ASHESI UNIVERSITY COLLEGE

MOBILE FINANCIAL SERVICES IN GHANA- MEASURES FOR ACHIEVING SAFETY AND SECURITY OF SERVICES.

UNDERGRADUATE THESIS

B.Sc. Management Information Systems

Stephanie Belnye

2017

ASHESI UNIVERSITY COLLEGE

Mobile Financial Services In Ghana- Measures For Achieving Safety And Security Of Services.

UNDERGRADUATE THESIS

Thesis submitted to the Department of Computer Science, Ashesi University College in partial fulfilment of the requirements for the award of Bachelor of Science degree in Management Information Systems

Stephanie Belnye

April 2017

Declaration

I hereby declare that this [capstone type] is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:

……

Candidate's Name:

……

Date: ……

I hereby declare that preparation and presentation of this [capstone type] were supervised in accordance with the guidelines on supervision of [capstone type] laid down by Ashesi University College.

Supervisor's Signature:

……

Supervisor's Name:

……

Date: ……

Acknowledgement

I want to thank God for guiding me through this project. I would also like to acknowledge everyone who contributed to making this paper a success. First of all, I wish to acknowledge my supervisor, Mr. Stephane Nwolley for his timeless dedication and constructive feedback throughout the supervision of this project.

I would also like to acknowledge the immense contribution of my father, Mr. Franklin Belnye for his professional guidance and constructive feedback.

I appreciate the contributions from all the faculty members for their guidance and constructive feedback during the presentations.

Abstract

The use of mobile phones has become part of the daily activities of about ninety percent of Ghanaian adults. This has contributed to the rapid adoption of mobile financial services by Ghanaians. In 2014, Bank of Ghana reported over two million registered users. Africa and the rest of the world have also experienced this exponential growth in the use of mobile financial services. Due to the huge money it is raising in that sector, fraudsters have made several attempts on these systems leading to the loss of enormous sums of money. The objective of this study is to understand the mobile financial service ecosystem in Ghana and internationally, assess what risks users may face and suggest measures to help prevent or reduce the effects of these risks.

In order to better understand the concept of mobile financial service, some academic papers were reviewed revealing the components of the ecosystem, risks that these players may face and some proposed solutions by scholars. Case studies, in-depth interviews and secondary data were gathered for this research.

Findings from the data collected show that some risks users may face include: malware infection of devices or point of sale terminals, corruption of information stored on the server of acquirers or service providers, theft of data during transaction, including man-in-the-middle attacks, advanced persistent thefts and insecure data connectivity.

Also some mitigation measures to these threats include enforcement of two factor authentication on systems, securing data connections using Secured Socket Layer (SSL) authentication, secure configuration, hardening of critical servers and data encryption during transactions.

This study is limited geographically because the interviews held included players in the mobile financial service ecosystem in Accra only. Also only three companies were interviewed for this study due to the limited time constraint.

Table of Contents

List of Abbreviations.

Abbreviation	**Meaning**
CGAP	The World Bank's Consultative Group to Assist the Poor
DSS	Data Security Standard
ECG	Electricity Company of Ghana
EMV	Europay, Mastercard and Visa
FSP	Financial Service Provider
ISACA	Information Systems Audit and Control Association
ISO	The International Organization of Standardization
Mobile Network Operators	MNO
MP	Mobile Payment
mPOS	Mobile Point of sale
NFC	Near Field Communication
NSP	Network Service Provider
P2P	Peer-to-Peer Transactions
PCI	Payment Card Industry
POS	Point of Sale
POI	Point of sale terminal
PSP	Payment Service Provider
QR code	Quick Response code
SIM	Subscriber Identity Module
SEMOPS	Secure Mobile Payment Service
SMS	Short Message Service
SSL	Secured Socket Layer
TGC	Trusted Computing Group
TPM	Trusted Platform Module
TSM	Trusted Service Managers
WIM	Wireless Identity Module

Chapter 1: Introduction

1.1 Background/Context of the Study

Mobile Financial Services is a set of mobile banking services which consist of using portable devices connected to telecommunications networks that provide users with access to mobile payments, transactions and other banking and financial services related to customer accounts with or without the direct participation of conventional banking institutions (Diniz, Albuquerque & Cernev, 2011).

The increased use of mobile phones has changed not only business and everyday life but also the way financial transactions are carried out. Cell phones are providing an opportunity for the growth of financial activity in developing countries where the number of phone owners surpasses the number of people with bank accounts. The wide use of mobile phones has created a new opportunity for service providers and merchants to create mobile wallets on phones which are then used for storing value and making payments.

According to a survey conducted by the Gates Foundation, the World Bank and Gallup World Poll, out of the top 20 countries in the world for mobile money usage, 15 are in Africa. Kenya has 80% of the world's mobile money transactions. Also, Kenya's M-pesa has nearly two million users registered with the system within a year of its nationwide rollout (Ivantury & Mas, 2008; Vaughan 2007). M-pesa also provides services to 15 million Kenyans (more than a third of the country's population) and serves as a channel for a fifth of the country's GDP and processes more transactions domestically within Kenya than Western Union does globally, providing more banking facilities to more than 70 percent of the country's adult population. (Bampoe, 2015).

Kenya is not the only country with a high percentage of its population adopting to mobile financial services: - in The Philippines, three million customers use the systems offered by mobile operators Smart and Globe (infoDev, 2006). South Africa recorded that 450,000

people use Wizzit—the bank in your pocket (Ivantury &Pickens, 2006) or two other national systems. And in Ghana, the number of active mobile money customers on the network of leading mobile operators—MTN, Tigo and Airtel were nearly 2.4 million as of end-2014 (Bank of Ghana). Tanzania is also mentioned as one of the leading countries in this sector. Considering the fact that Ghana is referred to as the most digitally financial services-ready country in Africa and also the current growth rate of mobile financial services in the country, it is possible for Ghana to take the position of Kenya in some years to come.

Mobile financial services are promoting socioeconomic development in emerging markets. Tom Standage stated in an *Economist* article (17 Nov 2011) that, "it is easier to use your mobile phone to pay for a taxi in Nairobi [Kenya's capital] than in New York." The Global Findex Database 2014 reported that 75 percent of Kenyan adults or eight out of every 10 Kenyan adults is banked through bank and mobile money accounts.

Mobile financial services adoption requires "mobile readiness". In 2015, a survey was conducted considering the four indicators of "mobile readiness". Ghana outranked Rwanda, Kenya and Tanzania. The World Bank's Consultative Group to Assist the Poor(CGAP), declared Ghana as "the most digital financial service- ready country in Africa" when it comes to the key elements needed for successful adoption (Adjorlolo, 2015). This is because, 92% of adults have the required ID necessary to open an account and 91% of Ghanaians already own a mobile phone (compared to only 74% and 72% in Kenya and Tanzania, respectively).

1.2 Research Problem

Notwithstanding the aforementioned benefits and role of mobile money or mobile payment in banking penetration, there remain some challenges. The growing global use of mobile phones has led to some significant security problems. Mobile devices and networks have become vulnerable in the ways that the networked desktops and laptops currently are.

As the importance of mobile phones to personal commerce and finance has grown, so they have become targets for criminals.

There have been several reports on fraud in the mobile money market and the numbers continue to increase. Fraud in the context of mobile money is the intentional and deliberate action undertaken by players in the mobile financial services ecosystem aimed at deriving gain (in cash or e-money), and/or denying other players revenue and/or damaging the reputation of the other stakeholders. (Mudiri, 2017). There have been attacks on some mobile payments systems in Kenya. The Africa News reported on Kenyan job seekers being victimized by phishers. The article stated that cyber-criminals had created vacancies for accountants, brew masters and some other positions. The job applicants were expected to pay a "refundable" application fee of approximately US$70 via Safaricom M-Pesa system. There have also been reports that Kenya could lose up to US$23 billion through cybercrime in the mobile banking industry if some security measures are not put in place immediately. Kenya is not the only African country on this list. Also according to an article by MicroSave, an average of at least hundred mobile money users lose money every week, some lose millions of shillings.

Some of the causes of fraud in the mobile money market include weak regulations guiding the systems, maturity of mobile financial services, weak or non-standardized processes within the system, unavailability of compliance monitoring, lack of consumer awareness and poor communication within the system. (Mudiri, 2017). Some other ways include PIN Appropriation, which involves fraudsters stealing or copying the code of users by watching them as they dial them while pretending to be making a transaction and finally by SIM replacement.

According to the World Bank, the main threats to the use of mobile banking across

the globe are money laundering and terrorist funding. These reported cases may be the beginning of the stated threats. Could Ghana be at risk or already a victim considering the causes of fraud listed above? This research will look into Ghana's mobile financial services and develop ways to improve the security of the systems.

1.3 Objectives of the Study.

1. To understand how these mobile payment systems work locally and internationally.
2. To find gaps in Ghana's systems to precipitate the issues raised above.
3. To propose measures to make mobile financial services safe for the users, service providers and the country.

1.4 Research Questions

1. How do we develop mobile financial services that are safe for the customers and businesses to use?
2. What are the risks that users and service providers may face and how can they be managed or minimized?

1.5 Significance of the Study

This study will add to the research done in the fields of financial inclusion and mobile innovation. It will also serve as a guide or resource for Mobile Network Operators, Software Development Companies, policymakers and other stakeholders in the mobile financial services industry when developing a framework for mobile banking products.

Also, this study will help stakeholders to understand the types of fraud in the mobile banking sector and highlight the importance of solving this problem. It will help to create awareness of the possible risks that users face and make the public more conscious. Developing a more secured system may win more customers and thus reduce the percentage of the unbanked in the country.

1.6 Scope of the Study

Recognizing the high possibility of growth of the mobile money payment systems, this study focuses on examining the issues posed to consumers and the security measures that are being put in place by the various stakeholders. The assessment of security standards will be based on compliance with some international standards such as the ISO 27001 to find out how our local regulations meet these standards. In examining fraud in mobile financial services, the study will consider it under three categories—consumer driven, agent driven and business partner related fraud.

1.7 Overview of Methodology

This study would require a careful examination of the policies set by the Bank of Ghana to govern mobile financial services in Ghana and some international standards that govern mobile financial services across the globe. The study employs some qualitative research approaches such as interviewing employees of the mobile financial service providers to gather information on how these services are run in Ghana as well as some of the threats that the companies have faced so far. It also includes assessing the structure of some international service providers to study how these systems are built internationally. The study made use of secondary data from research done in this field and other related fields.

1.8 Limitations of the Study

The limitation of this study include the small sample size that was interviewed during the data collection. This was due to the limited time constraint. This limitation can be alleviated by ensuring that a data collection period is done during less busy work period, probably during holidays in order to conduct in-depth interviews with more service providers.

1.9 Chapter Disposition.

The research paper is organized in five chapters. The content of each chapter is briefly described below.

Chapter One is an introduction or background to the study and also addresses the

research problem, the objectives of the study, the research questions/hypotheses, the significance of the study and the proposed methodology.

Chapter Two reviews the literature on the subject, highlighting the arguments and findings made by scholars who have worked in this research area. It gives the reader a theoretical background of mobile financial services, the processes involved, the players involved and some proposed academic solutions to the challenges being faced in the mobile payment services industry.

Chapter Three presents a detailed description of the methods used in the research. It also explains the reason for the chosen approach and the variety of individuals who took part in this study.

Chapter Four presents the analyses of the results of the study. It gives a detailed examination of the findings and thoughts of the author. It represents major points in tables and bullet points to ensure clarity and easy readability.

Chapter Five outlines the conclusion drawn by the author as well as recommendations. It explains the theoretical significance of the study and points out the limitations or flaws of the research design.

Chapter 2: Literature Review

2.1 Definition of mobile financial services.

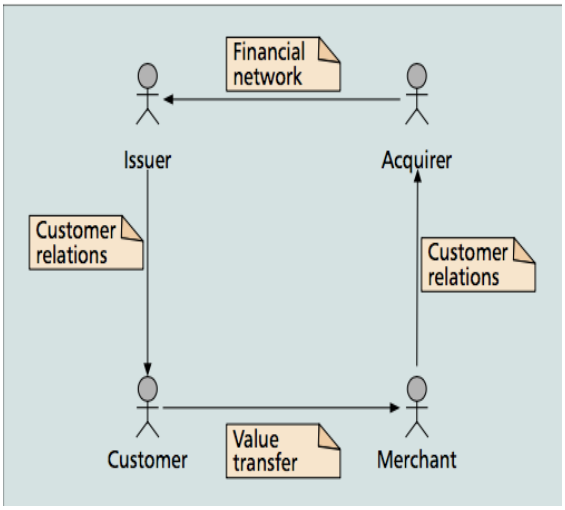
Mobile financial services refer to transactions carried out through mobile technologies and devices. It includes every kind of mobile transactions offered by technology whether it involves financial values or not. (Diniz, Albuquerque & Cernev, 2011). A mobile financial service provider is a company whose aim is to provide services that allow users to transfer money and/or exchange money for goods and services between two users of the service (Reserve Bank of Malawi, 2011).

Mobile financial services can be categorized into three concepts—mobile payments, mobile banking and mobile money. Mobile banking is the use of mobile phones to manage bank accounts that is, receive debit or credit card alerts and statements via SMS, check balances, transfer funds and pay bills via a mobile application (Kaya, 2013). Mobile payments on the other hand are payments services operated under financial regulation and performed from or via a mobile device (Penttila, Siira & Tihinen, 2016). Mobile money is the use of mobile devices to move funds from one account to another, make withdrawals and deposits or pay bills. Mobile payments are payments made using digital mobile technologies through handled devices, with or without mobile telecommunications networks. These payments are digital financial transactions, although not necessarily linked to financial institutions or banks.

Mobile money is similar to a mobile wallet which is a digital storage of electronic money developed and used on mobile devices, allowing peer-to-peer transactions(P2P), between mobile devices of the same mobile network. Just like the physical wallet, it is used to store money, credit and debit cards (Diniz, Albuquerque & Cernev, 2011).

2.2 The Processes and Major Players Involved.

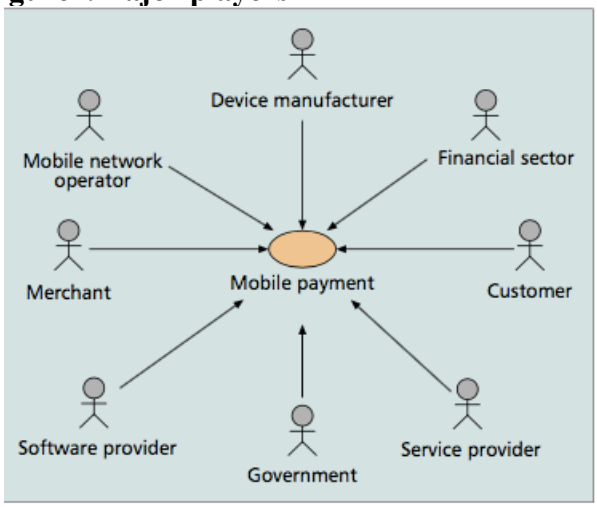
Figure 1. The Payment Process



(Karnoukos & Fokus, 2004).

Figure 1 shows the payment process in every mobile transaction or payment. The customer is the party making the payment; the merchant is the party accepting the payment; the acquirer is the third party from the financial network that has a relationship with the merchant and the issuer is the party affiliated to the financial network that has a link to the customer. In every payment process, the goal is the value transfer from the customer to the merchant. The mobile payment arena employs a similar procedure to the one followed by credit card companies. The customer "pays" a merchant for purchased goods/services. The merchant goes on to send the transaction details to the acquirer for clearing. The acquirer forwards the transaction details to the financial system which it belongs (e.g. VISA), which then forwards the details to the issuer. The scheme pays the acquirer, the acquirer settles the merchant, the issuer pays the scheme and the customer pays the issuer. The unique feature about the mobile payment process is that the customer and the merchant use mobile devices in order to realize a transaction.

Figure2.Major players



(Karnoukos & Fokus, 2004).

Figure 2 displays the main parties in a mobile payment scheme. These players interact with each other via the MP process. They include the mobile network operators(MNO), the financial sector institutions (that is banks, credit card companies, payments processors, etc.), the government (legislations and regulation constraints) and of course, the device, mobile application/ software and the service providers. (Karnoukos & Fokus, 2004).

The MNOs usually have an enormous customer base because they either control the subscriber identity module(SIM) or the wireless identity module(WIM) card of the mobile device, thus they have a great impact on the MP model. Nonetheless, they cannot fully run the MP system since they have limited experience in payment services. Due to this, they work with financial institutions who have great expertise in this field. The successful cooperation of both parties is key to empowering the MP era. The manufacturers of the devices used also play a very important role in the ecosystem. They regulate the technology and capabilities of the end-device, which affects the implementation and deployment of a MP service immensely. Hence it is very important that the producers of the devices cooperate with each other and other MP players to find a common approach to developing the mobile devices. The last player which is the software providers also develop applications or software that implements the mobile payment process. The service providers introduce the service to the market and adapt it to the

users' needs. Mobile network operators can also play the role of the service providers and offer limited MP service on their own. (Karnoukos & Fokus, 2004).

2.3 The Mobile Banking Ecosystem

The mobile banking ecosystem involves the following types of stakeholders: consumers, financial service providers (FSPs), payment service providers(PSPs), in-service providers (merchants) including contents providers, network service providers(NSP), device manufacturers, regulators, standardization and industry bodies, trusted service managers(TSM) and application developers. (ISACA, 2011).

These participants can take a variety of forms—financial institutions, debit/credit card networks, clearing/settlement organizations, software solutions providers, third-party payment processors, MNO/wireless operators, handset/chip manufacturers, customer and merchants. Each stakeholder fights to take a share of the revenue in the ecosystems with financial institutions, debit/credit card providers and MNOs competing for the role of FSP and NSP and for the related transaction fees. Mobile contactless payment is one application among the many. Figure 3 represents the life cycle of a Bank-centric NFC mobile payment. (ISACA, 2011).

Figure 3. Life Cycle of a Bank-centric NFC Mobile Payment

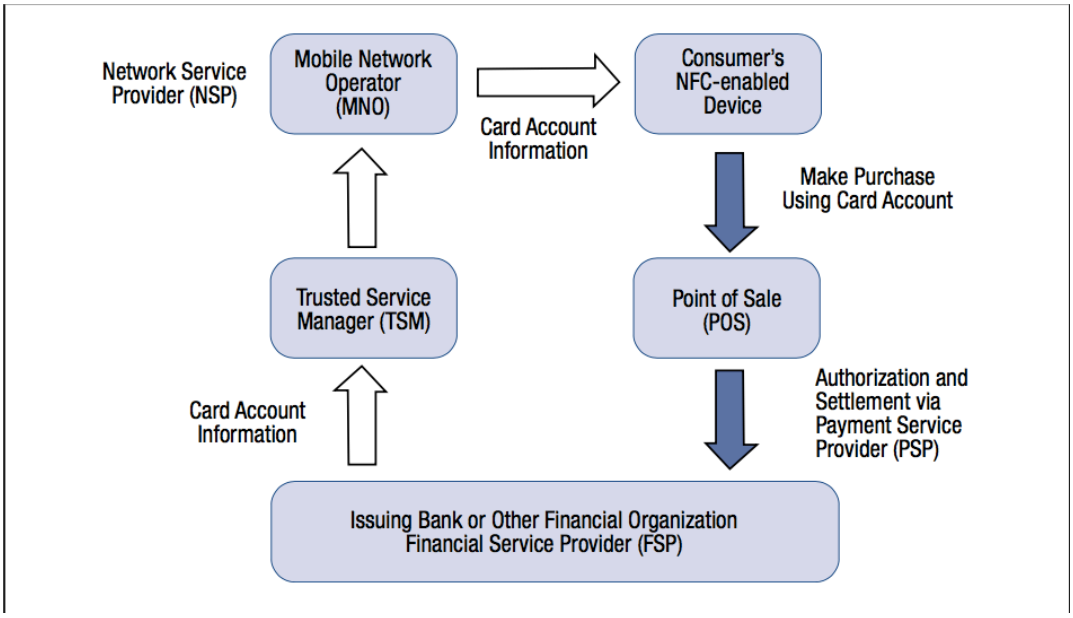


Figure 3. (ISACA, 2011).

From figure 3, we can see the flow of information concerning: the provision of the consumer's payment account information to the phone from the issuing financial organisation (personalization of the device) and the authorization of the NFC proximity mobile payment via an existing PSP provider network. The solid arrows used in the diagram indicates payment-related transactions, while the outlined arrows represent actions related to the personalization of the application. In drawing this cycle, there is an assumption that the user's mobile device that hosts the NFC chip is a trusted platform, that is, it utilizes a trusted platform module(TPM) as defined and specified by the Trusted Computing Group(TCG) (ISACA, 2011).

2.4 Type of Mobile Payment Systems.

Mobile payment supplements the traditional payment methods by introducing mobile devices as the point of sale (for the cardholder), using the mobile device as the point of sale (for the merchant or retailer), mobile payment platforms and direct carrier billing. Mobile payment systems can be categorized under five types: mobile payment as the point of sale(POS), mobile payment at the POS, mobile payment platform, independent mobile

payment system and direct carrier billing. Mobile payment at the POS is usually referred to as the mobile wallet and the mobile payment platform is used to make purchases from multiple merchants and retailers (Wang, Hahn & Sutrave, 2016).

- **Mobile Payment at the POS**: This method allows the user to pay for goods/services with a mobile phone at the POS. Most of the methods are based on a built-in NFC technology such as Google Wallet and Apple Pay. These built-in payments system are easy to set up on a mobile device. SMSGH new product Mpower is an example of a mobile payment platform at the POS. It has a mPOS application in the Google Play Store(Android) which permits merchants to accept electronic payment from platforms such as Visa cards from local banks, MasterCard, other debit and credit cards, mobile money and even international platforms such as PayPal.

  In setting up your Apple Pay account, you first either scan the card number with a camera or enter the number manually, including the three-digit security code, expiration date and the name of the card holder. Apple Pay checks with the issuer to make sure the information provided is valid. If it is, the user is asked to agree to the terms and conditions and then the card is added to the wallet. Android Pay and Samsung Pay follow similar procedures. (Wang, Hahn & Sutrave, 2016).

  Now moving on to how this system works, the user holds his phone over a NFC-enabled terminal to a make a connection using NFC. When the phone is unlocked, the transaction is validated with the secure element(SE) chip. This chip sends an authorization signal back to the NFC modem. The rest of the process is similar to how the traditional swipe credit card works. The terminal sends the merchant's ID number, card information and transaction amount to the card processor. When the processor reads the information, it sends an authorization signal to the card issuer. The financial institution which issued the card checks for fraud and verifies if there is enough money

in the card to cover the requested amount. It approves if there is enough balance, if there is not, it declines the transaction. It sends a message to the merchant concerning the decision made. (Wang, Hahn & Sutrave, 2016).

- **Mobile Payment as the POS**: This method permits merchants to use the mobile phone as the POS and process card payments. To use this method, a merchant downloads a mobile application to his mobile device and connects a credit card reader to his phone. This method is seen as very easy to use, time saving and convenient. (Wang, Hahn & Sutrave, 2016).

  Square Register is an example of the mobile payment which falls under this category. Square Register is mobile payment service popular in the United States of America. It supports both transactions from a keyed-in transaction and a credit card reader. Square Register accepts three types of credit cards: magnetic stripe cards, EMV chip cards and contactless chips.

- **Mobile Payment Platform**: This technique offers the user online payment services on a mobile device. The user is required to download a mobile application on his device. It can be used as mobile wallet to make payment at a POS. The credit card or bank account of the user is used to link the mobile payment account.

  Express Pay is an example of the mobile payment platform. Express Pay supports transactions from a credit card reader as well as keyed-in transactions. Express Pay allows users to top up credit by transferring funds from their bank account or credit card and with this money, pay for goods and services who are affiliated to the company as well. (Wang, Hahn & Sutrave, 2016).

- **Independent Mobile Payment System**: This method is very similar to the mobile payment platforms. Some companies develop their own online payment service to support mobile devices. These systems are referred to as independent mobile payment

systems. The independent mobile payment systems are developed for only the company. Some examples of such platforms include Amazon and Starbucks mobile payments services.

If the independent mobile payment systems are widely adopted by many merchants and retailers, it can be transformed into a mobile payment system. For example, WeChat red envelope was a program developed by WeChat in 2014. Due to its popularity, it was converted to a mobile payment platform. WeChat wallet is being used by numerous merchants and retailers in China. (Wang, Hahn & Sutrave, 2016).

- **Direct Carrier Billing**: This model allows users to purchase products or services using their mobile devices. It does not involve a credit or debit card as payment. The total cost of purchase made by the users is charged on the mobile subscriber's monthly phone bill. An SMS message is sent to the users containing the bill. A transaction code is provided to the user via a text message. The user enters the code on the website to confirm the purchase. (Wang, Hahn & Sutrave, 2016). It is very popular in Europe.

2.5 Literature of Some Proposed Solutions to The Security Issues in MFS

2.5.1 Secure and Efficient Protocol for Mobile Payments

SEMOPS (Secure Mobile Payment Service) is a system proposed by A. Vilmos and S. Karnoukos to provide a secure platform where competing service providers will give secure mobile payment services. SEMOPS was made to suit every type of mobile payment platforms thus, it is not specific to any technology and it is an open standard. It was designed to address the limited computational power of mobile devices and also the fact that not so many cryptographic operations can be performed on mobile devices. The entities in the system include the users, payment processor, bank and data centre.

In ensuring that this system makes mobile payment services more secured, it uses PIN authorisation to ensure that customer payment processor has proof of customer transactions.

This system also increases efficiency by grouping multiple micropayments and reduces effective payment cost overhead. A timer is used to check atomicity. Each entity in the system starts a timer when it sends a message to the next entity. The message goes missing, the timer expires and the whole transaction is cancelled. The customer payment processor signs each payment notice it sends to the merchant payment processor. The customer payment processor and the merchant payment processor keep records of who they interact with and are trusted by customers and merchants.

2.5.2Near-Field Communication-Based Secure Mobile Payment Service.

The Near Field Communication(NFC) based mobile phone payment solution offers the required data protection without requiring costly changes to the payment processing infrastructure. This prototype views the mobile phone as a single, user-trusted touch point. The strengths of this solution to mobile financial services security include better user control over the transaction and it supports both near and remote transactions.

There have been several reports on the loss of customer account information. The Payment Card Industry(PCI) Data Security Standard(DSS) provide the necessary tools and guidelines required to protect cardholder data, merchants and service providers. The PCI DSS is apportioned into six sections, with twelve high-level requirements that govern network security, data protection, access control, access monitoring and many more. Some measures put in place to ensure efficient data protection include

- The maintenance of minimum data storage on cardholders with the necessary data retention and disposal policies.
- No storage of sensitive authentication data after payment authorization.
- Masking of the primary account number when displayed.
- Using methods such as truncation and encryption to make unreadable the primary

account number.

- The protection of cryptographic keys used for encryption of the cardholder information.
- There should be documentation of the key-management processes and procedures for cryptographic keys used for encryption of the user's data.

2.6 Mobile Financial Services in Ghana.

The inhabitants of rural areas in Ghana remains unserved or underserved by financial institutions because of the low balances and transaction sizes that yield little revenue for banks. Consequently, financial institutions find it unfeasible to profitably serve the poor in developing countries (Kendall, 2010). Due to increased usage of mobile phones and the growth in mobile networks, there has been a paradigm shift in financial services for the poor in Ghana.

Mobile Financial Services is a relatively new development in Ghana. It was first introduced into the country by MTN Ghana in July 2009 and then followed by Zain (now Airtel) in March 2010 (Saliu, 2015). Tigo also introduced Tigo Cash in October of the same year and in July 2015, Vodafone joined the market. The patronage of these services has been on an ascending order. The value of transactions has increased from GHS2.4billion as at 2013 to about GHS11.6billion in 2014.

Over the years, there has been an increase in the number of mobile financial service providers across Ghana. It was first introduced by telecommunication networks but now, we have software engineering companies venturing into that market. The following are short descriptions of some of the mobile financial services in Ghana:

2.6.1 Slydepay

Slydepay started as iWallet and was created by DreamOval as an online payment solution that allowed customers to make purchases electronically. This financial service

provides its customers with access to over 10,000 goods and services from merchants and partners such as Palace Shopping Centre, Compu-Ghana, Ghana FX, Ghana Shoppers, Soronko Solutions and many others. It also allows its users to easily monitor their finances by giving them a visual representation of their money story. Slydepay enables users to pay for goods and services by scanning QR codes with Slydepay Mobile app or just entering a payment code.

Slydepay also provide special offers for businesses or merchants. It allows customers to make payment to merchants via whichever electronic means they wish and track it for the business. For businesses who would like to collect electronic payment at the business centre, Slydepay allows them to collect cashless payments at the POS with a tap of a button on the mobile app. This service implements the mobile payment as the POS model.

2.6.2 MTN Mobile Money

MTN mobile money is a fast, affordable and convenient means of transferring money, making payment for goods and services and performing other transactions via a mobile phone. This service is offered by MTN in partnership with over ten banks in Ghana. This service allows its customers to top up MTN airtime, pay bills such as DStv, ECG Post-paid, School fees and many more. Users can also pay for insurance, employees' salaries and purchase for airline tickets. This service employs a mobile payment platform model.

2.6.3 Vodafone Cash

Vodafone cash is a simple and secure service that permits its users to transfer money and make payment using a mobile phone. It can also be used to buy Vodafone Airtime, pay Vodafone bills as well as pay for other goods and services. In order to make deposits, the user has to visit a Vodafone Retail Shop or a cash agent. This service does not allow users to make transfers from their bank account to their Vodafone cash account. This services employs the mobile payment at the point of sale model since users are allowed to pay for goods and services via the mobile service.

Chapter 3: Methodology

3.1 Introduction

In this chapter, we are going to discuss the processes and tools that will be used to answer the research questions stated in the first chapter. It includes a description of the sampling process, that is how the respondents were selected and the sampling process that was used. It also discusses the sources of information that was used in the study, the tools that will be used to collect the information and the major parties that will be involved. Finally, it will describe the methods of analysing the data and how reliable or viable this is.

3.2 Research Purpose

A research purpose seeks to answer the question "why the study is being done". That is the goal of the research or what the researcher aims to discover at the end of the study. The major categories of research purpose include: exploratory purpose, which is done to examine a new field or a subject of study where little or no work has been done on; description purpose, which involves observing and describing the behaviour of a subject without affecting it in any way; and explanatory purpose which is done to explain a situation or problem and the relationship among its variables (Saunders et al., 2009).

3.3 Research Approach

There exist different approaches to conducting a research, but before deciding on an approach or method to use, the following factors must be considered. They include the study base, the study timeline, the qualitative or quantitative approach to be used and inductive or deductive research approach to be used.

The Study base is the source population or study group that the research focuses on. The study base may either be broad or narrow depending on the research question that is being answered. The selection of the respondents may also differ if the research requires a cross-sectional design, which compares two different base groups. The timeline of a research may include the period of time you collect data. This may be historical or prospective, which means

it is happening in the foreseeable future. Another factor to consider when conducting a research is whether it requires an inductive or deductive approach. This usually requires the building and testing of theories.

For this project, the study base used include mobile money service providers in the capital of Ghana. This research paper made use of information from what is currently happening in the mobile ecosystem and was a short term study. The research design that was employed in this study is the qualitative approach since the study seeks to examine the experiences and various activities that concern the security structures of mobile payment systems. This study also reviewed some existing security models that have been employed by international service providers to find out which of them best suits the Ghanaian mobile money ecosystem, thus it used the deductive approach.

3.4 Research Strategy

A research strategy includes clear objectives which are obtained from the research questions, to specify the basis on which data will be gathered, limitations associated with the research which may include time, money, data and access, location and other ethical issues (Thornil et al. 2003). This research paper implemented the observation method, interviews, case studies and secondary data.

A case study is a method employed in a research, involving an empirical analysis of an event that exists within the field of a situation in real life by searching for evidence (Robson, 2002). A case study allows a researcher to examine data within a specific context. Case studies are mostly used when the researcher aims to broaden his understanding of the topic. For this project, the case studies involved analysing three international service providers, examining their systems and security measures implemented in their systems. The author then compared the international measures with the measures being implemented in Ghana to suggest ways to improve our local techniques.

The second set of tools used to gather information include interviews. Interviews are a systematic way of talking and listening to people and are another way to collect data from individuals through conversations. In this type of interview, the interviewer used open-ended questions to collect information as well as gain knowledge from individuals. Interviews are also means by which researchers exchange views with two or more people on a topic of mutual interest to gain broader understanding of the topic. The three reasons why interviews will be used in this study includes the need to attain highly personalized data, its opportunity to probe and a good return rate as compared to sending out questionnaires. There are four types of interviews—structured, semi-structured, unstructured and non-directive. For the purpose of this research, the semi-structured approach was used. In a semi-structured interview, the order in which the various questions or topics are dealt with are left to the interviewer's discretion. He or she is allowed to conduct the conversation as he thinks fit, ask the questions he deems appropriate in the words he considers best, to give explanation and seek clarification if the answer is not clear, to prompt the respondent to elucidate further if necessary (Corbetta, 2003). Lastly, data was gathered from existing research papers related to this topic.

3.5 Research Design

Research design is defined as the procedure(s) for collecting, analysing, interpreting and reporting data in a research study (Creswell & Plano Clark, 2007). It is also defined as the blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings (Burns & Grove, 2003). Research can be divided into various groups based on the purpose and method that will be used. These categories include explanatory, descriptive and exploratory research (Ghauri & Grounhaug, 2002). Explorative research can further be divided into quantitative or qualitative or conclusive design which constitutes descriptive or casual research.

Explorative research is a form of research done to explore the research questions and does not intend to offer final and conclusive solutions to the existing problems (Dudovskiy,

2016). This type of research is done to have a better understanding of the problem. The sole aim is to discover the research topic at varying levels of depth. In this project, the explorative research approach is going to form the basis of the research design.

Conclusive Research design is one that is applied to generate findings that are practically useful in reaching conclusions or decision-making. This research required some exploration into the mobile payment service ecosystem to be able to understand how the system works, the roles of each player, the security system and detect if there are any challenges. Conclusions were drawn on the information that was gained.

3.6 Research of the Study

In the context of the above discussions, this research will be employing a qualitative research approach. It made use of qualitative interviews through face-to-face medium for exploratory purposes. It followed up with analysing international systems as case studies. The study also included the examination of techniques used by some local companies. In the literature review study, some proposed solutions to the threats of mobile payment systems were discussed. With knowledge of how the system works, analysis was done to find out if these methods can be implemented local companies and further recommendations were made in the results and findings.

Information was also gained through observation. With this, the researcher tested a few of the mobile payment platforms, watched other agents and users perform transactions to gain more insights on how the ecosystem functions in reality. The mobile payment platform that were used include MTN Mobile Money and Slydepay.

These tools and methods were selected to be used as the research design because of the exploratory nature of the project. The research involved the analysis and examination of a situation or problem at a point in time. The research problem was formulated based on current theories and its main goal was to create more knowledge about the topic. For this reason, a

deductive approach was adopted in this thesis. The project included the testing of some of the proposed security systems by scholars to see if it suited the kind of mobile payment systems being run in the country.

3.7 Population of the Study

A population or universe of investigation may be considered as the total number of units of the phenomena to be investigated that exist in the area of investigation, which is all possible observations of the same kind that a sample is acquired from (Kumekpor, 2002) (Bryman & Bell, 2007). The study was done using the mobile service providers in the Accra metropolis because it is the commercial capital city of Ghana. It also contains almost all the headquarters of the Mobile Payment Service Providers such as MTN Mobile Money, Slydepay, Express Pay, MPower Payment, iPay, Vodafone Cash, Airtel money and many others. The research will focus only on Ghanaians and Ghana-based mobile payment service providers.

3.8 Selection of respondents for the Interviews

Sampling is the process of observing a section of the population in order to gather information about the whole population (Cobetta, 2003). Sampling was done to save time and money since all the players of the MP ecosystem in Ghana cannot be studied for this research. This will be impossible to accomplish within the time constraints and with the limited financial resources which are available for the research.

This research focused on the components of the mobile financial service ecosystem in Accra. Since the interviews held were very in-depth, a very small sample size was used. The sample was selected using a non-probability sampling procedure. The research made use of convenience and purposive sampling. Convenience sampling involves the use of the readily accessible persons at the time of the study while the purposive sampling involves selecting cases based on the researcher's judgement. The respondents for the interview were selected based on individuals available during the time of the interview thus it made use of convenience sampling.

3.9 Data collection method

Data collection is an essential part of the research. According to Tashakkori and Teddie (2003), data collection is used when trying to derive data that will be used for making decisions and keeping records. This can be done through the use of interviews, questionnaires and observation.

Data was collected from mobile networks operator—MTN. The interviews were done by setting up meetings with employees from the mobile network operators(MTN), mobile payment service provider(Slydepay) and acquirer and issuer (Zenith Bank). Also academic journals from the website of Institute of Electrical and Electronic Engineers(IEEE) and publications from Organisations including the World Bank, PricewaterhouseCoopers Limited, Apple Incorporations, Google and others.

3.10 Method of Data Analysis and Presentation

Data analysis involves gathering, summing and collating the collected data with the results reflecting important aspects relating to the topic under study (Saunders et al, 2009). After all the data has been collected, it has to be analysed and interpreted to be able to draw conclusions.

The data collection required a combination of multiple methods. The data collected was analysed using framework analysis. This was done by examining my findings with pre-defined frameworks which share similar aims, objectives and interest as those of my research. This included the security systems proposed by scholars and the security measures being used by some of the mobile financial service providers.

The second approach that will be used is thematic network analysis. This takes a more exploratory perspective since it makes use of all the data gathered, allowing for new impressions to shape the interpretation in different and unexpected directions.

Chapter 4: Analysis and Findings

4.1 Case Studies

4.1.1 Apple Pay

Apple pay is a mobile payment service that can be accessed on only iOS devices including the Apple Watch. It allows the user to make payments with merchants who have implemented point of sales that support Apple pay contactless payments. It places a lot of emphasis on the protection of their customers' information. Apple pay employs a number of existing security technologies and security controls which involves users commencing payments and authorizing payment transactions between users, merchants and card issuers. (ENISA, 2016).

4.1.1.1 User Authentication:

In order to perform a payment using Apple pay, the user is required to authenticate the device. The authentication process involves the use of the user's fingerprint or the PIN number when using an Apple Watch. The goal of the security control is to limit what an attacker can do with a stolen device. The use of fingerprint identification or authentication is done to improve upon the traditional contactless payment where a stolen card could be used without any user identification/authentication.

4.1.1.2 Device Authentication:

When a transaction is completed on the Apple pay system, it generates a unique value that ensures that the transaction is coming from an authorized device. This unique value, token and cryptogram used to authorize the transaction, ensures that even if the token is stolen it cannot be used from another device because the token can only be used on the device it was generated from. Also the token is calculated with the unique amount of every transaction, hence even if it is intercepted in transit, it cannot be used by an attacker to perform another purchase.

4.1.1.3 How Apple Pay uses the NFC controller

The Secure Element in the Apple pay system has an NFC controller that ensures all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Contactless transactions are payment requirements which are sent from an in-field terminal marked by the NFC controller.

A payment is authorized by the cardholder using the Touch ID or passcode or double –clicking the side-button for those using Apple watch. When this is done, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. The payment authorization details for contactless transactions are limited to only the local NFC field and are never made visible to the application processor for security purposes. On the other hand, payment details for payments within apps are routed to the application processor after encryption by the Secure Element to the Apple Pay server. (iOS Security, 2016).

4.1.2 Google Wallet/Android pay.

Android pay is a free application on the Android platform. It is a fast and free way to send money through the application in Gmail or the web at wallet.google.com. It can also be used as a Google Prepaid Card or to store Citi Master cards. This technology can be used at PayPass terminals. Money can be sent to people by just entering their phone numbers or email addresses. This technology can be used at PayPass terminals. During such transactions, information is exchanged between the user's phone and the terminal wirelessly using Near Field Communications Technology. NFC transfers information over short distances and does not require the use of the mobile data plan of the phone. A digital receipt is displayed on the screen of the phone at the end of the transaction.

4.1.2.1 User Authentication

Android Pay uses multiple options to authenticate its users before a transaction is completed. These include fingerprint authentication, PIN code, password or pattern to authenticate a transaction.

4.1.2.2 Device Authentication

Android Pay assigns a virtual account number known as a token to every Android pay account, that will link the actual card number to the mobile account. The payment tokens are loaded on the device in advance before the payment. They are periodically recovered from Google servers when the device is connected to the internet. The token is unique to the card number it represents and does not change. The app user's mobile device keeps an encryption key in memory that it uses to decrypt limited-use and single-use keys for contactless transactions.

4.1.2.3 Data Protection

The Home Card Emulation (HCE) assumes that any data stored on a handset is vulnerable to any form of cyber-attack for example when the device is stolen or affected by malware. Due to this, it stores the card sensitive data on databases hosted in a secure cloud environment.

HCE uses the following four security measures to prevent unauthorized access. They include limited use security keys, tokenization, device fingerprinting and transaction risk analysis. The limited security keys used are set to expire quickly preventing their misuse. The use of tokens also helps to reduce risk by replacing the primary account number (PAN) with a limited use data that passes seamlessly through the payment system. Device fingerprinting validates the phone and transaction risk analysis provides real-time transaction assessment to identify unusual activity.

4.1.2.4 Further Security Checks.

The PayPass encryption technology transfers and reads the data during transactions. This encryption technology scrambles the data sent using an algorithm, which is then un-scrambled by the PayPass terminal. A third party who tries to access data in between will only get a file with jumbled letters or symbols which would not make any sense.

Under fraud protection, Google employs advanced risk modelling to detect fraudulent signals across Google services. Fraudulent transactions are terminated immediately they are

detected. Also, any other active transaction associated with the fraudulent credit card will be cancelled to protect the user.

4.1.3 M-pesa

M-pesa is mobile device based money transfer service that was launched in 2007 by Vodafone for Safaricom and Vodacom. It also offers financing and microfinancing services. It is currently being used in Kenya, Tanzania, Afghanistan, South Africa, India among others. M-pesa permits its users to deposit, withdraw, transfer money and pay for goods and service using a mobile device.

M-pesa is regulated by Kenyan national regulators and some international regulators such as the UK's Financial Conduct Authority(FCA) and the Payment Card Industry (PCI) to understand how to best protect client information and adhere to internationally recognized best practices.

4.1.3.1 User Authentication

In the registration process, M-pesa system ensures that the user is a Vodafone customer and registration is only done at authorized M-pesa stores by M-pesa agents. During the activation process, a customer receives a 4 digit start key randomly generated by the M-pesa system. This ensures that only the rightful owner of the account who has submitted the KYC documents activates M-pesa on his handset. Another security measure that is employed by the M-pesa system is allowing the user to create his own 4-digit numeric PIN of his choice. The PIN is confidential and only remains with the owner of the M-pesa account. During any transaction on the system, the PIN serves as the verification mechanism. In order to check the authenticity of the user, the application gets locked in a case where five incorrect PINs are entered consecutively. Lastly, the system sends an instantaneous SMS to the user when a transaction is done to further ensure high safety and security standards.

Using GSM as a transmission medium, M-Pesa sends, store and forwards SMS messages to parties of a transaction. The STK application installed on the phone by Safaricom provides the command and functionality for the above processes to run.

4.1.3.2 Further Security Checks

M-pesa sends confirmation messages to its users when he or she withdraws money from an agent. The user shows this message to the mentioned agent before he is given his money. The agent also receives a similar message. During a deposit, the customer is expected to handover the cash to the agent first before the transaction process is begun. This is done to prevent the customer from failing to hand over the cash at the end of the transaction.

M-pesa maintains a prompt response with its customers during a transaction. When a user makes a withdrawal from a certain agent. He receives a prompt stating the user's name, amount and name of the agent. This prevents customers from withdrawing money from a wrong agent and vice versa. The customer keys in an agent's number when withdrawing, which when misread may cause the transaction to be sent to another agent.

4.2 Interview Analysis and Discussion

After a thorough study of some mobile payment system outside Ghana, in-depth interviews were held with three major key players in the mobile payment service market in Ghana. They include MTN mobile money, Slydepay Ghana and Zenith Bank. The purpose of these interviews was to gain understanding of how mobile payment services work in Ghana and the roles these organisations play in the ecosystem. There were six questions asked during each interview but the table below focuses on the main aspects that are relevant to this study. The interview was structured into sections including the type of services offered by the company, local and international standards guiding the design of the service and security controls and measures that are been being put in place. The questions asked were standard open-ended questions. It also included some comparison of local methods with international ones.

The table below summaries the information that was gathered from the interviews held with the mobile service providers—MTN mobile money and Slydepay.

	MTN Mobile money	Slydepay Ghana
Types of services offered	Mobile/ Digital wallet	Mobile/ Digital wallet and Transfer account
Local and international standards used	ISO/IEC 27001- is a standard that specifies the requirement for establishing, implementing, maintaining and improving an information security management system such as Mobile payment systems.	PCI/DSS- an information security standard for institutions that handle credit card information (e.g. Visa card)
Security measures implemented in the system	1. Control access right- to protect customer information 2. Segregation of duties to reduce error or fraud on high risk procedures (e-money reconciliations). 3. Threshold limits- this helps to reduce the risk associated with Anti-Money Laundering and counter financing of terrorism.	1. Two set authentication- involving the use of a secret code created by the user and the last three digits on the credit or debit card of the user. 2. The use of passwords
Detective Controls for fraudulent attacks	1. Monitor agent transaction activity. 2. Monitor and analyse suspicious activities 3. Sending SMS alert to customers	Log entry trigger- this sends an alarm to the operator when an account is being tampered with by the wrong user.

4.3 Analysis of Data

4.3.1 Potential risks for Mobile Payments: Threats and Vulnerabilities

Over the years, the various players in the mobile financial services ecosystem have suffered a number of threats. The diagram below shows some threats and attack vectors on the components of the ecosystem. The components include mobile payment providers, card issuers, acquirers, merchants and cardholders.

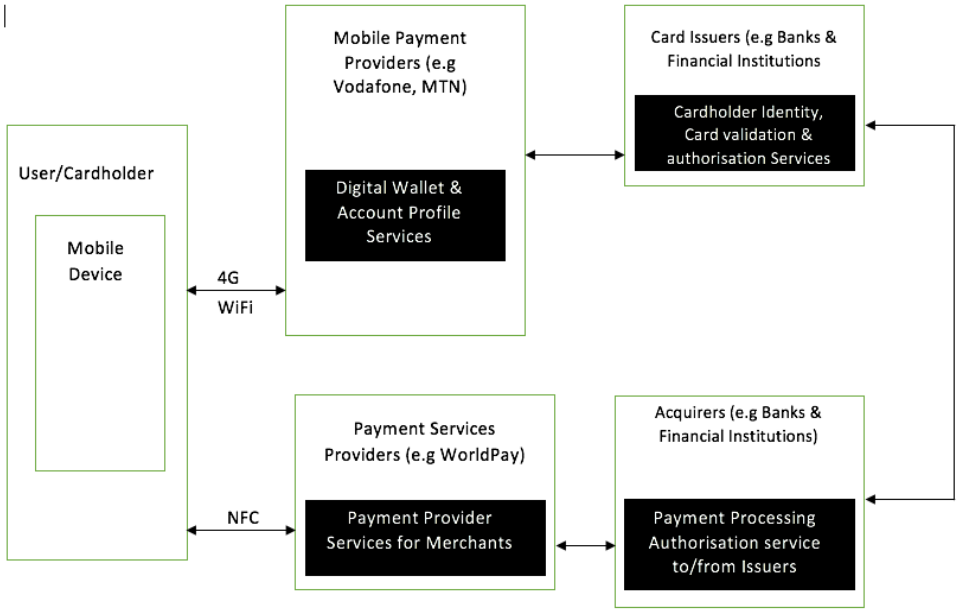


Figure 4.0

4.3.1.1 Mobile Payment Application Users Threats

The following are the major threats that users of Mobile Financial Services may face.

- **Phishing and social engineering**

A phishing attack is a form of hacking where the attacker tricks the victim into entering his personal information into a fake page which looks like a real login page of the actual website. Mobile phones contain the information of its users, they are usually used to store very critical data. These devices are also used to access information on various

platforms including the internet. The attackers target the users by phishing emails and social engineering exploiting different communication channels (such as phone, email, SMS etc) and data about the user available in the public domain (for example social media sites, search engines and the like). Some examples of information that phishers look for include credit/debit card details and personal data that the user knows about. Also stolen credit/debit cards can be sold in underground market forums or used for fraudulent payments. Lastly, personal information about the user such as name, date of birth, contact details—billing, shipping address, emails and phone numbers can be used for impersonation attacks and for identity theft.

- **Installation of fraud applications and malware**

Another technique used by fraudsters to steal personal information of mobile financial service users is by installing malware on the mobile device through phishing or social engineering. This occurs when a victim opens a malicious attachment in an email and that redirects the user to a menacing URL.

Users may also come into contact with malware infection when they access insecure Wi-Fi hotspots for example free Wi-Fi at internet cafes. There is also the possibility of a network spoofing attack. This occurs when a malicious user creates a fake access point with the same details as an already existing one. They go on to set up a fake website to "authenticate" users and use this means to collect their personal information.

4.3.1.2 Mobile Device Threats

The following are the major threats to mobile devices

- **Access to lost or stolen mobile devices.**

A user may lose his or her mobile device through theft or by misplacing the device.

When such device gets into the hands of fraudsters or malicious users, they can be used to the owner's disadvantage. The attacker may try to access the information stored on the device, by finding ways to bypass any PIN or fingerprint locks. The attacker can unlock a device protected by fingerprint authentication using fingerprints stolen from other sources of fingerprint data. For example, lifting latent fingerprints from surfaces. Other methods used by phishers to unlock stolen devices is by using commercial or open source forensics tools to break the device operating system to gain root access to the file system stealing data installed on the device.

4.3.1.3 Threats to the Mobile Payment Application

- **Tampering with the mobile payment application**

One of the major threats that mobile payment applications face is getting attacked by cyber attackers. The attackers find a backdoor entrance into the mobile payment application to capture the login details and forward them to an attacker controlled server. The attackers may download legitimate application from the app store, edit its source code, repackage and upload it back online.

They can also do this by accessing the source code, get access to all the assets hidden in the application such as tokens and cryptographic data. In such cases, the reliability of the application is compromised since the data storage has been corrupted.

Another device in the mobile payment ecosystem that is vulnerable to attack is the merchant's mobile POS. A fraudulent merchant can also access sensitive data such as users' card details, card verification method values and others by tampering with the mobile application.

- **Exploitation of mobile application vulnerabilities**

Cyber attackers may take advantages of the weak authentication system of some application to gain unauthorized access to the device. Through exploitation of mobile payment APIs used in app purchases, attackers can gain unauthorized access to mobile payment functionality. Additionally, fraudulent transactions can be done with stolen bank and credit card accounts linked to the mobile application. A fraudster might take advantage of any loop holes in the registration process to add another mobile device to the user's profile to make fraudulent transactions.

- **Installation of rootkits/malware**

Rootkits are a type of Trojan horse program which when installed on a victim's device or system changes the operating system of the attacked device such that the evidence of the attackers' activities are hidden from the user and attackers can get root access to the system. (Schultz, 2017). In mobile payment services, the existence of rootkits on mobile devices can be used to manipulate API calls collected to or from mobile payment API endpoint. This may result in manipulation of variables during a transaction, for example payment amounts.

4.3.1.4 Threats to Mobile Payment Service Providers

- **Manipulation of payment systems.**

The payment service provider offers point of sale(POS) contactless terminals for mobile payments (such as NFC enabled POS terminals), combined payment services for merchants by processing information from different channels consisting of person to person payment, online payments and mobile payments. The aim of most fraudsters who attack the payment service providers' channels is to corrupt the payment data in transit from the

merchants' point to their affiliated bank. Attackers seek to detect loopholes in the POS terminals that are used for transactions by the merchants. They also corrupt software vulnerabilities of POS servers' software installed on the merchant's POS server. By doing this, they are able to manipulate payment gateways and exploit weaknesses in enforcement of internal payment service providers' security measures.

- **Man-in-the-middle attack(MiTM)**

A man-in-the-middle attack is a type of cyberattack which involves a fraudulent person inserting him or herself into a conversation between two parties, imitates both parties and gains access to information which is being exchanged between the two parties. It is basically about a third party getting access to some sensitive information. (DuPaul, 2017). Attackers try to take advantages of insecure connections to conduct attacks such as MiTM to collect sensitive data in transit from merchant payment systems to the gateway point hosted by the payment service provider and from the Payment service provider to its affiliated financial institutions.

4.3.1.5 Threats to Acquirers

- **Corrupted payment processing systems**

During mobile financial service transaction, acquirers send authorization requests via tokens or cryptograms and receive authorizations from the issuer through the payment network. Due to this, payment processing services are possible targets by attackers seeking to collect large amounts of cardholder data. Attackers may hack into the acquirer bank payment processing server from the inside of the network by manipulating unauthorised access to payment gateways. They may also take advantage of weaknesses in implementation of internal security controls installed in the system.

- **Corruption of data connections**

Attackers may detect vulnerabilities in the point to point connection between the acquirer and issuer. With this knowledge, they may conduct attacks such as MiTM to gather sensitive information during a transaction between the acquirer and issuer via the payment network.

4.3.1.6 Threats to Issuers

- **Corruption of confidential cardholder's information**

The servers of banks or other financial institutions store the confidential information such as credit and debit card account details about their customers. Due to this, they may be the target of cybercriminals who aim at stealing this information for fraudulent activities. This may be difficult to attain due to the high security controls implemented on the issuers' servers and systems. Other techniques used by cybercriminals to access such information is through social engineering and Advanced Persistent Threats (APT)(which will be explained later in this chapter).

Social engineering is a non-technical approach used by cybercriminals to trick people into breaking standard security policies through human interaction. Social engineering techniques helps to manipulate its victims into executing certain actions that goes against the organisation's rules. (Lord, 2017). Internal employees of financial institutions who have access to the databases can act as social engineers by getting user information as well a second factor authentication to access the issuer's system.

An Advanced Persistent Threat is an attack where an unauthorised user gets access to view and also make changes to the data on an organisation's system or network within a long period of time without being noticed. The goal of advanced persistent threats is to steal data

not destroy the system. (Lord, 2017). APT usually installs a malware on the server of the target institution. This will help decrypt databases to obtain the plaintext format of the cardholders' information.

Chapter 5: Conclusion and Recommendation

5.1 Introduction

The purpose of the concluding chapter, is to give a recap of the purpose of the research, the tools that were used, the research findings, implications and direction for future study. The chapter also highlights some significant lessons from the study gained by the author and makes some recommendations for stakeholders.

5.2 Summary of the study

This research paper investigated the mobile financial service market globally and locally. It studied the factors that led to its growth, some of the benefits it has given its customers, operators and the general public. It focused on the security controls and measures that are put in place when designing these services. The research established that the services were prone to several fraud cases in Africa and beyond. That led to the main purpose of the research which is to understand the ecosystem of mobile financial services in Ghana, study the security controls implemented and propose measures to make these services safer for customers and businesses.

In order to answer the research questions outlined in chapter one, the author of this paper reviewed existing literature on mobile financial services in Ghana and beyond. The study also reviewed some literature on the major players in the mobile financial services, the threats that these services face and some of the proposed solutions by scholars. To better address the mentioned questions, the study involved the gathering of primary data through interviews and observation and secondary data through further research into journals and publications. In-depth interviews were held with the top two mobile financial services providers in Ghana—MTN mobile money and Slydepay Ghana. Also an employee from Zenith Bank one of the major banks that serve as an acquirer and issuer to most of the agents was interviewed to gain insight into the role financial institutions play in the Ghanaian mobile financial service ecosystem. This interview also highlighted some security controls that are put in place from the acquirer and issuers of credit and debit card. The research also

made use of case studies. A thorough study of Apple Pay, Android Pay and M-pesa was done. This broadened the author's knowledge on the practices that mobile financial service providers use internationally. Reviewing their security systems helped to answer some of the research questions mentioned above. Lastly, secondary data was gathered from organisations such as the World Bank, European Union Agency for Network and Information Security, GSM association and other academic papers.

This mobile financial service ecosystem consists of several players, but this study focused mainly on the mobile service providers, acquirers, issuers and users. After analysing the data gathered, the author highlighted the major threats that the mentioned players may face. Finally, it aims to suggest some measures that can be implemented locally and globally to help prevent the stated threats.

5.3 Major Findings

Findings from the study answered the research questions that were proposed in the of this paper. The key players in every mobile financial service transaction include the customers, agents/ merchants, affiliated banks or financial institutions, mobile financial service provider and mobile service application providers. After explaining the various roles of the players in the ecosystem, the study highlighted some threats that affect some of the players. These include the following:

- The corruption of payment data during a transaction and Man-in-the-Middle attacks, which involves fraudulent people acting as middle men to collect sensitive information during a transaction.
- Compromise of payment processing systems and corruption of data connections. Attackers take advantage of flaws in the security systems of financial institutions, and steal sensitive data during the transfer of data from one server to another on the network.

- Issuers faced the threat of the cardholders' information being corrupted or stolen by cyber criminals. This is usually done through social engineering and advanced persistent threats.
- The designers of the application used by the customers are also at risk. Some of the major risks they may face include fraudsters accessing the source code and corrupting the storage system such that the storage of user's information is compromised. There could also be the installation of malware on the mobile device which will affect the functionality of the application, leading to loss of sensitive data during a transaction.
- Lastly, the customers may face the risk of being attacked by phishers and social engineers. Attackers may also take advantage of weak authentication systems to gain unauthorised access to the user's information and mobile payment application.

The review also highlighted two proposed solutions to the threats that the players of mobile financial service may face as evidence from the literature review. They include Secure and Efficient Protocol for Mobile Payment (SEMOPS) and Near-Field Communication (NFC) based secure mobile payment service. SEMOPS seeks to improve the security of mobile payment service by the use of PIN authorisation and also uses a timer to check atomicity of individual transactions. The NFC based solution seeks to offer a more secure platform by providing the necessary data protection controls. It was built based on the Payment Card Industry(PCI) Data Security Standard(DSS).

Also after the analysis of the data gathered, some suggested solutions that may help reduce the risk that the players in the Ghanaian mobile payment system face include the following:

Mobile Payment Component	Threats	Possible Mitigation methods
Customers	1.Phishing and social engineering 2.Installation of fraud applications and malware	1. Customer authentication should be enforced by the use of biometric controls or strong PINs or patterns. 2. Perform transactions on only trusted networks (such as Wi-Fi hotspots) 3.Update the operating system of the device regularly to help improve the security controls.
Phone	Man-in-the-middle attacks	Encryption of SMS messages using strong asymmetric or symmetric algorithms.
Mobile payment application	1.Tampering of application source code 2.Malware on the device attacking the application	1.Avoid hard-coding sensitive information such as passwords or keys. 2.Implementing effective certificate pinning to check that the application is collecting data from the right source. 3.Verification of the running code to ensure that it has not been corrupted.
Mobile payment service providers	1.Manipulation of Point of sale devices. This may include the compromise of software running on the terminals or installed on the Point of sale servers. 2.Data connectivity (Vulnerable connections between the agent's server and payment service provider. Also insecure connections between payment service provider and acquirers	1.Frequent vulnerability testing, ensuring the default design is highly secured. Regular repair of software vulnerabilities in POI and payment gateways hosted at the payment service providers. 2.Enforce secured point to point connections and encryption of data during transaction.

Acquirers	1.Corruption of data processing systems 2.Insecure external and internal system connections 3. Malware Infection	1.Financial Institutions should acquire systems which enforce high security standard and makes use of two factor authentication for user access. Also these systems should enforce limited privileges for user access. 2. Improve point to point connection by the implementation of SSL/mutual connection. 3. Enforce malware detection measures, data leakage and fraud prevention.

5.4 Implication of The Study and Further Research

In Ghana, there is a rapid growth in the use of mobile financial services. This is being reported in our daily news. Currently, there are some academic paper on what this service is about, how it works, the benefits and menaces but there seems to be little academic work done on the security of these services. Also there are a few documentations on the roles that the individual components of the mobile financial service ecosystem play as well as what functionalities and processes are involved in our local services.

This current study contributes to the literature review on the Ghanaian mobile financial services and relationship with global development. Also the study reviews some of the security threats that are dominating the mobile financial services space globally and relates this to the Ghanaian system. The study also educates the users on some of the possible risks they may face and suggests measures that can be implemented to moderate if not prevent these dangers.

This study can be used as a guide by new investors or businesses in terms of understanding of the Ghanaian mobile money ecosystem, enabling them to design products or

services that better suit the needs and meets the required security standards for their customers.

Lastly, this study adopted a qualitative research approach which involved collecting data through in-depth interviews and the use of secondary data. Thus, further research may yield similar or slightly different results depending on the changes or influence of the conditions at a particular time. Further research could make use of control variables such as demographics as a moderating factor.

5.5 Research Limitations and Practical Challenges

The components of a typical mobile financial service ecosystem consist of about ten players. This study gathered its data by interviewing three players in Ghana's ecosystem due to the limited time constraints. Also the case studies used for this project included only one service provider from Africa. In the light of this, this study may not address all the risk that users of these services may face in Ghana. The scope of the study was limited geographically and numerically in terms of sample size.

Irrespective of these inadequacies, the conclusions drawn by this study are deemed appropriate.

References

About Mobile Money. (2014). Retrieved from http://www.mtn.com.gh/personal/mobile-money/about-mobile-money.

Adjorlolo, R. A. (2015). Ghana outranks Kenya, Tanzania in World Bank-CGAP report on digital financial inclusion. *Ghana Broadcasting Corporation.* Retrieved from http://gbcghana.com/1.8496974.

Apple Inc. (2016, May). iOS Security, iOS 9.3 or later. Retrieved from https://images.apple.com/ca/business/docs/iOS_Security_Guide.pdf.

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative research*, *1*(3), 385-405.

Corbetta, P. (2003). *Social research: Theory, methods and techniques*. Sage.

Dudovskiy, J. (2016). Exploratory Research. *Research Methodology*. Elliott, Robert, Constance T. Fischer, and David L. Rennie. "Evolving guidelines for publication of qualitative research studies in psychology and related fields." *British journal of clinical psychology* 38.3 (1999): 215-229. Retrieved from http://research-methodology.net/research-methodology/research-design/exploratory-research.

DuPaul, N. (2017). *Man in the Middle (MITM) Attack*. Retrieved from https://www.veracode.com/security/man-middle-attack.

Elliott, Robert, Constance T. Fischer, and David L. Rennie. "Evolving guidelines for publication of qualitative research studies in psychology and related fields." *British journal of clinical psychology* 38.3 (1999): 215-229.

European Union Agency for Networks and Information Security. (2016, December). *Security*

of Mobile Payments and Digital Wallets. Retrieved from https://www.enisa.europa.eu/publications/mobile-payments-security.

Firpo, J. (2009, January 21). E-Money – Mobile Money – Mobile Banking – What's the Difference? Retrieved from http://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference.

Godbole, R. M., & Pais, A. R. (2008, August). Secure and efficient protocol for mobile payments. In *Proceedings of the 10th international conference on Electronic commerce* (p. 25). ACM.

Google.com. (2017). *Google Wallet*. Retrieved from https://www.google.com/wallet/

ISO.org. (2017). *ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements*. Retrieved from https://www.iso.org/standard/54534.html.

Javelin Strategy & Research (2009, September). The State of Mobile Security in Banking and Financial Transactions. Retrieved from http://www.bankinfosecurity.com/whitepapers/state-mobile-security-in-banking-financial-transactions-w-293.

Kane, J. (2016). *Factors to consider when choosing a research design.* Retrieved form http://www.ehow.com/info_7844111_factors-consider-choosing-research-design.html.

Kaya, M. M. (2013). *Trust and Security Risks in Mobile Banking* (Doctoral dissertation, University of Oxford).

Kenya tops list of banked population due to high mobile money uptake. (2015, April 25). *The EastAfrican.* Retrieved from http://www.theeastafrican.co.ke/business/Kenya-tops-list-of-banked-population/2560-2697138-jh9o4iz/index.html.

Kendal, J., Maurer, B., Machoka, P., & Veniard, C. (2011). An emerging platform: From money transfer system to mobile money ecosystem. *Innovations: Technology, Governance, Globalization, 6(*4), 49-64. Kshetri, N. & Acharya, S (2012). Mobile Payments in Emerging Markets. *IEEE Xplore*. Retrieved http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6248655.

Kshetri, N. & Acharya, S (2012). Mobile Payments in Emerging Markets. *IEEE Xplore*. Retrieved http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6248655.

Lord, N. (2017, January 26). *What is Social Engineering? Defining and Avoiding Common Social Engineering Threats*. Digital Guardian. Received from https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

Lord, N. (2017, January 26). *What is an Advanced Persistent Threat? APT Definition*. Digital Guardian. Retrieved from https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition.

Malakata, M. (2013, December 2). *Kenya, bracing for $23 million in online fraud, to support African cybercrime pact*. PC Advisor. Retrieved from

http://www.pcadvisor.co.uk/news/security/kenya-bracing-for-23-million-in-online-fraud-to-support-african-cybercrime-pact-3491847.

Martyn Shuttleworth (2008). Descriptive Research Design.[Weblog post] Retrieved from https://explorable.com/descriptive-research-design.

Google (2017). *Merchant fraud protection.* Retrieved from https://support.google.com/payments/merchant/answer/7159352?hl=en.

Mudiri, J. L. (2016). Fraud in Mobile Financial Services. *Microsave*. Retrieved from http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf.

Mutie, J. (2015, November 23). *What does M-pesa use for security for its financial transaction system?* Quora. Retrieved from https://www.quora.com/What-does-M-PESA-use-for-security-for-its-financial-transaction-system.

Nagle, B., & Williams, N. (n.d.). Methodology Brief: Introduction to Focus Groups. *Centre of Assessment, Planning & Accountability.* Retrieved from http://www.mmgconnect.com/projects/userfiles/file/focusgroupbrief.pdf.

Neuman, W. L., & Robson, K. (2012). Basics of social research: Qualitative and quantitative approaches.

Neuman, W. L. (2007). Qualitative and quantitative research designs. *Communication Research Methods: Quantitative and qualitative approaches*, 175-204.

Nyaketcho, D., Lindskog, D. and Ruhl, R. (2017). *STK implementation in sMS banking in M-pesa -Kenya, exploits and feasible solutions*. Retrieved from http://infosec.concordia.ab.ca/files/2013/02/Doreen-Nyaketcho.pdf.

Ogwal, I. H. (2014, August). Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market. *Microsave.* Retrieved from http://blog.microsave.net/survival-of-the-fittest-the-evolution-of-frauds-in-ugandas-mobile-money-market-part-i.

Penttilä, M., Siira, E., & Tihinen, M. (2016). Mobile Payment Ecosystems in Transition. *International Journal of Scientific and Technical Research in Engineering (IJSTRE),* 1(6). Retrieved from http://www.ijstre.com/Publish/092016/371428264.pdf.

Pope, C., Ziebland, S., and Mays, N. (2000). Analysing Qualitative Data. *British Medical Journal*, 320: pp. 114–116 Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117368/pdf/114.pdf.

Sander, C. (2003). Migrant remittances to developing countries– A scoping study overview and introduction to issue for Pro – Peer Financial services. United Kingdom Department for International Development (DFID), London.

Santus, R. (2014, October 23). *Why Apple Pay Is the Most Secure Payment Platform on the Planet*. Mashable. Retrieved from http://mashable.com/2014/10/23/apple-pay-is-more-secure-than-your-credit-and-debit-cards/#wmJsKk7B9uqP.

Schultz, E. (2017). *Rootkits: The Ultimate Malware Threat*. Information System Security. Retrieved from http://www.infosectoday.com/Articles/Rootkits.htm.

Schultz, E. (2017). *Rootkits: The Ultimate Malware Threat*. Infosectoday.com. Retrieved from http://www.infosectoday.com/Articles/Rootkits.htm.

Slydepay-Business. (2016). Retrieved from https://www.slydepay.com.gh/business.html.

Slydepay-Personal. (2016). Retrieved from https://www.slydepay.com.gh/index.html.

Smith, M. & Amprimoz, J. (2012). *Is Google Wallet Safe? Learn What Security Measures Are Being Taken*. *Bright Hub*. Retrieved from http://www.brighthub.com/internet/security-privacy/articles/126261.aspx.

Support.google.com. (2017). *Tokenization - Android Pay Merchant Help*. Retrieved 7 Mar 2017, from https://support.google.com/androidpay/merchant/answer/7151299?hl=en.

Tashakkori, A., & Teddie, C. (2003). *Handbook of Mixed Methods in Social Behavioral Research*. Thousand Oaks CA: Sage Publications, Inc, p. 14, 16.

Zainal, Z. (2007). Case study as a research method. *Jurnal Kemanusiaan*. Retrieved from http://psyking.net/htmlobj-3837/case_study_as_a_research_method.pdf.