failure or otherwise	28	53.8

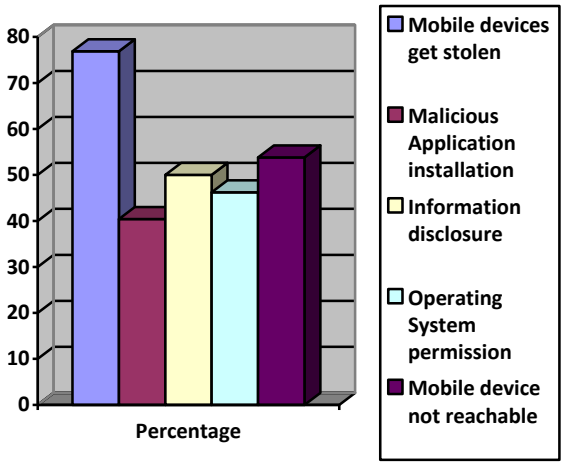

Fig.2. Vulnerabilities and Threats to Mobile Wallet System from Customers

E. Vulnerability and threat from mobile wallet service providers

Part of the information security risk analysis and management steps is the understanding of the vulnerabilities in mobile wallet system as provided by various service providers which pose threats to the confidentiality, integrity, and availability of the customers' information components. This becomes necessary as it will enable the likelihood of attack on each business and customer related information be identified for an informed security decision to be made. This paper asked different security related questions from mobile wallet users who are respondents in this survey. The security questions were based on assessing the possibility of unauthorized access or disclosure (Confidentiality), unauthorized modification (integrity), and the possibility of the failure of the service based on the failure of each of the identified important users' information. The result of the opinion of the mobile

wallet users regarding vulnerability and threat of the payment platform with respect to the security measures provided by various stakeholders in the service provides spectrum is given in table 6. To elicit the opinion of the mobile wallet users on the possibility of attack on their information, the research made use of five point Likert options ranging from "Not possible, Less Possible, Maybe, Possible, and Very Possible". For the sake of making the analysis easier and more presentable, the author re-categorized the scale into three Likert options where "Low" represents "Not Possible", "Medium" represents "Less possible and May be", and "High" represents "Possible and Very Possible" respectively. In selecting the overall attack likelihood, the likelihood with the highest number of responses with respect to the CIA related questions for each information component is selected as either Low, Medium, or High depending on the nature of the distribution. For instance, if response for confidentiality related question is high, and integrity related response is also high, while availability related question is low or medium, then, the overall likelihood for that information components will be high since it has 2/3.

Table 6. Vulnerability, Threat and Likelihood of Attack on Customer Information Component

Customer Information Component	**Security Properties**	**Question Options**	**Response**	**Percentage**	**Likelihood**	**Overall Likelihood**
Mobile wallet account Username	Confidentiality (possibility of unauthorized access or disclosure)	Not Possible	1	1.9	Low (1)	**High**
		Less Possible	4	7.7	Medium (25)	
		May be	21	40.4		
		Possible	17	32.7	High (26)	
		Very Possible	9	17.3		
	Integrity (possibility of unauthorized modification)	Not Possible	7	13.5	Low (7)	
		Less Possible	8	15.4	Medium (30)	
		May be	22	42.3		
		Possible	13	25	High (15)	
		Very Possible	2	3.8		
	Availability (possibility of service failure)	Not Possible	2	3.8	Low (2)	
		Less Possible	8	15.4	Medium (24)	
		May be	16	30.8		
		Possible	20	38.5	High (26)	
		Very Possible	6	11.5		
Mobile wallet account PIN	Confidentiality (possibility of unauthorized access or disclosure)	Not Possible	5	9.6	Low (5)	**High**
		Less Possible	9	17.3	Medium (23)	
		May be	14	26.9		
		Possible	20	38.5	High (24)	
		Very Possible	4	7.7		
	Integrity (possibility of unauthorized modification)	Not Possible	4	7.7	Low (4)	
		Less Possible	9	17.3	Medium (26)	
		May be	17	32.7		
		Possible	18	34.6	High (22)	
		Very Possible	4	7.7		
	Availability (possibility of service failure)	Not Possible	0	0	Low (0)	
		Less Possible	5	9.6	Medium (21)	
		May be	16	30.8		
		Possible	27	51.9	High (31)	
		Very Possible	4	7.7		
Mobile wallet account Number	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	2	3.8	Low (2)	**Medium**
		Less Possible	10	19.2	**Medium (26)**	
		May be	16	30.8		
		Possible	18	34.6	High (24)	
		Very Possible	6	11.5		
	Integrity (possibility of unauthorized modification)	Not Possible	3	5.8	Low (3)	
		Less Possible	8	15.4	**Medium (27)**	
		May be	19	36.5		
		Possible	16	30.8	High (22)	
		Very Possible	6	11.5		
	Availability (possibility of service failure)	Not Possible	2	3.8	Low (2)	
		Less Possible	5	9.6	**Medium (27)**	
		May be	22	42.3		
		Possible	18	34.6	High (23)	
		Very Possible	5	9.6		
Registered Phone Number	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	1	1.9	Low (1)	**Medium**
		Less Possible	8	15.4	**Medium (27)**	
		May be	19	36.5		
		Possible	15	28.8	High (24)	
		Very Possible	9	17.3		
	Integrity (possibility of unauthorized modification)	Not Possible	5	9.6	Low (5)	
		Less Possible	10	19.2	**Medium (27)**	
		May be	17	32.7		
		Possible	14	26.9	High (20)	
		Very Possible	6	11.5		
	Availability (possibility of service failure)	Not Possible	6	11.5	Low (6)	
		Less Possible	4	7.7	Medium (21)	
		May be	17	32.7		
		Possible	20	38.5	**High (25)**	
		Very Possible	5	9.6		

Registered E-mail Address	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	2	3.8	Low (2)	**Medium**
		Less Possible	8	15.4	**Medium (27)**	
		May be	19	36.5		
		Possible	19	36.5	High (23)	
		Very Possible	4	7.7		
	Integrity (possibility of unauthorized modification)	Not Possible	5	9.6	Low (5)	
		Less Possible	9	17.3	**Medium (27)**	
		May be	18	34.6		
		Possible	16	30.8	High (20)	
		Very Possible	4	7.7		
	Availability (possibility of service failure)	Not Possible	5	9.6	Low (5)	
		Less Possible	10	19.2	**Medium (26)**	
		May be	16	30.8		
		Possible	19	36.5	High (21)	
		Very Possible	2	3.8		
Supply E-mail Address Password	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	3	5.8	Low (3)	**Medium**
		Less Possible	9	17.3	**Medium (30)**	
		May be	21	40.4		
		Possible	14	26.9	High (19)	
		Very Possible	5	9.6		
	Integrity (possibility of unauthorized modification)	Not Possible	5	9.6	Low (5)	
		Less Possible	7	13.5	**Medium (26)**	
		May be	19	36.6		
		Possible	17	32.7	High (21)	
		Very Possible	4	7.7		
	Availability (possibility of service failure)	Not Possible	2	3.8	Low (2)	
		Less Possible	11	21.2	**Medium (32)**	
		May be	21	40.4		
		Possible	15	28.8	High (18)	
		Very Possible	3	5.8		
Linked Bank Account Number	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	3	5.8	Low (3)	**Medium**
		Less Possible	8	15.4	**Medium (25)**	
		May be	17	32.7		
		Possible	19	36.5	High (24)	
		Very Possible	5	9.6		
	Integrity (possibility of unauthorized modification)	Not Possible	2	3.8	Low(2)	
		Less Possible	9	17.3	**Medium (29)**	
		May be	20	38.5		
		Possible	13	25	High (21)	
		Very Possible	8	15.4		
	Availability (possibility of service failure)	Not Possible	1	1.9	Low (1)	
		Less Possible	6	11.5	Medium (25)	
		May be	19	36.5		
		Possible	24	26.2	**High (26)**	
		Very Possible	2	3.8		
Linked Bank Account Name	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	1	1.9	Low (1)	**Medium**
		Less Possible	8	15.4	Medium (24)	
		May be	16	30.8		
		Possible	21	40.4	**High (27)**	
		Very Possible	6	11.5		
	Integrity (possibility of unauthorized modification)	Not Possible	3	5.8	Low (3)	
		Less Possible	11	21.2	**Medium (26)**	
		May be	15	28.8		
		Possible	15	28.8	High (23)	
		Very Possible	8	15.4		
	Availability (possibility of service failure)	Not Possible	5	9.6	Low (5)	
		Less Possible	12	23.1	**Medium (27)**	
		May be	15	28.8		
		Possible	17	32.7	High (20)	
		Very Possible	3	5.8		
Linked ATM card details	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	3	5.8	Low (3)	**Medium**
		Less Possible	7	13.5	**Medium (25)**	
		May be	18	34.6		
		Possible	17	32.7	High (24)	
		Very Possible	7	13.5		
	Integrity (possibility of unauthorized modification)	Not Possible	4	7.7	Low (4)	
		Less Possible	10	19.2	**Medium (25)**	
		May be	15	28.8		
		Possible	18	34.6	High (23)	
		Very Possible	5	9.6		
	Availability (possibility of service failure)	Not Possible	3	5.8	Low (3)	
		Less Possible	11	21.2	**Medium (25)**	
		May be	14	26.9		
		Possible	20	38.5	High (24)	
		Very Possible	4	7.7		

Linked ATM card PIN	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	4	7.7	Low (4)	**Medium**
		Less Possible	5	9.6	Medium (21)	
		May be	16	30.8		
		Possible	18	34.6	**High (27)**	
		Very Possible	9	17.3		
	Integrity (possibility of unauthorized modification)	Not Possible	6	11.5	Low (6)	
		Less Possible	12	23.1	**Medium (26)**	
		May be	14	26.9		
		Possible	11	21.2	High (20)	
		Very Possible	9	17.3		
	Availability (possibility of service failure)	Not Possible	4	7.7	Low (4)	
		Less Possible	10	19.2	**Medium (25)**	
		May be	15	28.8		
		Possible	17	32.7	High (23)	
		Very Possible	6	11.5		
Transaction OTP	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	7	13.5	Low (7)	**Medium**
		Less Possible	7	13.5	**Medium (26)**	
		May be	19	36.5		
		Possible	13	25	High (19)	
		Very Possible	6	11.5		
	Integrity (possibility of unauthorized modification)	Not Possible	10	19.2	Low (10)	
		Less Possible	11	21.2	**Medium (26)**	
		May be	15	28.8		
		Possible	12	23.1	High (16)	
		Very Possible	4	7.7		
	Availability (possibility of service failure)	Not Possible	4	7.7	Low (4)	
		Less Possible	12	23.1	Medium (23)	
		May be	11	21.2		
		Possible	19	36.5	**High (25)**	
		Very Possible	6	11.5		
Transaction e-receipt	**Confidentiality** (possibility of unauthorized access or disclosure)	Not Possible	5	9.6	Low (5)	**High**
		Less Possible	6	11.5	Medium (23)	
		May be	17	32.7		
		Possible	18	34.6	**High (24)**	
		Very Possible	6	11.5		
	Integrity (possibility of unauthorized modification)	Not Possible	4	7.7	Low (4)	
		Less Possible	10	19.2	**Medium (27)**	
		May be	17	32.7		
		Possible	15	28.8	High (21)	
		Very Possible	6	11.5		
	Availability (possibility of service failure)	Not Possible	5	9.6	Low (5)	
		Less Possible	6	11.5	Medium (22)	
		May be	16	30.8		
		Possible	20	38.5	**High (25)**	
		Very Possible	5	9.6		

From table 6 it was observed that the Mobile wallet account Username, Mobile wallet account PIN, and Transaction e-receipt have high possibility of being attacked based on the results responses of users, while Mobile wallet account Number, registered Phone Number, Supply Email Address Password, Linked ATM card details, Linked ATM Card PIN are the most important of the customer information with "High" value or impact, while the Registered Email Address, Linked Bank Account, Linked Bank Account Name, Transaction OTP are considered less likely to be attacked due to current countermeasures already put in place by various service providers in the mobile payment system. The distribution of the likelihood of security incidents on the mobile wallet customers' information is summarized in table 7 based on the analysis performed.

Table 7. Summary of the Impact of the Mobile Wallet user Information

S/N	Mobile wallet Customer Information	Attack Likelihood
1	Mobile Wallet Account Username	High
2	Mobile Wallet Account Pin	High
3	Mobile Wallet Account No	Medium
4	Registered Phone No	Medium
5	Registered EMail Address	Medium
6	Supply EMail Address Password	Medium
7	Linked Bank Account No	Medium
8	Linked Bank Account Name	Medium
9	Linked ATM Card details	Medium
10	Linked ATM Card Pin	Medium
11	Transaction OTP	Medium
12	Transaction e-receipt	High

F. Prioritizing the Information Security Efforts

The final stage of the risk management program as recommended by the NIST (National Institute of Standards and Technology) as described in(Paulsen & Toth, 2016)is to combine the impact or value of identified information components (types) with the likelihood of security incidents, in order to help organization or business determine the information security efforts needed to secure users information and their information systems. Securing every aspect of business information with the same level of security may not be feasible as it might be too expensive for the business. Therefore, a need for prioritizing the security efforts is highly important. The table 8 shows the priority level that determines the security efforts needed to ensure security and privacy of the mobile wallet users based on the combination of the impact and the likelihood. Each priority level also indicates various processes and tools the businesses need to consider to protect the information and information systems based on the cyber security

framework.

Table 8. Prioritize Resolution Action

Impact	**High**	Priority 5	Priority 2	Priority 1
	Medium	Priority 7	Priority 4	Priority 3
	Low	Priority 0: No action needed	Priority 8	Priority 6
		Low	**Medium**	**High**
		Likelihood		

Source: Adapted from [7] and modified by the author

1) **Priority 1:** This level requires that the mobile wallet (payment) service provider should implement an **"immediate"** security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
2) **Priority 2:** it requires that the mobile wallet (payment) service provider should implement an **"immediate"** security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
3) **Priority 3:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
4) **Priority 4:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
5) **Priority 5:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
6) **Priority 6:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
7) **Priority 7:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
8) **Priority 8:** This requires that the mobile wallet service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
9) **Priority 0:** This requires no serious action to be implemented or scheduled from the information security professional

Therefore, from the prioritize resolution action in table 8 we then derive the prioritize security efforts needed by the mobile wallet service providers in order to ensure security and privacy of their customers' information and presented in table 9.

Table 9. Prioritize Security Efforts Needed

S/N	Mobile wallet Customer Information	Impact	Attack Likelihood	Priority Level
1	Mobile Wallet Account Username	High	High	Priority 1
2	Mobile Wallet Account Pin	High	High	Priority 1
3	Mobile Wallet Account No	High	Medium	Priority 2
4	Registered Phone No	High	Medium	Priority 2
5	Registered EMail Address	Medium	Medium	Priority 4
6	Supply EMail Address Password	High	Medium	Priority 2
7	Linked Bank Account No	Medium	Medium	Priority 4
8	Linked Bank Account Name	Medium	Medium	Priority 4
9	Linked ATM Card details	High	Medium	Priority 2
10	Linked ATM Card Pin	High	Medium	Priority 2
11	Transaction OTP	Medium	Medium	Priority 4
12	Transaction e-receipt	Medium	High	Priority 3

Based on the results of the customer information impact analysis as well as the likelihood of attacks on each of information which produces the security priority level shown in table 9, it can be deduced that customers believed that most of the information components identified are very important for the payment transaction, hence, the result of the rating that shows only high and medium. The result also shows that the mobile wallet system requires the security efforts that range between priority levels 1 to level 4. It also indicates that Mobile Wallet Account Username, Mobile Wallet Account PIN (Login PIN) are to be well protected as they provide access to the entire user's information. The priority level 1 requires an immediate implementation of security solutions that can detect and protect account credentials such as authentication, encryption, access control, and non-repudiation mechanisms. The Mobile Wallet Account No, Registered Phone No, Supply EMail Address Password, Linked ATM Card details, and Linked ATM Card PIN also deserved to be properly secured as the results shows that they need priority level 2, which requires that immediate security solutions be implemented immediately using various attack detection and prevention mechanisms be put in place. Some of the security mechanisms including patching of Operating systems and applications, regular changing of user and

server password, using a secure encryption technique for the stored and transmitted data, installation of malware and antivirus software as well as the installation of Firewalls and IDS (intrusion detection system) and maintain event logs among others. Only Transaction e-receipt requires the security level 3 acceding to the results of the analysis of mobile wallet customers. This is also necessary since most of the payment transactions mostly require the payees to present an evidence of payment such as SMS alert or email notification. Any compromise on the payment e-receipt may render the payment illegitimate, therefore requires a scheduling of security mechanisms capable of detecting and protecting any actions that can compromise the legitimacy of payment transaction e-receipt.

Finally, the prioritize security effort table also shows that Registered Email Address, Linked Bank Account No, Linked Bank Account Name, and Transaction OTP require level 4 security priority due to the fact that they have medium impact on the transaction and are moderately not likely to be attacked with respect to the security measures already provided by the concerned service providers. A schedule detection and protection measures should be provided in order to ensure security and privacy of the customer data as well as protecting the business from loss.

V. Conclusions

The paper conducted a research on security risk analysis and management in mobile wallet payment transaction by using Pagatech Nigeria limited as a case study. Mobile wallet customers are an integral part of the mobile payment ecosystem that determines the success of the platform. A cross section of mobile wallet users who are student customers were sampled using online survey platform to elicit their opinions concerning the vulnerability and threat in the mobile wallet system based on their experience. The results show that mobile wallet users agreed with the important customer related information components identified by the author from the literature and ranked the impact of the information. The analysis also revealed that there are vulnerabilities in the mobile wallet platform that cut across different service providers that are threat to the security of the customers' information and the adoptability of the mobile payment. The results of the analysis also revealed what parts of the customers' information are mostly prone to attacks and source of security nightmare for users. Based on the results various security priority levels were derived in order to protect each customer's information type or component. Finally, the research also revealed that there are vulnerabilities from the side of mobile users who are also posing threats to the security of the mobile payment system. These user's vulnerabilities need to be addressed, especially through awareness creation and implementation of security policies and procedures that will ensure that customers always comply with the minimum security guideline such as installation of antivirus and malware detection software on their devices, password management skills, and always install, update and upgrade to the latest original mobile wallet applications.

Recommendation

The result of the findings shows in order to have a secure and safe mobile payment transaction, both customers and service providers involved must take cognizance of the vulnerabilities that are posing threats to mobile wallet platforms at their ends and device a means to manage the risks holistically. It is recommended that mobile wallet service providers as well as other business organizations that deploy technologies for their business processes should make information or cyber security program as part of business strategy. This will enable the businesses to understand the vulnerabilities and the threats associated with the information and systems used for business processes, helps in determining the right security priority level needed to safeguard each information types as well as earning the organization loyalty among the employees, customers and partners. Finally, the Information System dependent organizations such as mobile payment service providers should endeavor to engage security professionals whether in-house or outsourced, to perform penetration testing activities for them regularly in order to discover vulnerabilities and threats in their systems because malicious actors get to know about and exploit them against the company.

For future work, the security risk analysis and management in mobile wallet transaction using another payment platform or focusing other stakeholders such as mobile payment agents, merchants, and service providers may be researched.

Aknowledgement

The authors wish to sincerely appreciate the Department of Cyber Security Science (Federal University of Technology Minna) and the Department of Information and Communication Science (University of Ilorin) respectively for providing us with enabling environment and the necessary research instruments while carrying out this work. More importantly, Dr. Joseph A. Ojeniyi is acknowledged for his scholarly guides and mentoring towards the completion on this work. Finally, we appreciate the respondents who participated in the survey and Pagatech Nigeria Limited for the information used in this work.

References

[1] Felix, N. E., & Gideon, K. E. (2012). Electronic Retail Payment System: User Acceptability and Payment Problems in Nigeria. *Arabian Journal of Business and Management Review*, *1*(6), 18–35.

[2] Taylor, E. (2016). Mobile payment technologies in retail: a review of potential benefits and risks. *International Journal of Retail and Distribution Management*, *44*(2), 159–177. https://doi.org/10.1108/IJRDM-05-2015-0065.

[3] Bosamia, M. (2018). Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible

security Measures, (April).
[4] Paga (2018). Getting Started. Retrieved from https://mypaga.atlassian.net/wiki/spaces/PFBRA/pages/1573201/Getting+started [Accessed on August 10, 2018]
[5] Investopedia (2018). Paga. Retrieved from https://www.investopedia.com/terms/p/paga.asp [Accessed on August 10, 2018]
[6] Bloomberg (2018). Company Overview of Pagatech Limited. Retrived from https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=129149971 [Accessed on August 10, 2018]
[7] Paulsen, C., & Toth, P. (2016). *Small Business Information Security: The Fundamentals*. https://doi.org/10.6028/NIST.IR.7621r1
[8] Agwu, E. M., & Carter, A.-L. (2014). Mobile Phone Banking in Nigeria: Benefits, Problems and Prospects. *International Journal of Business and Commerce*, *3*(6), 50–70. https://doi.org/10.1080/08874417.2015.11645781
[9] Thakur, R., & Srivastava, M. (2014). Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India, *24*(3), 369–392. https://doi.org/10.1108/IntR-12-2012-0244
[10] Slade, E. L. (2015). Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and University of Bristol - Explor, *32*, 860–873. https://doi.org/10.1002/mar.20823
[11] Ba, J. (2012). Analysis of Security Risks in Mobile Payments. A Case Study Using DNAT Acknowledgement.
[12] Salmela, H. (2014). Analysing business losses caused by information systems risk: A business process analysis approach, (April). https://doi.org/10.1057/palgrave.jit.2000122
[13] Yang, Q., Pang, C., Liu, L., Yen, D. C., & Tarn, J. M. (2015). Computers in Human Behavior Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *COMPUTERS IN HUMAN BEHAVIOR*, *50*, 9–24. https://doi.org/10.1016/j.chb.2015.03.058
[14] Yang, Y. (2015). Understanding perceived risks in mobile payment acceptance. https://doi.org/10.1108/IMDS-08-2014-0243
[15] Yusuf, S., & Lee, J. (2015). Technology Adoption: A conjoint analysis of consumers' preference on future online banking services. *Information Systems*, 1–15. https://doi.org/10.1016/j.is.2015.04.006

Authors' Profiles

Musbau D. Abdulrahaman born in 1987, is currently an MTECH student at the department of cyber security science, Federal University of Technology Minna, Minna, Niger State, Nigeria. He is an academic staff at the department of information and communication science, University of Ilorin, Ilorin, Nigeria. His current research interest including Network intrusion detection, cloud security, IoT security, machine learning, and information system security.

John K. Alhassan is a lecturer and current head of department of cyber security science, Federal University of Technology Minna, Minna, Niger State, Nigeria. Holds PhD in Computer Science. His area of research includes Artificial Intelligence, Data Mining, Internet Technology, Database Management System, Software Architecture, Machine Learning, Human Computer Interaction, Computer Security and Big Data Analytics

Joseph A. Ojeniyi is a lecturer and researcher at the department of cyber security science, Federal University of Technology Minna, Minna, Niger State, Nigeria. He is a Ph. D holder in cyber security, he has been carrying out several innovative researches and has supervised many MTECH thesis work. His research interest includes Network Security and Digital Forensic

Shafii M. Abdulhamid is a lecturer and researcher at the department of cyber security, Federal University of Technology Minna, Minna, Niger State, Nigeria. His research interest includes cyber security, cloud computing, soft computing, IoT security, and big data.

How to cite this paper: Musbau D. Abdulrahaman, John K. Alhassan, Joseph A. Ojeniyi, Shafii M. Abdulhamid,"Security Risk Analysis and Management in mobile wallet transaction: A Case study of Pagatech Nigeria Limited", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.12, pp.21-33, 2018.DOI: 10.5815/ijcnis.2018.12.03