Safety vs Convenience in Modern Financial System: A Contactless Payments

Ibrahim Muhammad Hassan*

*Department of Computer Science, Hussaini Adamu Federal Polytechnic, Kazaure
Email: - ibrahimhass003@gmail.com

Contactless payments represent cashless payments that do not require physical contact between consumer card, mobile phone and point of sale terminals by the merchant. Contactless payment system is expected to bring the following benefits speed and convenience at POS and provides a greater level of customer protection compared to cash. These payment methods bring about reduction in in cash usage and its associated costs. a micro-chip is embedded in to the cards that hold personal and financial information used to make payment on transactions. The paper put more emphasis on security, risk and abuse of Ethical, Social, Legal and some professional issues.

Index Terms: Point of sales, Near Field Communication, Radio Frequency Identification

1 Introduction

In recent years contactless payments system has changed the way consumers make daily payment and increases their spending habit, due to invention such as online banking, credit, debit, prepaid-card and mobile payment among others. However, the system is faced with the threats from abuse of Ethical, Social, Legal and some professional issues. The payment systems are the credit cards, the debit cards, and other devices like smartphones and mobile devices, that use Radio Frequency Identification (RFID) or near field communication (NFC).The setup is based on making all the payments in a secured manner where the embedded chip and antenna are able to handle the waving of the card or the other devices (Dixon and Knauft, 2015).

In the case of contactless cards, a computer chip is embedded in to the cards that hold personal and financial information used to make payment on transactions. Nevertheless, RFID technology was used for mobile payment transmission. However, the contactless cards comprise a microcontroller (or equivalents) and internal memory which has the capacity to store, secure, and give access to information of the card. The card micro controller assists in enhancing the security feature such as authenticated data access and the privacy of the information. The traditional cards (plastics) can also be transformed to the new contactless cards. Meanwhile, other smart- cards gives the same ability but have no provision of radio frequency interface that would allow it to be read as fast and convenient at a very short distance from the reading device(Turk and Cosar,2015).

The most recent technology found in mobile sector is the Near Field Communication (NFC), this technology enable the mobile device to become a “secure wallet”(prevent electronic pickpocket), It is a transaction payment that involves no direct or physical contact between the merchant physical point of sale (POS) terminal and consumer payment gadget(Alliance, 2007). A customer holds his device contactless in a closed range of below 2-4 inches to the POS terminal of the merchant, thereby allowing the payment account information to be reached wirelessly through radio frequency. The transaction limit using the contactless card in the United Kingdom is currently £30. This paper investigates the impact of contactless payments, risk and security concern and management and lastly correlate the mentioned with the Ethical, legal, Social, environmental and professional issues.

2 Related Review:

According to Dahlberg et al., (2008), majority of published papers were only being able to cover some technical issues like that of systems architecture, protocols, and security and consumer centric study. However, this limited scope can be elaborated by the new emerging technology in mobile payment research, therefore, there are anticipation to see much in the coming years as research in this field is reaching a maturity stage. (Selvadurai, 2015), opposes the complete consideration of only technical issues in mobile payment but, put emphasis on Legal and Ethical Responsibilities in Mobile Payment Privacy, so its agreed that mobile applications have the technical capacity to get all the details of consumer non-public data, if the consumer authorized the mobile payment application to get his privacy data. Legally or ethically is not wrong to do so. But it's very vital to protect such data from reaching the unintended parties. This research is in line with the second argument of Selvadurai j in consideration of legal/ ethical issues in protecting the consumer interest. Although, (Valcourt, Robert and Beaulieu, 2005) realized that only few papers are evaluating the tremendous potentiality of near-field communication (NFC) technology.

However, based on the above findings, it was realized that is good to exploit the potentials of NFC in mobile systems but, agreeing with Dahlberg et by looking in to the technical issues such as protocols and architecture, in taking major role in security. This is because *Consumers* depends on: speed, convenience to be able to track spend as well as the confidence in security.

Similarly, *Merchants* also depend on the speed, spending, cost, and security of their transactions. The Card *Issuer* is inclined towards revenue generation and maintaining the security of consumer's cards. In a nutshell Merchants, Consumers and issuers must prioritize the technical issues and then consider the potentials in NFC.

RFID Technology was accepted and implemented all over the world and it has a considerable and diverse impact our daily life (Lacmanović, Radulović and Lacmanović, 2010).Those wide areas of RFID applications involves monitoring, maintenance of products, logistical tracking, product safety, information and the payment processes. Different countries in the world are applying different tracking of goods and securing the cards.

Security issues and threats are the major challenge of RFID an NFC technologies. But one thing to consider in contactless payment card provide a greater security to the convenience of the end users. When compared it with other different method of payment options, it offers more storage and security in terms of reading and writing data. Using contactless card in payments either debit/credit cards, some addition security were imposed via different series of electronic keys and encryption algorisms. So, when we asked ourselves how secure are contactless cards payments? Reasons is that payments using cards is safe and secure as making a payment with your PIN because both terminals and the contactless cards are with an embedded with of anti-fraud technology and information that is transferred between terminals is secure and difficult to intercept. When the card is used in proper terminal it lets dozens of information to be interchange between cards, the bank and terminal, as a result the layer conduct authentication, offline PIN verification and cryptographic for safer card-present transactions, however, fraudsters are not able to create counterfeit cards.

Contactless payments provide benefits to consumers for making their transaction faster at their convenient time, obviating need to take cash to stores, and provide coupon and gifts in electronic form then paper based which one can easily have forgot or lost and finally, allows the customer to keep track of expenditures incurred and a receipt.

3 Risks and security Concerns

Many payment vehicles are being targeted by the fraudsters which probably to be the mobile payments. So upfront an analysis and control are required to mitigate the risk of this double edge tool. Risk in case of mobile payments can be divide in to two Traditional or emerging risk. The tradition al include theft or denial of service, loss of brand reputation and revenue whereas the emerging risk affects the mobile payments in terrorist findings and money laundering. However, the bank-centric NFC model is one of the most widespread mobile payment in terms of implementation.

The participants in mobile payments ecosystem rely solely on the user, network provider or service provider (Chatain et al., 2008).in the assessment of the risk in mobile we have to consider their target, the risk identification, possible threats ,vulnerability and countermeasure as shown in the table below:

Table 1: shows risk and Management in Mobile payment

Target Type	Risk	Threats	Vulnerability	Control Measure
User	Repay attack, identity theft, information disclosure	Traffic interception	Transmission between (Point-of sale) POS and NFC reader	Encryption and secure protocol, trusted Module platform
User	Lack of 2-way factor authentication.	User impersonating.	Provider liability and transaction fraudulent.	2-way factor authentication.
User	Decrease in adoption of the technology, security obscurity.	The setup complexity and Configurations.	To replace the mobile phone or change it.	Use of security parameters set to be trusted
Service provider	Message altering, theft of service and replay.	impersonating attack: Altering POS.	POS machine setup at merchant's place	Secure authorization and accounting, POS vendor secure.
Service provider	Digital Piracy, Theft of data, risk for digital rights violation	Mobile machine user disclosed information illegally.	None digital right control (DRC) on the mobile machine.	Allow cryptography in DRC, DRC to be superimposed in smartphones TPM.
Service provider	Loss of revenue and theft of service, unauthorized transfer of funds.	Message alteration, fraud control evasion.	Flawless of GSM device. Transmission encryption of OTA: SMS data on the mobile network	Regular sending message authenticators, strong protocol for encryption.

The above table describe the risk assessment and management in relation to mobile payments in contactless payment.

4 Security concern in card contactless payments

Attacker holding Mobile terminal

The card is vulnerable to theft, an article figure 1 on YouTube video that shows attacker with point-of sale POS terminal /mobile card reader in his hand and come very near to the pockets, thereby taking money up to 30 GBP. t is requested that by keying an amount into the terminal and holding it against the pockets of unsuspecting cardholder, he could steal money out of their accounts via their contactless cards.

4.1 Solution to the above threat

Contactless card holders should wrap their wallet or card in tin foil as the foil repels the reader and shields the card in close range. Metal cardholders and lined wallets are available from retailers if you want something a bit sturdier. But, the best way of protection is to keep your purse or wallet in a separate bag and keep it out of sight at all times.

5 A consideration of social, legal, ethical, environmental, and professional issues:

5.1 Social issues

The impacts on social issues perhaps is seen the biggest change, utilizing mobile technologies to send, move and transfer money from one costumer to another. The customer takes advance of secure contactless payments in mobile and cards to make transactions by interacting between the point of sale (POS) terminals and their Devices and cards.

The social issue is also related to cybercrime where the criminals are exploiting the speed, convenience of the Internet to commit the diversified range of the criminal activities. From the technological point of view.(Selvadurai)

Electronic payment systems allow for much greater traceability. Whilst this is designed to reduce fraud, some consumers will still not feel comfortable about the security of their personal information. Complex fraud prevention systems can be difficult for users, with numerous passwords having to be remembered or stored somewhere. Mobile payment systems could make these processes a lot easier - the user enters their mobile number to a website, receives a text from the vendor and then simply confirms that the transaction is genuine by texting a reply.

5.2 Legal Issues

One of the most vital aspect of payment industries is securing the customer privacy (1) mobile and contactless payment are at its infancy the requirements for respecting privacy is not too clear. In section 501 of GLBA, financial institutions are obliged to protect the safety and privacy of their consumer's non-public individual information (Code, 1999).

501 forces financial institutions to ensure the security of the customer privacy data by creating suitable managerial, technical and physical protections.

5.3 Obligation to provide Notification

In UK Law section 502 of GLBA, financial service providers are required to inform customers about their information sharing practices, this must be done at initially stage when someone joins as a customer and annually thereafter(Code, 1999). Basically, financial service provider should reveal how the non-public information of the consumer will be disclosed to affiliated and non-affiliated organizations

- Banking system are responsible for ensuring security takes priority over convenience, when the consequences of convenience taking precedence would prove harmful.
- "Everyone has the right to respect for his private and his correspondence" A8 HRA Data Protection Act 1998 (legislation.gov.uk 2016)
- Insufficient regulation

- Applying existing laws to new situations does not always work

- EU has a task force with specialists to come up with EU wide tech specific law. (Specific policies)

5.4 Ethical Issues

At times, what law mean to achieve may not be justified with ethics motives. In contrast, enacting the law for the resolution of interpreting the law with the regards to the specific conditions. Ethical standard is flexible and subject to good moral reasoning by customer taking the action. If one ethically reason with the self and others for the actions taken, his ground remain legal will start the best behavior, provided the action may not be harm to others interest (Mandal, 2010)

Contactless payment concern on the customer's information, the duty to protect these information, checking their accuracy, and accessibility to them.

The ethics of payment focus on promoting the idea that sufficient security should be considered before convenience.

Some of the ethics using Contactless payments:

Building trust between customer and the Banking industry in terms of security, convenience and privacy etc.

5.5 Environmental Issues

There is a solid drive to diminish environmental impact. The formation of a supposed "paperless society" is a critical part to plan and make it possible. Of the arrangements to make this conceivable. Some government while in power outline plans for some public services to be conveyed by advanced means, bringing about a decrease in the utilization of paper and wood, however maybe more essentially genuine money related advantages. This pattern is further strengthened through the Conservative pre-election vow to present rapid broadband all through the UK and more extensive worldwide activities.

Reduce the drive to the bank which in turn reduce environmental pollution produced by the vehicle exhaust, to the bank building. (Jon Wyllie, 2010)

5.5: Professional Issues

The major challenge in contactless payments security, here experts must enter vain not only those professional in the field of information technology also those people that are experts in the fields of modern financial market system. Together to address the issues of security threat regarding payment systems professionally

5.5.1 Security: The biggest security fear is the theft of consumer credit card or personal information in one of the following ways such as phasing, sniffing and false identification and control the information flow to the wrong hand. Security matters to companies - not just consumers, because poor security results in loss of consumer trust and loss of their business.

This security also helps to bring more trust, more customers, more benefit and less disadvantageous. (Moreton et al., 2015).

Conclusion

Contactless payments improve the security and convenience of identity verification and payment transactions. The use of NFC/RFID Technology not only creates a great method for mobile payments and data communications, but it also allows these experiences to be extended and create vision of future. Contactless chip technology enables strong security features along with convenience, durability, flexibility and reliability.

7.0: References:

Alliance, S. C. (2007) 'Contactless Payments: Frequently Asked Questions', *CPC-07001, February*.

Chatain, P.-L., Hernández-Coss, R., Borowik, K. and Zerzan, A. (2008) 'Integrity in Mobile Phone Financial Services', *World Bank Working Paper,* (146).

Code, U. S. (1999) 'Gramm-Leach-Bliley Act', *Gramm-Leach-Bliley Act/AHIMA, American Health Information Management Association*.

Dahlberg, T., Mallat, N., Ondrus, J. and Zmijewska, A. (2008) 'Past, present and future of mobile payments research: A literature review', *Electronic Commerce Research and Applications,* 7(2), pp. 165-181.

Dixon, P. B. and Knauft, C. L. 2015. Association of contactless payment card primary account number. Google Patents.

Lacmanović, I., Radulović, B. and Lacmanović, D. 'Contactless payment systems based on RFID technology'. *The 33rd International Convention MIPRO*, 24-28 May 2010, 1114-1119.

Mandal, S. K. (2010) *Ethics In Business & Corp Governance.* Tata McGraw-Hill Education.

Pasquet, M., Reynaud, J. and Rosenberger, C. 'Secure payment with NFC mobile phone in the SmartTouch project'. 2008: IEEE, 121-126.

Selvadurai, J. 'Legal And Ethical Responsibilities In Mobile Payment Privacy'.

Turk, I. and Cosar, A. 'Having 4G, enabling cloud based execution for NFC based financial transactions'. 2015: IEEE, 63-67.

Valcourt, E., Robert, J. M. and Beaulieu, F. 'Investigating mobile payment: supporting technologies, methods, and use'. *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.*, 22-24 Aug. 2005, 29-36 Vol. 4.