Mobile Payments and End Users' Sensitivity to Information Disclosure

Mr. Abdulwaheed Johnson, Pace University

Abdulwaheed Johnson is a cybersecurity enthusiast who is currently in the second year of his Masters' Degree program in Telecommunication Systems and Networks at Pace University, New York. His first degree was in Electrical Engineering, and is looking to specialize in cloud security after the completion of his Masters Degree program.

Dr. Anthony Joseph, Pace University

Dr. Anthony Joseph has a Ph.D. in electrical engineering with specialization in digital signal processing. He conducts research in digital signal processing, neural networks, and teaching and learning in higher education. Some recent applications include compression, modeling, and prediction in economics and finance, as well as speech recognition, globalization, entrepreneurship and innovation, and computing and engineering education with emphasis teams, teamwork, collaborative and team-based learning, and cooperative education.

Mobile Payments and the End Users' Sensitivity to Information Disclosure

Abstract: The adoption of electronic and mobile payments has improved significantly in recent years. A number of payment channels that provide convenience are now ubiquitously available for conducting electronic transactions. These payment methods range from credit cards to the Near Field Communication (NFC) tap and pay methods. A recurring premise in these electronic payment methods is the guaranteeing of security and privacy of the end-user's personally identifiable information especially with respect to financially sensitive information. However, recent high profile information breaches have seemed to suggest otherwise. While information security administrators have scrambled to secure financial institutions' payment gateways and enterprise networks, an often overlooked domain is end user security. This paper aims to examine mobile payments security as well as the end user's sensitivity to disclosing personally identifiable information in relation to preferred payment methods. The methodology employed is the statistical inferencing of a survey on 138 valid respondents consisting mostly of university students, to assess the information disclosure sensitivity across the various subpopulations. The results of these assessments showed that business students and professionals were significantly more sensitive to information disclosure than other assessed subpopulations.

1.0 Introduction

Mobile technologies have advantages such as ubiquity, customization, and personalization. According to the Groupe Speciale Mobile (GSM) Association (2016), there are 4.7 billion unique mobile subscribers, which is equivalent to 63% of the world's population [1] [14]. The mobile device has become almost universal to everyone and can provide services which make them especially suitable for use as an electronic payment method. The current payment landscape is gradually shifting to mobile payment technologies, an increasing trend that utilizes cloud and mobile technologies in carrying out financial transactions over end users' smart mobile devices [2]. Mobile payments can be seen as a venture for investors and service providers because of the available benefits [1]. Hence, the drive towards mobile payments adoption is an expected phenomenon.

There is an increasing call for mobile payment adoption, as it transparently secures transactions and contributes to assurance of trust to the end user [3]. However, early forecasts of mobile payments uptake have been lower than expected. Mobile payments were introduced with various impeding factors such as cost, complexity, and lack of trust from consumers which have contributed to its non-adoption [4]. Advancements have been implemented on the mobile payment systems, and its adoption is gradually increasing. Such advancements are towards enhancing trust, curbing risks, and improving security. These improvements are largely seen to be better than the security of plastic payment cards. Improved security controls such as tokenization, device specific cryptograms, and two-factor authentications have made mobile payments (MP) an attractive payment option for both merchants and the end users [3]. Mobile payment service providers are PayPal, MasterCard, LevelUp and Square, with recent entrance from enterprise participants such as Apple, Google, and Samsung. These companies invested in the mobile payment platform in various ways, to keep up with potential mass adoption of mobile payment systems.

2.0 *Mobile Payments*

Mobile payments are a form of electronic payment that operate using mobile devices such as smartphones, tablets, and PDAs. Mobile payments combine payment systems with mobile devices and services to provide users with the ability to initiate, authorize, and complete financial transactions over a communication network. It is a payment system like a credit card or any form of electronic payment except it relies on the usage of mobile devices rather than the conventional banknote, credit card, or check to transmit the payment [4][5]. Two categories of Mobile payment systems exist; these are Remote Mobile Payment and Proximity Mobile Payment. The difference between the two is the level of direct interaction needed between the consumer's device and the merchant's payment terminal [4]. In proximity mobile payments (also known as contactless payments), the payment terminal has to come in direct contact with the mobile device, examples are Radio Frequency Identification (RFID) and Near Field Communication (NFC) devices. In remote mobile payments (generally regarded as online mobile payments), the payment terminal does not have to come in direct contact with the mobile device; examples are carrier billing, mobile payment applications using a barcode, QR codes, and cloud technologies such as implemented in PayPal, Starbucks, and Dunkin Donuts applications [4][6][7]. Mobile payment systems are similar to mobile commerce, which involves the use of mobile devices (usually smartphones, tablets, and other handheld computing devices) for initiating or completing an electronic transaction [9], but the difference lies in the role of the mobile device and the type of transaction. In mobile commerce, the transaction is carried out entirely over the internet by the end-user to the recipient, while in mobile payments there is an exchange of information between the end user and the merchant, usually through a mobile payment terminal which is linked to an Automated Clearing House (ACH). Moreover, mobile commerce penetration is helping to spur mobile payment adoption [15].

The concept of mobile payments was first developed by Coca-Cola in 1997, using a Radio Frequency-Identification (RFID) terminal. This spurred innovation of several other methods of mobile payment over the years, such as PayPal which was founded by eBay in 1998, to replace the existing payment methods [4]. However, end user acceptance of mobile payments has fallen short of projections. Although some regions of the world have found more success in mobile payments adoption than for example Japan, China, and Turkey, Asia Pacific in particular leads the mobile payment adoption charts, with the highest level of confidence in these transactions at 65%, and in 2016 China accounted for 58% of this region's mobile payments [16]. These data are in comparison to the level of confidence in the United States which is 41% [1][4]. Mobile payments platforms also have mobile applications utilizing various remote payment methods. These mobile applications could facilitate consumer-to-consumer (C2C) transfer services e.g. PayPal, Commercial Bank applications, and Enterprise applications such as offered by Starbucks and Dunkin Donuts [4][6].

In September 2011, Google launched the Google Wallet application, in competition to eBay's Paypal, it featured a way for securely storing payment card information and payments using NFC technology [4][8]. Thereafter, as NFC technology was gradually rolled out on mobile phones, other NFC applications were developed from 2014 to 2015, by companies such as Samsung, Apple, and Google, with technologies such as Apple pay, Android pay and Samsung pay respectively. PayPal also became independent from eBay to allow for its unrestricted

development [4], the entry of Apple and Google into the mobile payment ecosystem, along with other reputable companies, migrating from their conventional business models, has been heralded as a much needed catalyst for increased mobile payment adoption by end users as well as merchants. The emergence of Apple Pay in particular was predicted to give mobile payments adoption a boost especially in NFC adoption because of Apple's device proliferation (iPhone and Apple watches), [1][4].

2.1 *Classes of Mobile Payments*

There are two broad classifications of mobile payments, based on the level of interaction between the end –user's mobile device and the payment terminal. These are the Proximity Mobile Payment and the Remote Mobile Payment (also known as Online Payments).

Remote Mobile Payments - These mobile payment methods are initiated without the need for any direct contact between the consumer's mobile payment device and the merchant's payment terminal. This is typically done through a mobile application. Examples of remote mobile payments are Carrier Billing, QR Codes, Bar Codes, and Cloud technologies. Remote Mobile payment implementation requires less investment by the merchant and the consumers. However, users may need to download more than one payment application which could be an inconvenience. Remote mobile payment systems may also need integration to a current/updated payment terminal system which might require additional equipment such as scanners. These online payment methods are necessary alternative forms of mobile payment because only a few mobile devices support proximity mobile payment methods. Remote payments methods are typically linked to a less costly Automated Clearing House (ACH) or proprietary pre-funded methods [2][4].

Proximity Mobile Payments - These mobile payment methods require some form of direct contact between the consumer's mobile payment device and the merchant's payment terminal. Typical examples of proximity mobile payments methods are the Near Field Communication (NFC) and Radio Frequency-Identification (RFID) payment methods. The NFC is a type of proximity payment method that operates by enabling two-way short range communication for information exchange between two NFC capable devices that are in close proximity, typically an NFC enabled mobile device and an NFC payment terminal. Its advantages lie in its ease-of-use, and speed of transaction processing. NFC functionality is embedded in some newer mobile devices and is seeing increasing implementation [4][10][11].

2.2 *Properties of Mobile Payments*

Mobile payment systems when compared with other traditional and electronic payment systems provide distinct properties which make them the future of the payments industry. These include mobility, ease-of-use, speed, security, and efficiency of transaction processing. Mobility refers to the capability of mobile payment transactions to be carried out at any time and in any place. Ease of use is the ease with which transactions can be performed using mobile payment methods. Mobile payments are completed in a relatively short time when compared to other forms of payment, hence the speed attribution, and the security of mobile payments is also a benefit that makes mobile payments adoption particularly advantageous [1][4][5]. The ease-of-use, speed,

and efficiency of transaction processing are factors that boost merchant adoption as well [2]. "The acceptance of mobile payment method[s] by merchant[s] especially small and mid-sized business[es] (SMBs) has risen tremendously…[to] 21% of SMBs …by July 2014; a significant rise of 11% as compared to 10% of acceptance in July 2012…" [4].

2.3 *Factors Affecting the Adoption of Mobile Payment*

Privacy and security concerns are two major factors that affect the adoption of any electronic payment solution including mobile payment systems: the threat of cybercriminals theft of sensitive information such as Personally Identifiable Information (PII) and, specially, Financially Sensitive Information (FSI). The Lack of authority on transactions increases the risk perception of customers and negatively influences trust [1]. Laws exist such as the Payment Card Industry Data Security Standard (PCI DSS) that prevent storage of customer payment data on the payment points. This secures sensitive data and increases trust in the payments platforms [2]. Other factors that affect the adoption of mobile payment are: perceived reputation, perceived risk, trust, perceived usefulness, perceived ease-of-use, attitude, cost, performance expectancy, network externalities [1][2][4].

Trust in the mobile payment system refers to the belief by the end-user that the platform is risk-free [1]. It is the belief that all parties involved in the processing of the transaction will fulfill their obligations and protect the participants from financial loss. The greater the number of positive experiences the higher the level of trust [2][5]. Perceived reputation is seen as the greatest predictor of trust while perceived risk is the uncertainty that comes with a negative experience from using mobile payment system technology. Environmental and operational factors such as the novelty of mobile payments contribute to this uncertainty which also affects trust [1]. Perceived usefulness is the belief by the end-user that the use of mobile payments will enhance productivity and effectiveness [1]. Perceived ease-of-use is the level of effortlessness or tediousness associated with learning and utilizing the mobile payment system. Attitude refers to the feeling towards the intention to use a mobile payment technology [1]. Cost is the associated monetary value of implementing a mobile payment system, which could be significantly high for the end-user and the merchants in terms of the cost of a mobile payment capable smartphone and mobile payment terminal respectively. The specific costs include upgrading the mobile payment terminals, training, software integration, and the cost per transaction processing fee of the chosen mobile payment method [2][4]. Performance expectancy is driven by hedonic motivation and habits; it is defined as the degree of satisfaction a consumer expects to receive when using the mobile payment technology [5]. Limited network externalities refer to limited implementation of mobile payments terminal [4]. Network externalities refer to the compatibility of different implementations of similar mobile payment technology. This could also extend to incompatibility of the various mobile payment platforms. The lack of standardization and compatibility can lead to a fragmented market, a market in which several mobile payment technologies exist but none gains enough traction to propel the industry forward. Coexistence and compatibility of the mobile payment service providers is necessary to prevent market fragmentation [2][4].

2.4 *Enhancing the Adoption of Mobile Payments*

In order to improve the adoption of mobile payments, the end user has to be guaranteed that the platform is risk free. Security and privacy centers around the perceived risk about mobile payments, issues such as authentication, authorization, and confidentiality are major examples. However, recent research has shown mobile payment systems like PayPal, Apple Pay, and Google Wallet are safer and more secure than using credit cards [4]. Various methods have been implemented to secure mobile payment systems such as tokenization, two-factor authentication, device specific cryptograms etc. Cloud-based mobile payment systems such as Google Wallet store, encrypt, and monitor any unauthorized access to financially sensitive information [3][4]. The issue of network externalities is also being addressed by the mobile payment service providers who are working together for the common interest of increasing compatibility among the various mobile payment platforms. This improves mobility; as more types of payment transactions can be done on the go. The speed of transaction is also a driving force of the technology, because it saves time, which is an oft-cited advantage of mobile payment systems for consumers when making purchases over the cloud and using remote payments instead of at the POS (point of sale) [4]. Also, noteworthy, is that the regions with high mobile payment (MP) penetration, largely involve government participation through MP capable government-infrastructure as well as government-to-person disbursements [6]. Provision of these conditions facilitates end user adoption.

2.5 *Security Features Available in Mobile Payments*

Tokenization - This is a property of mobile payments, where when the transactions are to be processed, the payment application and Point-of-Sale (POS) platform do not transmit the primary account number, but instead send randomly-generated tokens to the POS terminal or the payment network [3]. Only the issuing bank and authorized entities can securely map tokens back to the original payment card data. Tokenization solves the issue of security of financially sensitive information in transit, as well as protects the end-user from any unsafe or unauthorized payment from criminals and cybercriminals. These tokens can be configured to work within only given parameters such as location, time schedule, specific retailers, and payment amount range. Alerts are sent to the users when any unusual activity is detected [3][4].

Device specific cryptogram – This is used to whitelist specific devices, ensuring that only payments originating from that device are authorized. The cryptogram sent from a specific mobile payment device/terminal cannot be used on another device [3]. This makes it harder for cybercriminals to perform man-in-the–middle (MITM) attacks.

Two-factor Authentication - This is a security measure that is beginning to gain widespread acceptance in information systems. Two-factor authentication helps protect against unauthorized access by providing an additional authentication mechanism for access confirmation. Examples are biometric authentication such as fingerprints, facial recognition and iris scan, as well as the one-time password (OTP) generated on hardware token devices or software tokens (sent via email and SMS or generated on an authenticator application). It eliminates the issue of liability in Card Not Present (CNP) or Card Present (CP) transactions [2][3][12].

Apart from these mobile payment security features, mobile devices also come with integrated security features such as passwords and remote wipe in case the device is lost or stolen: For

example, any mobile payments application on the mobile device has an extra layer of security and any credential stored on the phone can be wiped remotely if it is lost/stolen without the need for payment mechanism replacement [3].

Generally, mobile payments reduce overall operating costs when paired with m-commerce due to reduced fraud loss and lower payment processing costs in online payment methods. However, it could lead to higher costs especially with NFC-based payment terminal equipment investments, especially in a fragmented market.

3.0 Literature Review

Hayashi and Bradford [2] carried out a study on mobile payment in which interviews were conducted with 20 large and mid- sized business merchants implementing mobile payment platforms. The study concluded that most of the merchants preferred barcode, and cloud payments to NFC payments. While customer shopping experience and the high interchange fees of card payment at the Automated Clearing House (ACH) in comparison to mobile payment fees are motivators for adopting mobile payment technology. Another cited attribute was customer data control, which enabled the merchants to engage in highly targeted marketing by offering incentives such as discounts and coupons to the customer [2]. However, in a previous study by the same author [10], where the focus was the consumers, the ability to receive targeted advertisement was seen as a potential cause for concern, stating "they might dislike targeted marketing because they view the use of personal information as an invasion of privacy" [10]. This ambiguity is rooted in the customers' that are highly sensitive to the disclosure of personally identifiable information (PII).

Security and privacy are advantages of mobile payments, features like Apple's "One-use transaction token" and Google's "Unauthorized transaction tracking", have helped increase security as well as end-users' confidence levels [4]. However, getting the end-user to shift from the conventional payment methods that have worked fine albeit with some issues is still a hindrance to increasing the mobile payment adoption rate to 1 billion users [4]. The issue of privacy and security is a major factor in the adoption of any electronic payment. Unfortunately, there is an assumption of insecurity of mobile payments. Even security experts wrongly assume that mobile payments are unsafe, according to a 2015 survey by ISACA (Information Systems Audit and Control Association), only 23% of IT and cybersecurity professionals believe that mobile payments keep personal information safe [3]. While some vulnerabilities exist in mobile payments, merchants and consumers are encouraged to adopt mobile payment systems and regularly evaluate any developments to prevent any breach [5].

Mobile payments are the next revolution of payments replacing cash and credit cards; however, there is a necessity for continued improvement to reduce market fragmentation and network externalities while increasing reliability, privacy, and security. These improvements will advance mobile payment adoption for merchants and customers whose preferences will continue to influence industry direction [5]. According to Ooi Wei et al (2015), "[T]here will be tremendous increase of NFC terminal[s] in most SMBs [small to medium sized businesses] credited mostly to Apple Pay…" [4]. Current improvements in the electronic payment industry include migration to chip based (EMV) credit cards to enhance security, implementing a Card is Present (CP)

transaction to shift fraud liability [2]. Adoption of EMVs is being used to push NFC adoption, as EMV card readers in the US, also have integrated NFC terminals with a minimal cost difference between the EMV contact card readers and EMV contactless card readers [2]. NFC payment terminals are also known as contactless card readers; they can be used in conjunction with CP payment applications on compatible devices [2]. Apart from NFC, other predominant forms of mobile payments exist, such as QR, barcode, and cloud-based payments. Cloud technology utilizes remote servers to carry out transaction processing. Barcode, QR codes and cloud technologies are online payment methods and can be classified as Remote Mobile Payments [2].

The global number of payment users is expected to reach 1.09 billion by 2019, up from 44.55 million in 2014. As sited in [1], -in a study of 15 countries, some countries had as much as 56% penetration of mobile payment, whereas others had only 33%.It was found that the difference in use was largely due to the proportion of Generation Y persons in each country's population.

Several models have been proposed to study the adoption of mobile payments technology. Popular models are the Unified Theory of Acceptance and Use of Technology (UTAUT) and the Technology Acceptance Model (TAM), both are popular models for predicting the adoption of technology by taking into account, end user perceived usefulness, perceived ease-of-use, and perceived cost of adoption and subsequent technology acceptance [1][5].

4.0 Methods and Materials

The objective of this paper is to analyze the impact of sensitivity to information disclosure on mobile payment adoption and describe the state of mobile payments usage within our sample. The merits and demerits of the current mobile payment landscape will also be explored and potential solutions will be suggested. In order to accurately understand the attitudes of the end user towards mobile payment adoption, the users were asked to complete a survey as well as an interview to understand their rationale for certain preferences. Each respondent's responses were quantifiably coded and then grouped into intervals based on the normal distribution curve of their sensitivity to the disclosure of PII (Personally Identifiable Information) and FSI (Financially Sensitive Information) in relation to their preferred payment method.

The survey was conducted on 138 respondents who were asked to confirm or reject the following six hypotheses that relate to mobile payments and information disclosure:

- Users of mobile payment technologies are more likely to have a higher sensitivity to PII disclosure than non-mobile payment users.
- Users of Apple products are more likely to adopt NFC payments as a method of payment.
- Users rank the disclosure of Personally Identifiable Information as **Sensitive**.
- Users rank the disclosure of Financially Sensitive Information as **Very Sensitive**.
- Computer Science students and Professionals are more sensitive to the disclosure of Personally Identifiable Information and Financially Sensitive Information) disclosure than other non-computing students and professionals.
- Users aged 22 – 30 (Generation Y), are more likely to adopt mobile payment technologies than other age groups.

Survey responses as well as the hypotheses were used in establishing' survey respondents' mobile payment preferences, in the context of their level of sensitivity to personal information disclosure.

The data were collected from a total of 150 surveys handed out between April 21, 2016 and June 3, 2016 to a diverse and reasonably representative group of mostly computing students from three New York City metropolitan area universities. The target population was mainly residents of the New York City metropolitan area. The majority were single individuals between the ages of 16 and 30 years old. The survey, which was designed using Google Forms, was distributed electronically and in hard copy. It consisted of 38 questions categorized as follows: general respondent information, computer experience/literacy, mobile shopping habits, mobile security habits, network security habits, and sensitivity towards personal information disclosure. The survey consisted of questions to group respondents by age, profession, education, and preferred payment methods. The section on sensitivity towards information disclosure consisted of ranking on the PII (including FSI).

Of the 150 responses, twelve were excluded from assessment because of incomplete data, reducing the number of considered responses to 138. The electronic survey responses were exported to a Microsoft Excel spreadsheet using the Fudok plugin while the hardcopy responses were manually put into Excel. In the Excel spreadsheet the survey response data were evaluated, converted to quantitative values, and subjected to initial statistical analysis before using the Minitab statistical software to perform further analyses. Google Docs and Microsoft Word were also used for word processing. The researched books and articles used in this study were primarily obtained from searches in the Association for Computing Machinery (ACM), Elton B. Stephens Company (EBSCO), and Wiley e-library databases. The key search terms included *mobile payments*, *Near Field Communication, personally identifiable information*, *mobile commerce*, and *mobile security*. In addition, specific internet queries were made to find current trends and statistics in the mobile payments industry. The cited publications were mainly dated from 2012 to 2016**.**

5.0 Calculations and Analysis of the Results

The quantitatively coded values from the information disclosure sensitivity section of the survey were tabulated as Personally Identifiable Information (PII) and processed by Statistical Analytics Software (SAS/STAT) tool to determine the mean, standard deviation, skewness, and kurtosis of the values. The coded response values pertaining to Financially Sensitive Information (FSI) were tabulated separately from the Personally Identifiable Information (PII) and the same descriptive statistics were computed. The PII and FSI values were then compared against the key sample parameters of gender, marital status, age group, educational status, and profession to generate tables and visually representative charts. In testing the hypotheses, appropriate categories were analyzed using one-sample z, two-sample t, and two-sample proportion tests.

5.1 *Survey Results*

Of the 138 valid survey responses, 55 (39.9%) were from females and 83 (60.1%) from male respondents. In addition, 44.2% of the respondents were between the ages of 22 and 30

(Generation Y), 40.5% were between the ages of 16 and 21(Generation Z), 13% were between the ages of 31 and 50 (Generation X), and the remainder was above the age of 50. Moreover, 67.4% of the respondents were users of mobile devices running the Apple IOS operating system while 32.6% were users of mobile devices with the Google Android operating system. In addition, 59.4% cited their highest/current educational level as undergraduate, 34.8% indicated graduate, and 5.8% indicated postgraduate education; whereas 73.3% were students, and 26.8% were professionals. Within the entire sample, 43.5% were enrolled/employed in computing and information technology fields, 17.4% were enrolled/employed in business, finance and marketing fields, 11.6% were enrolled/employed in liberal arts areas, 5.1% were employed in education and library fields, 5.1% were enrolled in social sciences disciplines, 4.3% were enrolled in the health sciences fields, and 4.3% were enrolled in physical sciences fields. The remaining 8.7% comprised of respondents from other fields such as Engineering, Customer Service, and Management (See Figure 4).

Regarding the respondents' most preferred payment preferences, 50% chose Credit Card, 34.8% chose Debit card, 9.4% chose Online Payment Services and 2.2% chose Near Field Communication and 3.6% chose Other (See Figure 5). On the other end of the spectrum, when asked about the least preferred payment preferences, 26.1% chose Cash Payment, 20.3% chose Near Field Communication, 15.2% chose Online Payment Services, 14.5% chose Credit Card, and 13% chose Debit card and the remaining 10.9% of respondents chose Other payment methods.

5.2 *Calculating the End-User Sensitivity to Information Disclosure*.

To measure the respondents level of sensitivity to revealing personally identifiable information (PII), each respondent was asked to select a level of sensitivity they would ascribe to revealing these data on a Likert scale with ratings of "Not at all sensitive", "A little sensitive", "Somewhat sensitive", "Sensitive" to "Very sensitive" for the following information: Name, Marital Status, Address, Income, Phone Number, Credit/Debit Card Details, Banking Details, Location Sharing, Social security number, Personal Photo. While most of these data are personally identifiable information (PII), the Credit/Debit card Details, Banking Details, and Social Security Number are financially sensitive information (FSI).

The responses to the level of sensitivity to disclosing PII were collated and quantified by assigning a numerical value to each Likert scale, with "Not at all sensitive" being assigned a score of 1, through "Very Sensitive" being assigned a score of 5. Therefore, the lowest possible aggregate score was 10, if the respondent rated all the information "Not at all Sensitive", and the highest possible aggregate score was 50, if the respondent rated all the information "Very Sensitive". After calculating each respondent's rankings, the lowest obtained score was 19 and the highest obtained score was 50. For the entire sample, the mean score was 39.536 and the standard deviation was 7.437.

The responses to the disclosure of financially sensitive information (FSI) were collated separately and quantified using the same Likert scale values and rating score combining methods as the PII. This resulted in the lowest possible respondent aggregate score of 3, and the highest possible aggregate respondent score of 15. After calculating each respondent's ratings, the lowest

obtained score was 3 and the highest obtained score was 15; score across the sample the mean was 14.210 and the standard deviation was 2.36.

Figure 1 is a chart of the frequency of ratings for the PII and FSI responses, while Table 1 is a summary of the average level of sensitivity of PII and FSI disclosure for a variety of respondent subsamples with their associated mobile payment adoption percentages.

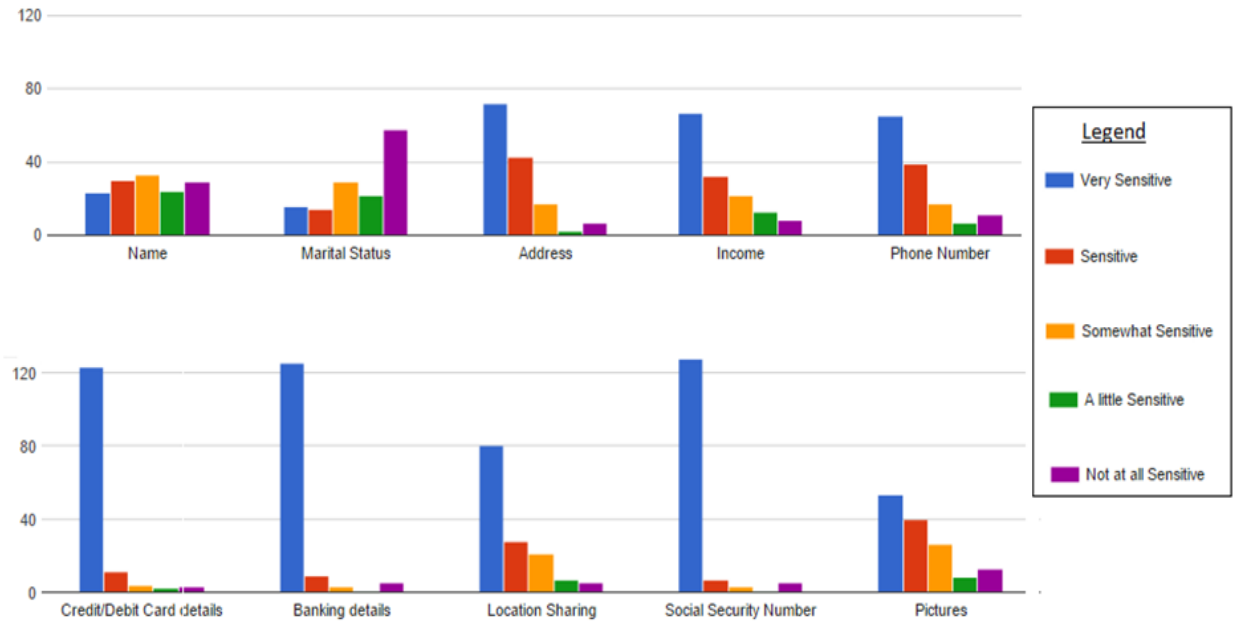

***Figure 1**: Frequency Distributions of PII and FSI Sensitivity Ratings*

In order to illustrate the results in greater depth, additional descriptive statistics such as percentile rank, kurtosis, and skewness were generated. These data are presented in Figure 2 as well as the mean, median, standard deviation, and confidence interval at 0.95 of each type of information. The normal curve distributions of the PII and FSI data with their corresponding standard deviations are presented in Figure 3. The distribution of the respondents' grouped according to their industry membership is illustrated and compared with each group's corresponding PII disclosure average sensitivity score in Figure 4. In Figure 4 the chart shows that respondents in the business related fields as well as respondents in the arts, liberal sciences, and health sciences higher average levels of sensitivity to personal information disclosure in than the PII overall mean sensitivity score to disclosure. Respondents in the computing and I.T. fields scored slightly less than the overall mean, while the subcategory of respondents in the engineering field had the lowest average sensitivity score to PII disclosure. Figure 5 shows the rank of the various forms of respondent payment preferences and the corresponding PII disclosure average sensitivity scores. From the Figure 5 chart one can infer that the respondents that preferred NFC payment and cash payment methods were more sensitive to disclosing their PII.

Table 1: Respondent Categories' Average Levels of Sensitivity to PII and FSI Disclosure with Associated MP Adoption Percentages

Respondent Categories		Average PII Sensitivity Scores	Average FSI Sensitivity Scores	MP Adoption Preference Percent		
				NFC (%)	Online Payments (%)	Total (%)
Gender	Male	39.169	14.301	2.4	9.6	12
	Female	40.091	14.073	1.8	9.1	10.9
Marital Status	Single	39.669	14.280	2.5	9.2	11.7
	Married	38.706	13.588	0	10.5	10.5
Age Group	<21	38.518	14.161	3.6	10.7	14.3
	22 -30	40.000	14.098	0	8.2	8.2
	31 - 50	42.111	14.722	5.6	11.1	16.7
	>50	33.667	14.333	0	0	0
Educational Level	Undergraduate	39.089	14.259	2.5	9.9	12.4
	Graduate	40.125	14.229	2.1	10.4	12.5
	Postgraduate	40.500	13.500	0	0	0
Profession	Student	39.143	14.129	2.0	9.9	11.9
	Professional	40.322	14.487	2.7	8.1	10.8
Industry/ Discipline	Education and Library	39.286	14.714	0	0	0
	Computers and I.T.	39.167	14.033	3.3	13.3	16.6
	Business and Marketing	40.792	14.667	0	0	0
	Arts	40.313	14.438	0	18.8	18.8
Mobile Phone OS	Apple IOS	39.699	14.280	2.1	8.5	10.6
	Android OS	39.386	14.091	2.3	11.4	13.7
Total Sample		39.536	14.210	2.2	9.4	11.6

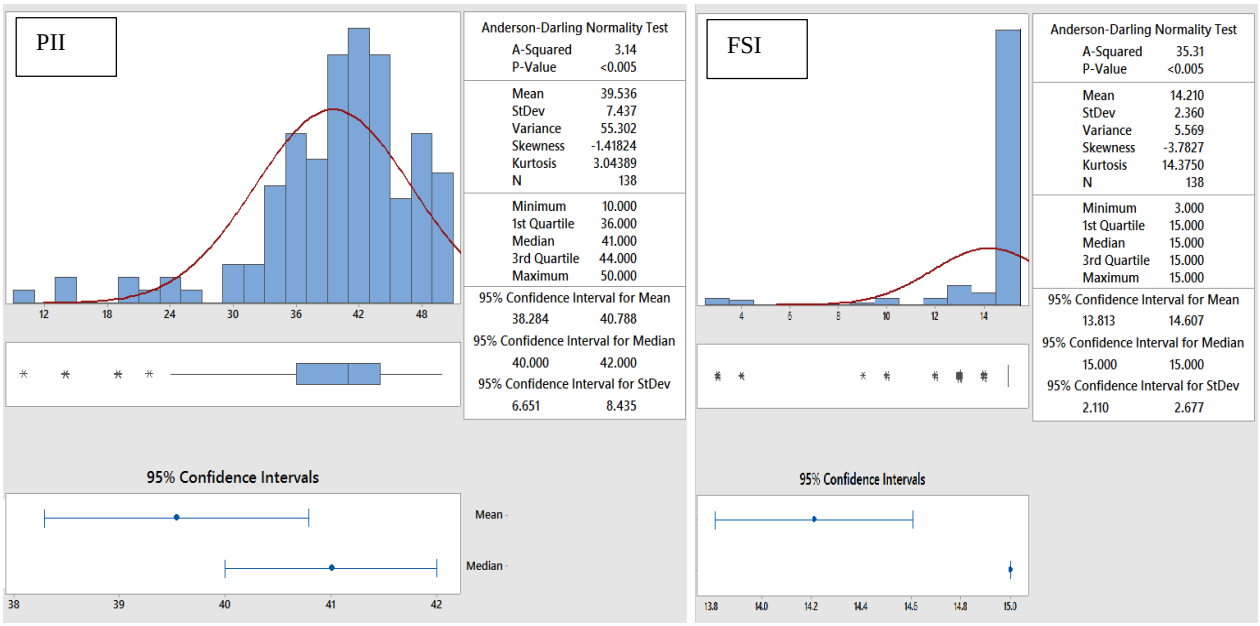

***Figure 2**: Descriptive Statistics of Total Sample PII and FSI Sensitivity Disclosure Data*

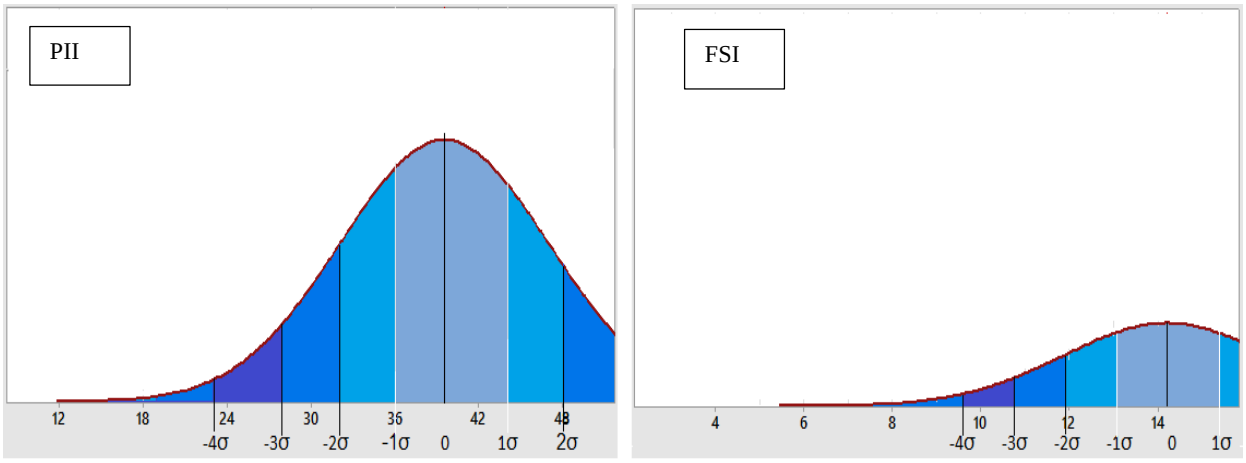

***Figure 3**: Normal Curve Distributions of Sensitivity Scores for Disclosing PII and FSI*

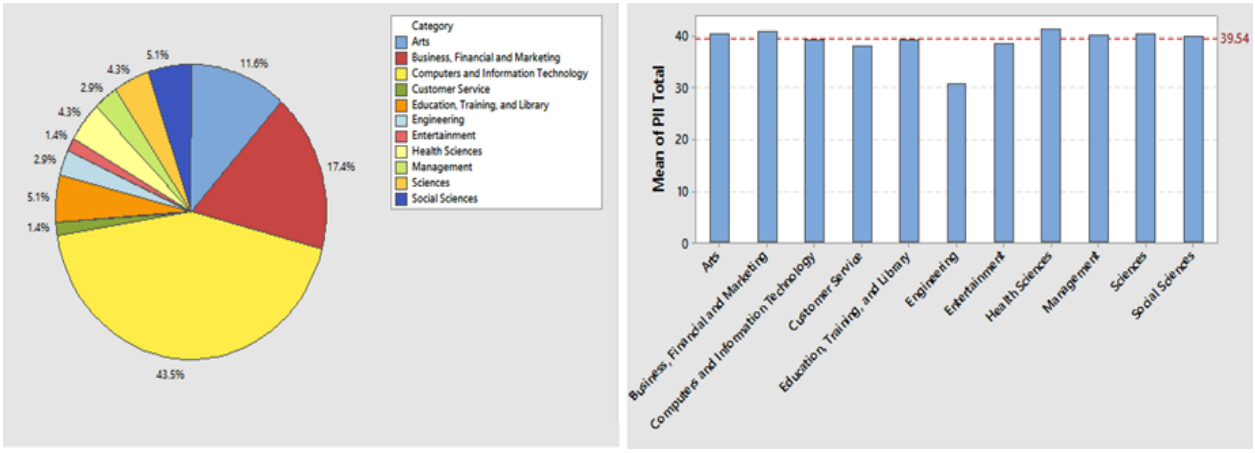

***Figure 4**: Respondent Occupational Groups with Associated Average Sensitivity Scores to PII Disclosure*

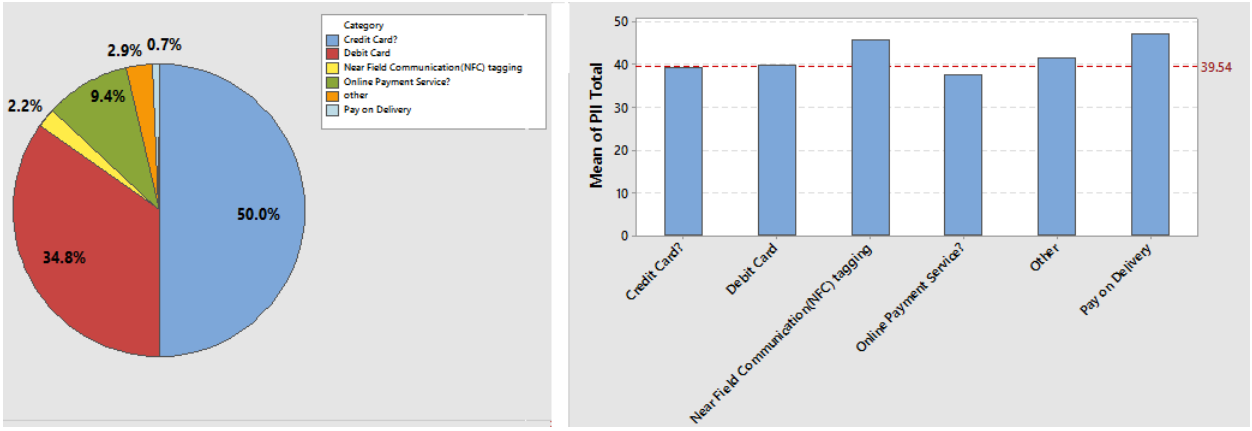

***Figure 5**: Respondent Payment Preference Groups with Associated Average Sensitivity Scores to PII Disclosure*

5.3 *Hypothesis Testing of the Survey Data*.

Average PII and FSI scores were used to test four out of the six study hypotheses: *(1) Users of mobile payment technologies are more likely to have a higher sensitivity to PII disclosure than non-mobile payment users; (3) Users of mobile payment technologies rank the disclosure of PII as Sensitive; (4) Users of mobile payment technologies rank the disclosure of FSI as Very Sensitive;* and *(5) Computer Science students and professionals are more sensitive to the disclosure of PII and FSI disclosure than other non-computing students and professionals.* For hypotheses 1 and 5 the two-sample t-test was used, for hypotheses 3 and 4 the one-sample z-test was used. The remaining two hypotheses *(2) Users of Apple products are more likely to adopt NFC payments;* and (*6) Users aged 22 – 30 (Millennials/Generation Y), are more likely to adopt mobile payment technologies than other age groups*; were tested using two–sample proportion tests. The summary of the results of the hypotheses tests is itemized in Table 2. For each test, the confidence interval was set at 0.95, and the significance level probability (α Value) threshold was set at 0.05 for the rejection of the null hypotheses.

Table 2: Summary of Hypothesis Tests

Hypothesis	***Test***	***α Value***	***p-Value***	***Conclusion***
Hypothesis (1) Users of mobile payment technologies are more likely to have a higher sensitivity to PII disclosure than non-mobile payment users.				
$H_o > H_a$	Two-sample t	0.05	0.238	ACCEPT Null Hypothesis
Hypothesis (2) Users of Apple products are more likely to adopt NFC payments.				
$H_o > H_a$	Two-proportion	0.05	0.019	REJECT Null Hypothesis
Hypothesis (3) Users of mobile payment technologies rate the disclosure of Personally Identifiable Information as **Sensitive**				
$H_o > H_a$	One-sample z	0.05	0.768	ACCEPT Null Hypothesis
Hypothesis (4) Users of mobile payment technologies rate the disclosure of Financially Sensitive Information as **Very Sensitive**.				
$H_o > H_a$	One-sample z	0.05	1.000	ACCEPT Null Hypothesis
Hypothesis (5) Computer science students and professionals are more sensitive to the disclosure of Personally Identifiable Information and Financially Sensitive Information disclosure than other non-computing students and professionals.				
$H_o > H_a$	Two-sample t	0.05	0.688	ACCEPT Null Hypothesis
Hypothesis (6) Users aged 22 – 30 (Millennials/Generation Y), are more likely to adopt mobile payment technologies than other age groups.				
$H_o > H_a$	Two-proportion	0.05	0.906	ACCEPT Null Hypothesis

These results statistically confirm that for this sample of respondents: (a) Users of mobile payment systems are more sensitive , than non-mobile payment adopters about the privacy of their PII; (b) The assertion that the entry of Apple into the mobile payment industry boosted mobile payment adoption among its users can be rejected; (c) The average mobile payment users' sensitivity to PII disclosure (based on this study's PII Likert scale) ranks at Sensitive; (d) The average users' sensitivity to FSI disclosure (based on the FSI Likert scale) ranks as Very

sensitive; (e) Computer science students and professionals are generally more sensitive to the disclosure of Personally Identifiable Information as compared to others; and (f) Users aged 22 – 30 (in the Millennials/Generation Y group), are more likely to adopt mobile payment technologies than other age groups.

6.0 Discussion

The results show the attitudes of the end users to disclosure of identifying and financial information, and link their preference for mobile payment adoption across a variety of subcategories. From the results, it appears that the majority of the sample takes seriously the risk of Personally Identifiable Information (PII) falling into the wrong hands and are especially more concerned about the privacy of their financially sensitive information (FSI) as illustrated in the normal distribution and summary charts (see Figure 2 and 3, respectively). Another observation is that the sample is relatively disinterested in adopting mobile payments, despite the many advantages they provide. One such advantage is the protection of the end-user's PII and another more important aspect is the security of the users' FSI, especially in relationship to the NFC payments. Despite the expanded efforts of the mobile payment service providers to increase the adoption of mobile payments, in this sample NFC payments only make up 2.2% of the respondents' preferred method of payment. Other forms of mobile payments, namely online payments accounted for 9.4% of the respondent's preferred payment method, making an overall total of 11.6% for mobile payment methods. Even more interesting is the percentage of users; 35.5%, that chose a mobile payment method their least preferred payment method. This is in contrast to the card payment methods, which had an overwhelming adoption preference of 84.8%. The pertinent question therefore is why are these users who seem so sensitive about disclosing their personal information, so opposed to the adoption of the payment platform that is best for protecting their PII.

Interview data from some of the respondents revealed that their rationale for non-adoption of mobile payment technologies was a lack of -information about the technology and its security and privacy of PII benefits. The interviewees that knew about these benefits said they had to do some personal research to find out more about the benefits. Hence, signifying that even with the dissemination of information about NFC payments, only the convenience and mobility factors were focused on. As part of the survey, users were asked what could be a source of discouragement to adopting a payment technology and the majority of the respondents (72%) chose "Payment information sharing" as their top concern.

Another reason why the end users might be hesitant to adopt mobile payment is the significant costs associated with some mobile payment technologies, specifically the NFC technology. The NFC capable devices, which are relatively new, are also high priced. This is not an issue when it comes to online mobile payment methods like QR codes and cloud based technology, because they can work on older and cheaper smartphones as well. When the interviewees were asked about their knowledge of online mobile payment technologies, all their responses indicated that they had heard about the technology in one of its popular forms, especially the PayPal and Starbucks applications. Most of the interviewees touted the efficiency of these mobile payment applications, as well as the targeting of deals and customer rewards as attractive features, but when asked why they do not use these applications their answers ranged from inconvenience,

uncertainty regarding the benefits of the payment platform, and mistrust of the platform regarding privacy of their personal information. It is noteworthy, that the privacy of personal information is a factor that encourages adoption in the NFC platform, but discourages adoption of online mobile payment platforms. This is reflected in Figure 5 which shows that adopters of NFC payment and cash payments are more sensitive towards disclosure of PII with a score significantly above the average PII, while the adopters of online payment were less sensitive towards the disclosure of PII, with the lowest score across all the payment preferences.

With regard to the distribution of the respondents by industry (see Figure 4), the respondents in the Business industry and health science industry are apparently more inclined to protect their PII, with a score above the average population score. Unlike the computer science industry respondents that scored below the overall sample average sensitivity score. This casts doubt on the assumption that computer science industry respondents should be more aware of the consequences of non-sensitivity to PII disclosure than other industries. A possible explanation is that the business industry understands the consequences of non-sensitivity in PII disclosure from a risk analysis standpoint. However, from the results of hypothesis 5's test the assumption that members of the Computer Science industry are highly sensitive to PII disclosure is an acceptable conclusion.

The hypotheses tests also confirm that end users are very much concerned about the disclosure of PII and especially sensitive to the disclosure of their FSI (see hypotheses 3 and 4) as corroborated multiple times in this study. Both assertions were deemed acceptable by the results of the hypotheses tests. The results of Hypothesis 1 prove that the prospect of PII privacy is a driver for mobile technology acceptance. While the results of hypothesis 6 confirm that the end-users in the Generation Y age bracket (Millennials) are more likely to adopt mobile payment for its advantages. The only hypothesis that was rejected was hypothesis 2, which asserted that Apple device users were more likely to have a favorable preference toward the NFC payment technology. This is noteworthy because, most of the interviewees had heard about NFC technology through the Apple Pay advertisements, but did not really see the necessity for adopting this mobile payment technology. As asserted earlier, the lack of focus on the security and privacy benefits of Apple's NFC technology may have been a reason for the non-urgency by the end users to adopt this technology.

After interviewing a subgroup of the respondents, I provided them with a brief lecture about the benefits, as well as the disadvantages of mobile payment adoption. After the lecture all of them had a more positive disposition toward the adoption of mobile payment technology. Some who had NFC capable smartphones asked for details on setting up NFC payment; others that already had NFC set up on their devices said they were going to use it more, and the remaining interviewees pledged to be more open minded towards possibly adopting mobile payments technology.

7.0 Conclusion and Further Research

Since the inception of the Mobile Payment technology, it has been predicted that it would become the dominant method of payment, replacing the existing electronic payment technologies, with as much as 1.0 billion users predicted for the technology by the end of 2015

[4]. However, that has not been the case; mobile payment adoption has fallen short of the predictions. While the technology has found success in East Asia and some parts of Europe, the adoption rate is relatively underwhelming in other regions [1]. The possible reasons for this lethargic adoption of the technology have been identified as cost, complexity, security and limited network externalities [4]. The mobile payment service providers have taken appropriate steps to boost the possible adoption by working on these factors that hinder the adoption and highlight the factors that could enhance the adoption.

One such factor is the security and privacy of personally identifiable information, which is a major factor that could boost the adoption of mobile payments technologies. Through a survey on 138 respondents in the New York metropolitan area this paper investigated the impact of information disclosure sensitivity on the adoption of mobile payments technology as well as identifies the need for a change in the information dissemination of the benefits of mobile payments technology by the mobile payments service providers. The results of the survey show a relatively high sensitivity to Personally Identifiable Information disclosure (PII) across subcategories of the survey respondents, and a low level of mobile payments adoption, especially with regard to Near Field Communication (NFC) payment technology. This finding is despite the recent proliferation of NFC capable devices by dominant mobile device companies like Apple, Google and Samsung, who are also relatively new entrants into the mobile payment industry. The results also indicate that most of the end users are under-informed about the benefits of mobile payments, specifically regarding these systems provision of enhanced security and privacy of PII. Hence mobile payments service providers are, encouraged to focus part of their marketing strategy on the security and privacy benefits of the technologies, as opposed to only communicating about the mobility and convenience benefits. This is because other electronic payment methods provide mobility and convenience, but the benefit of masking personally identifiable information is a unique and differentiating factor for mobile payments.

Further research will include conducting the survey on a larger, more diverse sample, to determine if there is positive correlation between PII sensitivity and mobile payment adoption. The research will also include studying the motivating factors for mobile payment adoption and examining the incentives in place to encourage the adoption of mobile payment technologies.

References

1. Daştan, İkram, & Cem Gürler. "Factors Affecting the Adoption of Mobile Payment Systems: An Empirical Analysis." Retrieved 8 Jan. 2017 https://www.researchgate.net/publication/292943809_Factors_Affecting_the_Adoption_of_Mobile_Payment_Systems_An_Empirical_Analysis.
2. Fumiko, Hayashi, and Terri Bradford. "Mobile Payments: Merchants' Perspectives." Retrieved 8 Jan. 2017: http://econpapers.repec.org/article/fipfedker/00014.htm.
3. Information Systems Audit and Control Association (ISACA). "ISACA Challenges Mobile Payment Security Perceptions". Retrieved 8 Jan. 2017: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Challenges-Mobile-Payment-Security-Perceptions.aspx.
4. Ooi Wei, Shen, and Rashad Yazdanifard. "Has Mobile Payment Finally Live Up to its Expectation in Replacing Cash and Credit?" Retrieved 8 Jan. 2017:

https://www.researchgate.net/publication/279205728_Has_Mobile_Payment_Finally_Live_Up_to_Its_Expectation_in_Replacing_Cash_and_Credit.

5. Slade, Emma, et al. (2015). “Exploring Consumer Adoption of Proximity Mobile Payments." *Journal of Strategic Marketing*, Vol. 2, No. 3, pp. 209-223.
6. Conick, Hal. "The Future of Cash: Should Marketers Plan for Mobile Payments?" Retrieved Feb. 2017: https://www.ama.org/publications/MarketingNews/Pages/future-cash-marketers-plan-mobile-payments.aspx.
7. Kujala, Sari, Ruth Mugge, and Talya Miron-Shatz. "The role of expectations in service evaluation: A longitudinal study of a proximity mobile payment service." Retrieved 8 Feb. 2017: https://www.researchgate.net/publication/308537095_The_role_of_expectations_in_service_evaluation_A_longitudinal_study_of_a_proximity_mobile_payment_service.
8. Ghag, Omkar, and Saket Hegde. (2012). "A Comprehensive Study of Google Wallet as an NFC Application." *International Journal of Computer Applications*, Vol. 58, No. 16, pp: 37-42.
9. Johnson, Abdulwaheed and Anthony Joseph. "Mobile e-Commerce Security: A Study of the End Users’ Security Perceptions." Retrieved 8 Feb. 2017: https://www.highbeam.com/doc/1P3-4223287051.html.
10. Hayashi, Fumiko. "Mobile Payments: What's in it for Consumers?" Retrieved 8 Feb. 2017: https://www.kansascityfed.org/publicat/econrev/pdf/12q1Hayashi.pdf.
11. Cobanoglu, Cihan, et al. "Are Consumers Ready for Mobile Payment? An Examination of Consumer Acceptance of Mobile Payment Technology in Restaurant Industry." Retrieved 8 Feb. 2017: http://digitalcommons.fiu.edu/hospitalityreview/vol31/iss4/6/?utm_source=digitalcommons.fiu.edu%2Fhospitalityreview%2Fvol31%2Fiss4%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages.
12. Dmitrienko, Alexandra, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. "On the (In) Security of Mobile Two-Factor Authentication”. Retrieved 8 Feb. 2017: https://www.trust.informatik.tu-darmstadt.de/publications/publication-details/?no_cache=1&tx_bibtex_pi1%5Bpub_id%5D=TUD-CS-2014-0015.
13. Slade, Emma L., et al. "Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust." Retrieved 8 Feb. 2017: https://www.researchgate.net/publication/275462723_Modeling_Consumers%27_Adoption_Intentions_of_Remote_Mobile_Payments_in_the_United_Kingdom_Extending_UTAUT_with_Innovativeness_Risk_and_Trust.
14. Groupe Speciale Mobile (GSM) Association. *The Mobile Economy 2016*. Retrieved 8 Feb. 2017: http://www.gsma.com/mobileeconomy/.
15. Master Card. *The Mobile Payments Readiness Index: A Global Market Assessment*. Retrieved 9 Feb. 2017: https://mobilereadiness.mastercard.com/globalreport.pdf.
16. Evans, Michelle. "5 Trends Shaping Mobile Payments Worldwide in 2016." Retrieved 9 Feb. 2017: https://www.mobilepaymentstoday.com/blogs/5-trends-shaping-mobile-payments-worldwide-in-2016/.