EXPLORING SECURITY PERCEPTION OF MOBILE WALLET IN THAILAND

NAREENART KHUMJUANG

A THEMATIC PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF MANAGEMENT COLLEGE OF MANAGEMENT MAHIDOL UNIVERSITY 2017

Thematic paper
entitled

EXPLORING SECURITY PERCEPTION OF MOBILE WALLET IN THAILAND

was submitted to the College of Management, Mahidol University
for the degree of Master of Management
on
December 23, 2017

………………………..…...………......
Miss Nareenart Khumjuang
Candidate

....
Asst. Prof. Peter De Maeyer,
Ph.D.
Advisor

....
Assoc. Prof. Roy Kouwenberg,
Ph.D., CFA
Chairperson

....
Duangporn Arbhasil,
Ph.D.
Dean
College of Management
Mahidol University

....
Ronald Surachai Thesenvitz,
Ph.D.
Committee member

ACKNOWLEDGEMENTS

First of all, I am so thankful for my thematic advisor, Asst. Prof. Peter De Maeyer for his supervision, guidance and support throughout the process of the thematic paper to get it done in the right direction.

I would also like to thank you all 12 respondents for their time and valuable information and willingness to help me conduct this research.

Lastly, I am so grateful for my family, colleagues and friends especially, my parents who always support and encourage for studying in the master of management at the College of Management, Mahidol University.

Nareenart Khumjuang

EXPLORING SECURITYPERCEPTION OF MOBILE WALLET IN THAILAND

NAREENART KHUMJUANG 5949093

M.M. (MARKETING AND MANAGEMENT)

THEMATIC PAPER ADVISORY COMMITTEE: ASST. PROF. PETER DE MAEYER, Ph.D., ASSOC. PROF. ROY KOUWENBERG, Ph.D., RONALD SURACHAI THESENVITZ, Ph.D.

ABSTRACT

The purpose of this study is to explore more what are the consumer perception toward mobile wallet security and what could be best practice for mobile wallet providers do to overcome those security concerns. Hypotheses were tested by in-depth interview and collect data from twelve respondents who are early majority characteristics.

The findings of this research showed that security concern is not considered as high level among this early majority group. In contrast, perceived usefulness becomes the main barrier that deter people from adopting it.

KEY WORDS: Mobile Wallet/ Security Concern/ Early Majority/ Mobile Payment/ Security Features

28 pages

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

CHAPTER I
INTRODUCTION

The research topic of this thematic paper is about consumer security perception of mobile wallet in Thailand. The main focus of the research is in the area of security on doing transaction via mobile device. Less than three decades ago, nobody could ever imagine how life will be if one day we can pay everything through mobile phone. Today, the growth rate of smartphone users has been increasing each year because of the technology and the Internet access. This results in mobile and online payment become more popular and rapidly widespread across the world. Mobile wallet is now an interesting trend that could possibly change the consumer purchase forever. The concept of convenience and ubiquity, mobile wallets are increasingly being used for transactions in mobile commerce. According to the Research and Market, the global mobile wallet market is expected to reach $635 billion by 2020 from $113.5 billion in 2015, increasing at a compound annual growth rate (CAGR) of 41.1% from 2015 to 2020.

Back to Thailand, Thailand is one of developing countries that has a number of smartphone users using mobile transaction at 50% as their daily life and only 17% adopting mobile wallet. However, the market growth likely to change in the future as the number of transactions via mobile wallets is 5 times per month which is higher than mobile banking transaction (Marketbuzzz Research, 2016). However, most of Thai people still are not keen much in using mobile wallet transaction because of security concerns. According to Visa Research (2017), Thai people are afraid of mobile data hacking with 34%, stolen mobile phone as the second rank at 22% and accessing private data without permission at 17%. It is obviously seen that mobile wallet service providers need to overcome this problem and build a trust into consumers in terms of security. Today, mobile wallet service providers see a great opportunity in Asia market that tends to grow in the near future due to an increase in a number of smartphone users. However, security concern is still the main reason that deter Thai people from using mobile wallet.

1.1 Research Questions

- What are consumer’s perception regarding security of mobile wallet?
- What are best practices in terms of security?
- What could mobile service providers do to overcome consumers' security concerns?

1.2 Research Objectives

- To study about the perceptions of Thai consumers regarding security features of mobile wallet
- To explore the safety method and what would Gold Standard security look like for mobile wallet

1.3 Research Scope

In this research, it will be mainly focused on exploring the safety stop for mobile wallet payment. Qualitative methodology will be used for the data collection. It intends to interview 12 respondents who are classified as early majority. The in-depth interview is to be used for understanding current perception of Thai people and to study what are their acceptable levels of the security.

1.4 Expected Benefit

The final report will contain recommendations that can be used for implementing security standard of mobile wallet in Thailand. The result will be knowledgeable and practical for the companies, financial institution and government that are interested in investing in digital payment especially in mobile wallet. It can be the guideline for the companies to understand consumer perception through online transaction users that can be developed for further mobile wallet security features in the future.

CHAPTER II
LITERATURE REVIEW

2.1 Definition of Mobile Wallet

Mobile Wallet acts like a digital version of physical wallets that store user's credit cards, debit cards, coupons and loyalty card. It is an app that would need to be installed with the smartphone. The user needs to install the app and inputs his payment information, the wallet stores user's information by linking a personal identification format like a number or key, QR code or an image of the owner to each card that is stored (Investopedia, 2017)

2.2 Types of Mobile Wallets

There are several different ways to classify the different mobile wallets. According to Networld Media Group (2015), we can view the types of mobile wallet based on different service providers. There are three types of mobile wallets that can be used at the point of sale.

- Retailers or merchants create their own mobile apps which feature a mobile wallet capability such as Walmart, Starbuck, GrabTaxi etc.
- Financial institutions (FIs) such as banks, credit card issuers and credit unions develop mobile wallets for use by their cardholders in various retail stores.
- Intermediaries such as Apple, Google, and Samsung have developed mobile wallets that can contain cards from multiple issuers.

2.3 Mobile Wallet Technology

With the advanced technology developed from mobile payment, there are three main methods of making a mobile wallet payment at point-of-sale included are NFC, QR codes and Bluetooth.

2.3.1 Near field communication (NFC)

NFC is the key technology to make a contactless payment. According to Federal Reserve Bank of Boston (2017), NFC is a wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. However, there is a limit of using this technology because not all smartphones contain NFC chip. For example, iPhone which are launched before iPhone6 cannot make a payment at POS with NFC card reader. Today, there are still few merchants who support NFC reader in Thailand. Consumers who use Apple Pay will be able to pay at POS with only merchants who have NFC readers while Samsung Pay support for both NFC and MST (a magnetic strip on a traditional payment card reader at terminal POS which most merchants already have).

2.3.2 QR code

Some mobile service providers such as Starbucks, Walmart, WeChat offer QR code-based systems that store payment information in the cloud instead of the handset and can be executed on any smartphone (Networld Media Group, 2015). Customers open up the app and then activate the phone camera to scan a QR code on the reader at point of sales. It connects the phone to the payment and after that customers will receive an e-receipt application via the app.

2.3.3 Bluetooth

Bluetooth Low Energy (BLE) or known as Beacons, it enables Bluetooth 4.0-based smartphones and other mobile devices to communicate with BLE-based wireless transmitters (Connected Lighting, 2014). Once customers enter the stores, their mobile payment app senses a BLE Beacon, and “checks in” to alert the retailer’s POS to the customer’s existing. The customers will receive promotions and product’s information right at the moment via their mobile phone. This also help merchants to identify the consumer who is making the payment. PayPal and Apple also uses Beacons as one of their payment options for customers.

2.4 Perceived Security

There are a number of smartphone users increasing each year, mobile payment becomes a key tool for e-commerce and offline businesses. However, security system is still the most reason that people concern. Jamie, Sushma, Karen and Fred (2016) suggested that lack of awareness, lack of availability, and perceived security risks are all significant barriers to adoption of mobile payments. Many past researches concluded that perceived security risks could be a barrier to acceptance of mobile payments (Cyril et al., 2008; Kim et al., 2010; Loilier, 2013; Mallat, 2007; Misra & Wickamasinghe, 2004; Zhou, 2011). As well as the findings from Alexios (2014) showing that the perception of risk in terms of privacy, m-payments, legislation and product quality deters customers from using mobile payment. Moreover, customers have negative intention to adopt mobile device for making a payment as they feel the risk of unauthorized transaction in the case that device is lost or stolen, the wireless network, operating system and mobile application is unsecured. Therefore, it is important to build trust for users with privacy policy in order to inform them how and what for they are going to use the following elements: data user, data element, purpose of use, conditions and obligations (Steinfield, 2007).

According to a survey published by Gallup (2015), 55 % of US respondents were concerned about some kind of security issues such as a hacking or losing their mobile phones. 21% of respondents do not know enough about mobile wallets to make a decision to adopt it. As well as in Thailand, 69% of smartphone users prefer to research online but they purchase offline (Yozzo, 2016). According to RFi Group’s 2014 Global Payment Evolution, most Thai people still prefer using cash. Three-quarters of consumers indicated that they prefer cash for low-value purchases. Another important reason that Thai people shy away from adopting mobile payment is security concerns. A.T. Kearney (2014) found that 62% of online shoppers in Thailand are reluctant to provide their credit card information online. They concern about personal information privacy. However, it is interesting that 94% of Thai respondents tend to adopt mobile wallet in the future if the security method is more trustful (Visa Thailand, 2016).

2.5 Key Security Features

From the past researches, to ensure and protect security friction for mobile wallet, most mobile wallet providers request users to identify their authentication to access the account before making a payment at POS. Girmay Teamrat Desta (2012) concluded that the main three authentications should be implemented are something you know (password, PIN code), something you have (smartcard, token, ID card) and something you are (biometric characteristics like Iris, voice, fingerprint, face recognition). If the service providers use all three of these, it would be called 'strong authentication' which can strengthen the security of transaction. In other words, we need a password-token-biometric combination.

Authentication is one of the major security systems that provide more convenience for users when making mobile payment. In this research, we will mainly focus on knowledge-based authentication (something you know) and biometric authentication (something you are).

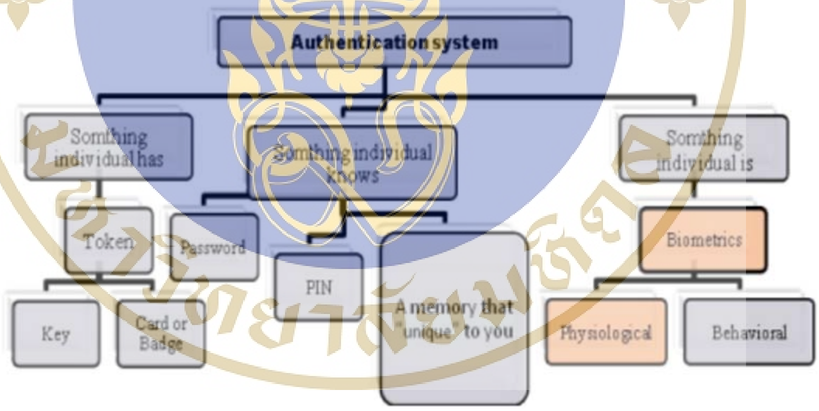

Figure 2.1 Emergence of authentication system

Source: http://ijcea.com/wp-content/uploads/2014/02/pinki_sharma_et_al-1.pdf

2.5.1 PIN and password authentication

This method is most commonly used for authentication on mobile devices. There is a slight difference between PIN and password, PIN is used only with numeric value while password can be a combination of numbers and characters which makes the authentication mechanism more secure than PIN. Thus, password is created to solve out that problem and make the authentication system more complex and difficult to predict or hack. A study of Furnell et al. (2000) showed about attitudes towards different authentication and supervision techniques that 90% of the respondents preferred passwords as a mean of authentication although many of them could accept voice verification and fingerprint recognition as a way of authentication (68%-67%).

OTP (One Time Password) is developed to be more security layers. The system provides a mechanism for logging on to a network or service using a unique password which can only be used once. This prevents some forms of identity theft by making sure that a captured user name and password cannot be used a second time. One-time passwords are classified as a strong authentication, providing much better protection to on-line bank accounts, corporate networks and other systems containing sensitive data (Gemalto, 2015).

2.5.2 Biometric authentication

Biometric authentications are human individual characteristics which could be one of the most reliable authentication mechanisms to verify unique identity of a user. Biometrics are usually classified as physical or behavioral types. The physical type includes biometrics based on stable body features, such as fingerprint, face, iris, and hand (Lawrence O'Gorman, 2013).

Birgit Kaschte (2005) predicted that the usage of biometric authentication will be increased more and more in the future. This will be supported by the advancement of the technologies and the reduction of the prices for hardware and software. Having biometric and password authentication will be adopted together to strengthen security layers potentially. Clarke et al. mentioned that a method of authentication, combining biometrics and PIN code, appears to be an acceptable future method for authentication.

2.6 Possible Killer Apps

To attract customers to use mobile wallet, identifying a killer app is important to drive a high volume of transactions onto the platform. Japan is an interesting case that they produced FeliCa chip embedded in mobile phone. FeliCa was developed by a big company Sony and NTT DoCoMo. Later on, they introduced Osaifu-keita in 2014 which is a mobile wallet service that gathers all kinds of cards and services such as public transportation, bus ticket, railway station, other tickets and buying from convenient stores in one app. Moreover, NTT DoCoMo has signed a deal with MasterCard that allows mobile credit card holders being able to make payments at MasterCard Paypass merchants in 41 countries as well as at 560,000 Osaifu-Keitai points of sale in Japan (Sarah Clark, 2012). This provides Japanese life with more convenience even traveling abroad because they just tap mobile device on NFC reader and go. From this model, it would be very useful for Thai people if we can link all public transportation like Rabbit card, MRT card and bus ticket to be in one and can also purchase anything from convenient stores with the same app.

Another killer app that could be installed in mobile wallet is used for taxis and public transportation. It has been an irritated problem for long time when people take a taxi and they do not have an exact amount for the taxi fare and taxi drivers sometimes do not give a change back. After paying the taxi or transportation fare via mobile wallet app, customers will receive the e-receipt through e-mail. It provides convenience, ease-of-use, ubiquity and the more people use, the more people trust in the mobile wallet. As well as paying for vending machine, mobile wallet can make life easier when people do not have coins to pay. They can scan QR code with contactless payment reader at the vending machine instead of using cash or coins.

2.7 The Chasm Diffusion Model

To develop framework of the research, I would apply the theory of Crossing the Chasm to understand the technology adoption life cycle of different group of people and used for screening process. Mobile wallet is still in its early stages of development, therefore, Diffusion of Innovation and Crossing the Chasm would be useful to look at.

Rogers (1962) explains about the Diffusion of Innovation theory that how innovations and ideas spread across the populations. He says in a social system the innovation is communicated by the process of diffusion. Rogers categorized adopters in five main groups comprised of innovators, early adopters, early majority, late majority and laggards. Innovators are a group of people who look for cool products and they are keen to be the first to try out a new technology, however, they are very small part of this cycle. Second group is Early adopters, this kind of people are visionaries who see potential opportunities in the products and seem to be risk takers. Early Majority is a largest group of the market about 34% of population that foster technology product to be widely used. However, they are more pragmatic and thoughtful about technology and risk averse. They tend to buy the product only after perceiving the solid references and safety measure. They would adopt those technologies once they see positive feedback from Innovators and Early adopters. Next is Late majority who are conservative that can wait and see proof results before deciding to buy a product. This group is very large proportion as early adopters. And the last group, Laggards, would prefer to avoid new technology and will buy it only if they really must.

Later, Moore (1991) sees the significant differences among these groups as “markets” in the “selling” of an innovation to adopters. He argues there is a chasm between the early adopters and the early majority. Moore believes visionaries and pragmatists have very different expectations, and here there is a chasm that challenge marketers to find the way to across. If a company wants to succeed in crossing the chasm, it will be adopted by the market. That means that once an innovation will be adopted by more than 16% of the market, its probability to succeed will grow dramatically.

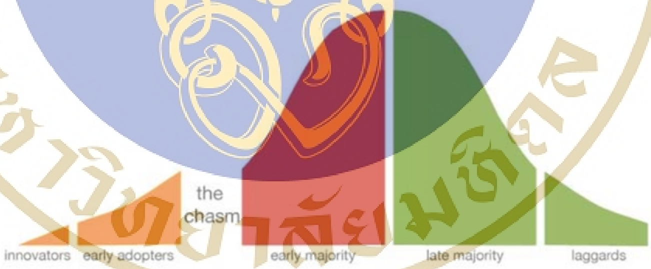

Figure 2.2   Crossing the Chasm: How to Market, Sell And Improve Your Innovative New Product

Source: Jake Nielson, Crossing the Chasm: www.theinnovativemanager.com/crossing-the-chasm-theory-how-to-market-sell-and-improve-your-new-invention/

In conclusion, the framework of this research is to explore and understand consumer perception regarding security concerns which the Chasm Diffusion Model will be applied to help describe and screen a group of respondents. We will mainly focus on a group of early majority to study about their security perception towards adopting mobile wallet regarding security. Because this target is a big player in the market for technology products as they have 34% of the market. It is interesting to find out how can we cross the chasm of the gap between early adopters and early majority.

CHAPTER III
RESEARCH METHODOLOGY

3.1 Research Design

The objective of this research is to understand consumer's perception of security system and explore what could make mobile wallet more security, how many levels of security can people accept? The study will need to be involved in the details of understanding in form of exploratory research; therefore, the "Qualitative" interview approach will be used in this research. Individual in-depth interviews for the total of 10 participants will be conducted

3.2 Data Collection Methodology

3.2.1 Population

The number of Thai users who use mobile payment is at 84% in the last year (Visa Research, 2017) and more than 70% of the overall population uses smartphones in Bangkok (National Statistical Office, 2017). In this research design, the researcher will select respondents living in Bangkok and were classified according to a simplified version of the Chasm Diffusion Model. The researcher will focus on only early majority since they are the segment that influence technology adoption in long term and could be potential target to gain some useful information and insights.

3.2.2 Sampling

In this research, the researcher chooses to conduct 12 sample sizes with depth-interview. To relate with Crossing the Chasm framework, the researcher aims to interview 12 respondents of early majority who play a big role in the market because this target group has the highest number of people and they tend to have the most purchasing power. Thus, exploring in this target group will let us know more about their perspective and attitude toward adopting mobile wallet in terms of security concerns, and to explore what could convince this kind of target to use mobile wallet in the near future. The researcher will perform preliminary judgment for each individual to be interviewed to ensure that the participants are capable to response the questions with well understanding and represent the characteristic of early majority.

3.2.3 Data Collection

Data collection will be gathered during the interview conducted to explore on consumer's feeling, perception and behaviour towards the trusts and perceived risks when considering to make a payment via mobile wallet. The data collected shall also include the opinion and the level of what kind of security they are comfortable to adopt and hopefully could get useful recommendation from consumer side.

The opening questions will begin with regard to respondent's perception and attitude toward using transaction via mobile wallet. And then the researcher will relate them to more detailed questions to find out what kinds of security standard they can accept. More detailed questions will be asked in order to get in-depth understanding how trust in making payment via mobile device in general and what levels of security provided to make respondents comfortable and relaxed to adopt mobile wallet and we can also learn how much they know or get familiar with security method from mobile service providers or Financial Institutions.

3.3 Research Instrument

The interview sessions will be conducted and then transcribed for analysis and part of them will be used for the presentation.

The following questions will be used to gather information from the participants. The questions are structured into four parts:

- Part 1: Personal information

1. Age
2. Occupation

- Part 2: General information about mobile payment

3. Do you usually use mobile phone for shopping or doing transaction? If yes, how often?

- Part 3: General information about mobile wallet

4. Have you ever made a payment via mobile wallets?

If yes, how often?

Do you think what are the advantages of using mobile wallets?

If no, which option do you use instead?

- Part 4: Security perception

5. Do you think mobile wallet/mobile payment is secure?

If not, what do you worry about?

6. Please rate yourself on a scale of 1-5, with 5 having the most concern and 1 having the least concern about security.

1	=	Not concern
2	=	Slightly concern
3	=	Somewhat concern
4	=	Very concern
5	=	Extremely concern

- Part 5: Security Features

7. What could make you feel secure?
8. Do you think password system is secure?
9. What do you think about biometric authentication e.g. fingerprint, iris recognition, face recognition?
10. Lastly, how likely would you adopt it in the near future?

CHAPTER IV
RESEARCH FINDINGS

4.1 Findings

After interviewing 12 participants which were divided into two groups; mobile wallet users and non-users. There are some similarities and dissimilarities in terms of security perception towards mobile payment. These 12 participants were selected based on the characteristics of early majority who are the main target group in the market today. The researcher would like to explore about this group's perceptions toward security system and find out what could be best practice to make them more comfortable to adopt mobile wallet in the future. All of them live in Bangkok and show the characteristics of early majority as pragmatic users who are thoughtful about accepting change and need more details supported before trying out. There are 2 main dimensions that are relevant in this research that must be asked to every participant which are security perception and security features.

Table 4.1 Participants Information

Users			Non-Users		
Sex	Occupation	Age	Sex	Occupation	Age
Female	Office worker	29	Female	Office worker	26
Female	Office worker	26	Female	Office worker	26
Female	Office worker	27	Female	Office worker	28
Female	Office worker	28	Female	Office worker	25
Male	Office worker	26	Male	Office worker	27
Male	Business owner	30	Male	Office worker	28

For both mobile wallet users and non-users, the researcher started the question with ‘Do you usually use mobile payment for transaction?’ to see how much they are familiar with mobile payment in daily life. Most of them answered that they normally made a payment via mobile phone at least 1-2 times per month and some of them used it more than 5 times per month. They used mobile payment for various reasons such as online shopping, bills pay and money transfer. In this semi-interview comprised of 6 participants who are mobile wallet users and 6 participants who never used mobile wallet for making a payment.

4.1.1 Mobile Wallet Users

For respondents who have experienced with mobile wallets, the researcher found that 3 out of 6 respondents are using TrueMoney wallet which belongs to True Corporation Company. One respondent uses this mobile wallet app every week. He said that he could use the mobile wallet to make a purchase at any 7-11 convenience stores by adding some amount of money into the e-wallet and letting staff scan barcode on his mobile phone instead of paying by cash. Sometimes the app offered promotion or discounted price when purchasing through its mobile wallet.

Mobile wallets are also useful for people who do not hold credit card. The main reason for the second respondent using TrueMoney Wallet is she did not have a credit card, but she wanted to buy some movies from Netflix which required to connect with credit card only. Thus, this mobile wallet app provides a visual credit card for her and she could use it to purchase through Netflix without having a real credit card at all. Another respondent uses TrueMoney Wallet to pay mobile phone bill and also purchase something at 7-11 convenience stores. And for the rest of respondents use various mobile wallet service providers such as AirPay, BluePay, Line Pay etc. Two respondents use AirPay for buying movie tickets because of discounted price and use Blue Pay for buying game items and pay bills. Another respondent uses Line Pay to buy stickers and food deals in the app.

4.1.2 Non-Users

For those who are non-users, they did not know mobile wallet and never use the app. However, 3 out of 6 respondents have ever heard of mobile wallet’s names but did not know how they work. When asking what options they normally made a payment via mobile phone, all respondents answered mobile banking as the first option and credit card as the second option. Mostly used for online shopping and transaction via mobile banking.

Interestingly, there is a non-user who shared her experienced about a vending machine that located near a fitness center at her condominium. It offered a QR code on the machine, so people who came in this fitness could buy a bottle of water by scanning QR code via mobile wallet app (BluePay). She said that she wanted to try paying the vending machine with the mobile wallet next time and she had already downloaded the app into mobile phone. “I think it’s useful for people like me who came to the fitness and did not bring much money or a wallet. Normally I only bring a mobile phone to the fitness.”

4.2 Security Perception

In terms of security perception, there are various reasons that make participants concern about. The interviewer asked all 12 respondents with the same question “Do you think making a payment via mobile app or mobile wallet is secure?” and then dig down into their perception “If not, what do you worry about?” to see what are the main reasons and how much they concern about security system.

4.2.1 Data Hacking

After interviewing, most of the respondents mentioned about cyber hacking while doing transaction via mobile phone. One respondent who did not use mobile wallet said that she was quite concerned about data hacking and personal information privacy because she had to link her card number with the app, so hackers might be able to access her data anytime and she could not know when that would happen with her. That is a reason why she did not want to use mobile wallet. However, she used mobile banking 1-2 times per month for paying bills and she felt more securable with mobile banking than mobile wallet because it is from the bank not from the private company.

A respondent, non-user aged 26, showed me how concern about security she was. Whenever she had to bring her mobile phone to get repaired, she would delete all mobile banking apps before sending to the technician and after getting the mobile phone right back, she would go to ATM and check all balance of every bank account she has in order to make sure that her money amount was still the same. She was afraid of being hacked by those technicians. However, in terms of using mobile payment for online shopping, she slightly concerned about it because there were notifications every time she was going to make a payment and asked for authentication like password before purchasing.

As well as a respondent who is a mobile wallet user, he was not concerned much about being hacked as he believed that those hackers should take their effort hacking into millionaire or rich people instead of middle income people like him, and he always put money in the e-wallet for the exact amount that he wanted to spend, he did not add too much money in the wallet, so he did not concern about security or data hacking.

4.2.2 Data Privacy

Two respondents of non-users mentioned that they concerned about personal information because their data would be kept by others and they could not know what the companies or government would do with their data. Then they gave an example of PromptPay which was launched by the government to support the idea of cashless society, that they were not comfortable to use PromtPay even though all major banks are now encouraging people to adopt.

However, a respondent who used to apply PromtPay said that she was not concerned about that, she thought it was convenient for her to receive money from the government and it took the process faster and easier. She did not to wait and go to pick up the cheque anymore. The money was transferred into her account directly in a short time.

Moreover, 4 out of 6 non-user respondents did not want to link their bank cards with many apps because when any problem occurs, they can contact directly to the banks, but if they had many accounts linking with mobile apps, it would be messy when forgetting some accounts and making too complicated to solve out.

4.2.3 Stolen Mobile Phone

Three non-users concerned about lost mobile phone or stolen mobile phone. They were not confident to use mobile wallet app because they did not know how much the company could provide security solution for them when having this kind of problem. But if it’s from financial institution like banks, they would have less concern. When asking the mobile wallet users, four respondents did not aware of this because they thought that it was the same case when people lost their purse and they had to call banks for stopping the card usage. As well as the process of using e-wallet, when this situation happened, users could contact mobile service providers immediately or go to its website and log into their account and select to deactivate account regarding lost mobile phone or whatever. They think it was more safe than losing physical wallet as thieves could take their money right away at the moment, but for mobile phone, they had to take time to figure out the way to access the account. It would be difficult to hack unless they knew password.

A female user, aged 27, suggested about service for mobile service providers to make users more trustful “Service providers should always be clear about their policies and what they would do to compensate should damages done. They should also have helpful call centers that can assist customers 24/7.”

4.2.4 Reputation of Mobile Service Providers

Being well-known of the companies is also important for some respondents. One respondent who is using TrueMoney app said “I do not and will never link my entire bank account with an app. I choose to add only necessary amount into the app just to make each payment so I don’t have to worry much about my money mysteriously disappearing. I know how online banking works and what problems that could come with it (e.g. hacking, personal data stealing, server error) but because I understand what I got myself into, I choose the safest way for myself and that’s why I’m not too worried about it. However, I’d say it depends on the company that owns the app, too. If I’m not familiar with them, I would be very concerned and wouldn’t use their apps. She also added “I always think everything has loophole but as far as everyday-life usage, I’d say right now all companies probably provide the most secure method that most people can afford. If they have same security standard as actual banks, then I'll be fine with it."

One respondent who never uses mobile wallet also mentioned "I think it's not only about security, but it depends on what company and how well-known it is. I would use mobile wallet as long as those companies can prove that I can trust them and show me the credible process to link my account with the app. They should state clearly about the security and solution when any problem occurs. The system must be ready and stable for widely used in a short time"

Furthermore, one user and two non-users shared the same opinion that they normally would search for feedback and reviews from others who have experienced with any mobile payment app before making a decision to adopt. If those who reviews no natter from friends, families or from social media and they shared positive feedback, the respondents would likely to use it.

4.3 Security Features

In this section, the interviewees were asked about security features that could make them feel secure when making a payment via mobile phone to explore which security features they are comfortable with. Moreover, two types of authentication which are password and biometric authentication e.g. fingerprint, iris, face recognition would be asked in this part.

4.3.1 Password Authentication

From the interview, all respondents agreed with password authentication as the most favorable method for security system. Some of them said that they were more familiar with password than biometric authentication. In their opinion, using password was more safe because only users who knew the password could access the account. One female respondent, a mobile wallet user, said that she preferred password as there was a chance to touch and to put password herself which took a little time before accessing the account while fingerprint was too fast for her and did not even realize that it had already read her fingerprint. A female user, aged 29, said I think everything has loophole but at the same time I believe it's the best method (password) that nearly everyone can afford.

OTP (One Time Password)

Moreover, most of the respondents mentioned about OTP (One Time Password). They suggested that it would be the best secure method when there is OTP requirement every time before making a payment. They wanted more security layers like OTP to verify users again. This would make them more confident with the mobile transaction. One female user, aged 26, said "Maybe add about two or three authentications. One Time Password is widely used method but if my phone got stolen, the thief might be able to access my wallet app, and so I think there should be double password – password to access the app (just like when you access email or social media apps) and OTP for every time I need to transfer money."

Another respondent, a mobile wallet user, said "Some apps did not provide OTP but they required users to put password instead before doing transaction. I think this is not secure enough. They should have both password and OTP to verify again, or the password for transaction should be a different one, so that it would make the process a little more complicated and this makes me more secure. I also wanted a confirmation of the total amount that I have to pay before my money would be cut off."

4.3.2 SMS/E-Mail

Sending SMS or Email to notify users are the most secure feature that all respondents are highly satisfied with. Most of the respondents desire for real time messages to let them know the exact amount of money or any transaction occurred at the moment.

A male user, aged 30, said "Every time after money is transferred, the app should generate a proof of payment and save it automatically to the phone or send the document to the owner's email." He also suggested about having feature of budget control. "Users should always be able to set limit of money they can transfer and put their accounts on hold/temporarily close their accounts if needed."

Moreover, two respondents talked about the same function that there should be SMS to notify users when the amount they had set was going to run out, so that they could manage their money more effectively and to remind them how much they already had spent.

From the interview, 12 respondents are more confident with security when mobile wallets or mobile payment send them SMS or E-mail every time when transaction occurred. One user said “Actually, I don’t worry much about security so far as there are several security layers for authentication. I have evidences of all transactions, so when there is any problem, I can track the payment history and show the receipt to companies and be able to deal with the problem immediately if I got any mysterious transaction message.

4.3.3 Biometric Authentication

5 out of 12 respondents were satisfied with biometric authentication like fingerprint because it was very convenient and they thought it was difficult to hack or copy. It is useful in some situations, for example, they forgot the password. So, using fingerprint could save their time a lot. Two respondents preferred Iris recognition as they believed it was the most secure biometric authentication. And the 5 remainders insisted to use password rather than all kinds of biometric authentication. In their opinions, using password is the most secure method. A user respondent, aged 28, said “I don’t think biometric authentication is secure enough, but I would say it provides more convenient. For me, password is still the most trustful one.” Another respondent, aged 29, expressed her opinion about biometric authentication “As of now, this sounds like a nice add-on feature. I still think we shouldn’t rely on this alone – there should still keep other authentication methods but biometric will definitely strengthen security system to some extent.”

4.4 Conclusion

In conclusion, from both users and non-users’ interview, they have similar major concerns about security which are data hacking, data privacy and stolen mobile phone. However, users who have experienced with mobile wallets did not have high level of security concern as there are many security layers e.g. password, OTP, SMS, real time messages, evidence of transactions which could make them more comfortable to make a payment and they have not faced any bad experiences with those mobile wallets yet. Thus, they thought it was convenient for using it. While among non-users of mobile wallets, they were slightly more worried about security system than users. They were satisfied with those security systems like password, OTP, SMS etc. However, they were afraid of linking bank account with many apps and still did not perceive usefulness of mobile wallets. One respondent expressed his opinion that if he could use mobile wallet with various merchants through only one app, he would likely try it in the future because he could manage and less concern about linking cards with many apps that would make him insecure. But today there are still a friction of each mobile service providers, for example, paying mobile phone bills through TrueMoney app is limited to only users who are using True mobile network.

CHAPTER V
RECOMMENDATIONS

According to the Chasm Diffusion Model, early majority is the main group in the market who has high influence on technology product adoption in long term. Thus, convincing this target group is also important to focus on for mobile wallet service providers. From the findings, this target group is already familiar with mobile payment because they used it in daily life, and they still have had good experienced in mobile transaction so far. Therefore, they did not have high level of security concerns when comparing with late majority and laggards, but they are aware of making payment through mobile devices. Most of the respondents want confirmation and authentication layers that could make them more comfortable to adopt. Interviewing non-users showed that they prefer to link bank cards with only one major app like mobile banking which has more creditability than other wallet apps in their opinions.

Moreover, the researcher found that perceived usefulness becomes the main barrier for convincing a group of Early Majority to adopt it. Even though they did not concern much of security as expected, mostly of non-users did not see necessary to use mobile wallet in daily life.

5.1 Recommendations

From the findings, there are some helpful information that can be the recommendations for mobile wallet service providers in Thailand. To improve and understand more about early majority's perception, there are two points from the interviews regarding security that users can accept and usefulness which becomes the main barrier for technology adoption instead.

5.1.1 Managerial implication on security system

5.1.1.1 Require strong user authentication

The results revealed that most of the respondents are satisfied with several authentication layers to verify users before making a payment. The companies should require different authentication systems to get confirmation and to build confidence from the users, for example, requiring password when entering the app and requiring OTP or different password before making a payment.

5.1.1.2 State clearly about security policies and solutions

Most of the respondents wanted to know what are the companies' solution plans offered to customers in case there is any problem occurred e.g. lost mobile phone, mysterious transaction appearing etc. When mobile phone was stolen, the companies should clearly inform customers about who to contact and how to reach them instantly. Providing 24 hrs. call center can be the most satisfactory service that mobile service providers can do.

5.1.1.3 Provide notifications and setting of limits

The respondents want to see what is happening with their account in real time, so the companies should implement alerts for customers, e.g. via phone calls, SMSs or e-mails when they have transactions, or inform cumulative amount over a certain period of time. Moreover, they should let the users be able to set limit of money they can transfer and put their accounts on hold or temporarily close their accounts if needed.

5.1.1.4 Develop connection with various merchants

To meet customer's needs, the companies should provide them like a one-stop payment app that customers can purchase various products at many merchants/stores. The companies should expand and collaborate with more merchants that support a day-to-day scenario, so that customers will have convenience and good experiences in making a payment everywhere. For example, paying for bus tickets, movie tickets, coffee shops, taxis, clothing shops, grocery stores should be able to be paid via only one app. Customers do not have to link their cards with many apps. They can transfer money to their friends, scan QR codes, pay utility bills, pay at restaurants and everywhere else.

5.1.2 Managerial implication on increasing adoption regarding communication

From the findings, there is another interesting thing to point out, that is most of the non-users did not perceive usefulness of using mobile wallet and this seem to be the main barrier for mobile wallet adoption. Some of the respondents did not even know how it works and what are the differences between mobile banking and mobile wallets. The researcher found that security is not the main barrier for Early Majority group. Thus, the thing to focus on is boosting the actual app design to attract users, offering useful features that support daily life and the way to communicate with them to create the perception of usefulness instead. Companies need to communicate and educate people what are the benefits of the mobile wallets and how it helps change their life in a better way. The companies can use online channel to promote and communicate with the target because this group is familiar with social media. They can access the internet through their smartphones everyday and everywhere.

5.2 Limitations and further researches

This paper aimed to explore and focus on the group of early majority to study their security perception toward mobile wallets. With the limit of time, the author chose to collect qualitative data with 12 sample size and found out that security is not the main barrier for this group but perceived usefulness is the point to focus on. Therefore, the future researchers can continue fleshing out in greater detail about what might make these mobile wallet apps useful in the eyes of customers and should conduct with greater sample size encompassing different demographic groups than these sample.

REFERENCES

Ajeet Khurana. (2015). *The Future of Biometric Authentication for Digital Payments*. Retrieved October 20, 2017, from https://www.mastercardbiz.com/2015/03/30/the-future-of-biometric-authentication-for-digital-payments/.

Bill Fisher. (2017). *Trust and Security Remain Big Issue for Mobile Payment*. Retrieved October 10, 2017, from http://www.telegraph.co.uk/connect/better-business/trust-and-security-big-issues-mobile-payments/.

Donald L. Amoroso1 and Rémy Magnier Watanabe. (2012). *Building a Research Model for Mobile Wallet Consumer Adoption: The Case of Mobile Suica in Japan*. Retrieved October 15, 2017, from http://www.scielo.cl/scielo.php?pid=S0718-18762012000100008&script=sci_arttext.

Elisa Tavilla. (2015). *A Case Study in Mobile: Paving the Way for Mobile Payments in Thailand*. Retrieved November 5, 2017 from file:///Users/Palale/Downloads/Mobile-Payments-in-Thailand.pdf.

Erika Chin1, Adrienne Porter Felt2, Vyas Sekar†3 and David Wagner4. (2012). *Measuring User Confidence in Smartphone Security and Privacy*. Washington, DC. United States.

Girmay Teamrat Desta. (2012). *Security for Mobile Payment Transaction*. Master of Science Dissertation, KTH Industrial and Engineering Management. Sweden.

Hanul Sieger. (2015). *Perceived Security and Percieved Usefulness of Mobile Payment*. M.A. Dissertation, The Technical University of Berlin. Germany.

ISACA. (2011). *Mobile Payments: Risk, Security and Assurance Issues*. Retrieved October 15, 2017, from https://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf

Jake Nielson. (2014). *Crossing the Chasm: How to Market, Sell and Improve Your Innovative New Product*. Retrieved November 14, 2017 from https://www.theinnovativemanager.com/crossing-the-chasm-theory-how-to-market-sell-and-improve-your-new-invention/

Ngoc Doan. (2014). *Consumer Adoption in Mobile Wallet*. Retrieved October 10, 2017, from http://www.theseus.fi/bitstream/handle/10024/86343/Ngoc_Doan.pdf ?sequence=1.

Noam Ben-Asher, Hanul Sieger, Asaf Ben-Oved, Niklas Kirschnick, Joachim Meyer and Sebastian Moller. (2011). *On the Need for Different Security Methods on Mobile Phones*. Stockholm. Sweden.

Rabbit Finance. (2017). *Cashless Society*. Retrieved October 10, 2017, from https:// today.line.me/TH/pc/article/0da651190d6d1092787ca3be55e71d99b1cdfa 4fea968284551d703902522b3c.

Robin Arnfield. (2015). *Mobile Wallets 101*. Retrieved October 20, 2017, from https:// emergingpayments.org/wp-content/uploads/2017/02/Mobile-Wallets-101-Cardlinx.pdf.

S.Karatzouni , S.M.Furnell, N.L.Clarke1, R.A.Botha. (2007). *Perceptions of User Authentication on Mobile Devices*. Las Vegas. United States.