Challenges and Risks of Developing a Payment Facilitator Model

Mohammed Alsadi[1], Haci Ali Mantar[2]
Gebze Technical University
Turkey
mehmet.alsadi@gmail.com
hamantar@bilmuh.gyte.edu.tr

Vedat Coskun[3], Kerem Ok[4], Busra Ozdenizci[5]
Isik University
Turkey
vedat.coskun@isikun.edu.tr
kerem.ok@isikun.edu.tr
busra.ozdenizci@isikun.edu.tr

ABSTRACT: *Following traditional payment methods using banknotes, credit and debit cards enabled significant increases in consumer spending power. The traditional way for consumer to purchase a service or an item in a shop is by presenting their –physical- credit card on a point of sale (POS) device, which is called as Card Present (CP) transaction. Motivated by the growth of Internet and Smartphones, e-commerce became a reasonable alternative for timesaving purchasing activities. Significant growth in the e-commerce market has been observed through the world especially in the recent years. Remote transactions where the customer does not physically present her credit or debit card during payment are termed Card Not Present (CNP) transactions. CNP includes mail order, telephone and internet transactions. The main advantage of CNP transaction is easying the customer's shopping experience, since the customer can buy anytime and anywhere without the need to physically present the payment card. In order to maximize the efficiency of CNP transactions, a payment facilitator is needed to sponsor retailers. It frees retailers from the need to perform the administrative procedures necessary with the acquirer. The aim of this research study is to identify the challenges and risks to developing a secure methodology to provide secure CNP-based transactions with a payment facilitator. We analyse and use the requirements imposed by regulators, identify detailed security requirements for a mobile payment system, and develop a roadmap for developing a secure methodology for mobile payment transactions.*

Key words: Payment Systems, Mobile Payment, Payment Facilitators, CP, CNP, Fraud, Security, e-commerce, m-commerce, NFC.

Received: 12 January 2016, Revised 18 February 2016, Accepted 23 February 2016

1. Introduction

Developments on the Internet have re-shaped our life. Traditional actions in almost every aspect of our life are changing to electronic version. Such events have gained a lot in popularity, mainly due to the ease of use and widespread of supporting technologies. E-commerce is one of the fields that have been affected by such progress. Billions of dollars are spent and

exchanged throughout the Internet nowadays.

E-commerce sales are classified into 4 main categories [1]. The first one is Business-to-Consumer (B2C) in which companies sell their online goods and services to end consumers. Consumer-to-Business (C2B) is the second category in which consumers post their products or services online waiting for suitable bids from different companies. Third category is Business-to-Business (B2B), in which companies sell their products or services to other companies. The last category is Consumer-to-Consumer (C2C) in which consumers sell their online products or goods to other consumers.

E-commerce success mainly depends on electronic payment systems. Such systems are used to transfer an electronic value of payment from payer to payee through some kinds of electronic mechanism. Electronic payment can be roughly defined as an online financial exchange that takes place between buyers and sellers. The content of this exchange is usually in some form of digital financial instruments such as encrypted credit card numbers, electronic checks and digital cash. In 2014, retail e-commerce sales amounted to 298.26 billion US dollars and are projected to grow to 481.94 billion US dollars in 2018 [2].

Later on, the progress in Smartphone sector led to changes in the previously used electronic payment systems and the introduction of mobile commerce (m-commerce). M-commerce can be defined as buying and selling transactions in which consumers can use their mobile devices such as Smartphone or tablets to buy or sell goods and services. E-commerce and m-commerce have some similarities; but m-commerce has its own unique characteristics such as mobility, short response time, and simplicity [3, 4].

In 2002, Varshney and Vetter [5] proposed a framework for m-commerce that allowed developers and providers to strategize and effectively implement mobile commerce applications. Several new classes of applications reviewed networking requirements, and discussed application development supports that are considered as the beginning of m-commerce.

The aim of this study is to identify the challenges and risks when building a payment facilitator model. When the intended payment facilitator model is developed, it will provide commercial gain to retailers and provide an easy payment method to users. The rest of this paper is organized as follows. Section 2 presents the literature review on the related topics. Section 3 discusses payment facilitator model and the related security considerations. Finally the study is concluded in Section 4.

2. Literature Review

Wherever Transactions occur in situations in which card and cardholder are present at the time of sale are called as Card Present (CP) transactions. While transactions occur with the absence of card or cardholder at the time of sale are Card Not Present (CNP) transactions. Some examples are mail order/telephone orders (MOTO) and online credit card payments via virtual Point of Sale (POS) machines. CP transactions are easier to manage, since presenting the identity of card and cardholder at POS provides inherent security. On the contrary, in CNP transactions the physical authentication of the cardholder is not possible; hence different authentication mechanisms are required. For example, an m-commerce transaction between a consumer and a merchant through the merchant's website is a CNP transaction. In CNP transactions, there is no opportunity to physically check the card to ensure the authenticity or identity of the cardholder. Therefore, payment fraud is a risk that is always associated with CNP transactions.

EMV® is a global standard for credit and debit payment cards based on chip card technology. The name comes from first letters of the major payment companies: Europay, MasterCard, and Visa [6]. In EMV cards data are stored on integrated circuits rather than magnetic stripes, although many EMV cards also have stripes for backward compatibility. During EMV card transaction a contact is made between the chip on the card and the chip reader in a terminal such as POS terminal. This type of connection is either contact; in which a physical contact occurs between the card and terminal chip or contactless; in which the card must be within a specific range near to the terminal. Payment transactions of EMV cards are accomplished through three stages: [7]

- Card authentication in which terminal checks the authenticity and legitimacy of the card.
- Cardholder verification, in which the cardholder is verified to the terminal by comparing the PIN code entered by the cardholder with the one found on the card.
- Transaction authorization, ensuring that the issuing bank approves the whole transaction.

The process of payment in which credit or debit cards are used includes interactions between different actors (consumer, merchant, acquiring bank (merchant bank), issuer bank (consumer bank), and card association). First, consumer asks the merchant to complete purchase using his/her card. Through POS founded at merchant, the transaction data is collected. The data is sent to the acquirer bank and then the acquirer bank forwards the transaction data through card network to the issuer bank who responds by approving or declining the transaction. The response is sent back to the acquiring bank through card network, then it reaches merchant.

According to [8], electronic payment systems can be classified into four types.

- **Credit Cards:** Payment cards are issued to users as a method of payment. Users can pay using their credit cards based on their promise to pay it again later to the card issuer. This method is the most frequently used among the others (Chou et al. 2004). Issuing companies need to agree with merchant to accept their cards. Card verification is needed to accomplish transaction done by such cards.
- **Debit cards:** These cards depend on the money funded in the consumer's bank account. In other words, debit cards provide consumer with an online access to their accounts. Payments using a debit card are immediately transferred from the cardholder's designated bank account.
- **Pre-paid cards:** These cards are loaded with some amount of money by the consumer. They look like any credit or debit cards with a card number, signature strip and company brand. They are usually used in store-based transactions. They are different from debit cards since they are linked to a bank account with an overdraft facility. This is because consumers can't borrow money with a prepaid card - they can only spend money they have loaded onto it. In [9] pre-paid cards are defined as "There are many types of prepaid cards available for different purposes. You'll see gift, travel and everyday money cards, to name but a few but they all share the same benefit of being safer and more convenient to use than cash".
- **Electronic-cash:** Usually used for micro payments (i.e. payments which is subject to small amount as 35 TRL). In this method a unique identification number is associated with a specific amount of money. In order to use this method consumers purchase digital cash from issuing banks. E-cash scheme has three main elements: the issuing bank, a set of merchants, and users. A wallet of electronic coins is withdrawn from the issuing bank based on user's request, and then users spent them to purchase goods from merchants. Later merchants are able to deposit the collected coins to their banks. Double Spending is the major problem in E-cash; coins can be easily duplicated.

Transactions in remote payment cases in which the consumer and merchant are not interacting face-to-face are also defined as CNP transactions. The payment credentials related to both card and cardholder maybe entered through digital input methods such as PC keyboard or through a mobile device. On one hand, the introduction of CNP makes it much more attractive and useful for both consumer and businesses. Consumers can easily order goods or services any time anywhere if Internet connection or telephony service is available. For businesses, CNP exceeds the geographical boundaries of their locations, thus increase buying activities. On the other hand, since authentication of card/cardholder is not possible physically, the possibility of frauds is higher than CP transactions. Frauds in CNP involve the unauthorized use of card/cardholder data (card number, card expiration date, etc.) to accomplish the transactions. Identity authentication is the process of ensuring that the data used for a transaction is given by the owner of the account. In other words, it is ensuring that the person claiming that he/she is the cardholder is in fact the real cardholder. According to some studies [10, 11], at least two of the following authentication factors must be provided by any person wishes to accomplish a CNP transaction:

- Something the person has (ownership factor) such as credit card.
- Something the person knows (knowledge factor) such as PIN.
- Something the user is or does (inherence factor) such as fingerprint.

Combinations of these factors are called two-factor authentication (2FA) where two factors are deployed. Till now, there is no commonly accepted authentication standard for CNP transactions. Nowadays, many methods are in use such as PINs, address verification, Card Verification Value (CVV), One-Time Password (OTP), tokens, voice verification, security questions.

Mobile technology has become increasingly common in today's everyday life. Besides the great development in Internet, mobile sector is also recording an amazing progress. According to The Mobile Economy 2015 [12], the mobile industry

continues to scale rapidly. At the end of 2014, the number of mobile subscribers was about 3.6 billion. It is predicted that by the end of 2020 this number will increase by at least 10 billion taking the global penetration rate to approximately %60. It is nowadays possible for Smartphone users to purchase goods or services, transfer money, or pay for bills using their mobiles. The volume of transactions accomplished through mobiles is huge and it is increasing massively. According to Forrester [13] U.S. mobile payments will reach $142 billion dollars by 2019. Mobile payment has become much easier and highly recommended by consumer s. Samsung, Apple, and Google have developed their own mobile payment systems and have released them to be used by their consumers.

Mobile payment systems generally have a number of entities cooperate with each other to accomplish the required work. These entities are the same as those used in traditional payment process; furthermore, new actors have been introduced such as mobile network operator MNO, Mobile Payment Service Provider MPSP, and payment gateway that is used for payment-clearing purposes. During mobile payment transaction, an authentication mechanism between virtual POS and mobile may be required. This could be achieved using Over-The-Air (OTA).

In [14], a detailed study about mobile payment types and their security and threads has been done. Mobile payment systems can be divided into five categories:

- **Mobile Payment at the POS:** Consumers are able to pay with their smart phone at the POS. Near Field Communication (NFC) is one of the commonly used techniques. There are many applications that use the card information to complete transactions conducted in this category.
- **Mobile Payment as a POS:** This method allows merchants to use the mobile as a POS to process card payments. Some applications have to be installed before start working. Square Register [15] is an example of such applications.
- **Mobile Payment Platform:** It provides online payment services on a mobile device. A mobile application that is linked to a bank account or credit/debit card account must be installed on the mobile. PayPal [16], BKM Express [17] are examples of this method.
- **Independent Mobile Payment System:** This method is similar to the previous one with one main difference in which the system can be used just for a special company.
- **Direct Carrier Billing:** This method does not require a bank account or credit/debit card account. Consumers are able to purchase what over they want through the Mobile Network Operator (MNO). The cost of the purchase is added to the consumer's monthly phone bill. To get such a system works; an agreement between merchants and MNO must be achieved. Completing the transaction is done through SMS; a consumer enters his/her mobile number to make a purchase then a code is sent via SMS to the specified number. The transaction is successfully confirmed if the consumer enters the correct code.

Since mobile technologies rapidly keep evolving, new forms of payments have been emerged. NFC is one of the emerging technologies that allow consumers to use their Smartphones as a wallet to accomplish payment transactions. Mobile payment transactions within NFC enabled devices can be made in two forms. Using the mobile secure element (SE) and through host card emulation architecture (HCE).

3. Payment Facilitator Model And Security Considerations

A payment facilitator or formally Payment Service Provider is an entity that takes legal responsibility for funds in the process of directing them from buyers to sellers. The payment facilitator signs a merchant acceptance agreement on behalf of the acquirer [18].

Payment Facilitator is an optional model for participating in well-known card issuers (Visa, MasterCard) acquiring. It is designed to provide an alternative model to acquirers and small merchants, different than the traditional acquirer-merchant direct relationship. Payment facilitator provides a new business model to small merchants with the opportunity to accept credit cards, debit cards, pre-paid cards, and contactless payment. It collects transactions on behalf of the acquirer, and performs real transaction with the acquirer itself.

In traditional model illustrated in Figure 1, the acquirer has a direct relationship with the merchant, so the funding process is done directly between them after transactions occurred and as a result the value of accomplished transactions is transferred to merchants. In models which use payment facilitator as shown in Figure 2, a third actor as a payment facilitator is utilized to enter

into agreement with small merchants (called sub-merchants) and collects transactions for them on behalf of the acquirer. Sub-merchants are merchants that processes transactions with assistance from a reseller (aggregator, PSP, payment facilitator), who is playing the role of an intermediary.

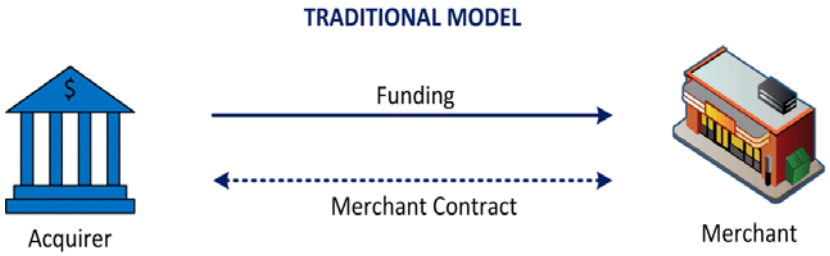

Figure 1. Traditional Model

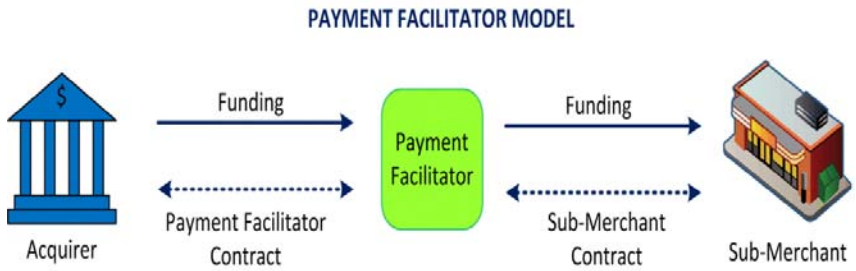

Figure 2. A model uses Payment Facilitator

In most cases, it is difficult for small merchants to make agreement with an acquirer to accept CNP payments. Regardless to the merchant size and transaction volume, the administrative efforts (underwriting, processing, funding) needed to service a merchant are the same. The payment facilitator connects them together in way that benefits both. The acquirer makes an agreement with the payment facilitator (as a merchant) who also makes agreement with sub-merchants. The acquirer and sub-merchant must be located within the same area of use, while the payment facilitator can be located anywhere.

The payment facilitator model is a win-win model for all actors within the ecosystem. For consumers, such a model makes it possible for them to complete payment transactions using alternative payment methods. Payment facilitators can offer innovative payment methodologies for consumers. Payment facilitator gets commercial benefits from commission obtained from sub-merchants. Moreover, it becomes better for sub-merchants to use the payment facilitator rather than getting their own virtual POS because of the lower commission that payment facilitator requests. Another benefit for sub-merchants is that they can propose innovative payment methods to consumers and improve customer satisfaction.

3.1 Security Requirements for Payment Facilitator Model

Sensitive data is transmitted transferred among the actors during payment; thus secure communications and transfer of such data is required [19]. After significant studies of academicians and professionals, the security risks of CP transactions became almost negligible. On the contrary, significant security risks still exist in CNP transactions [20, 21, 22].

CNP based mobile payment transactions are open to fraud and non-repudiation and companies lost huge amount of money due to fraud in CNP transactions. As an example; according to the statistics published by the UK Card Association between January and June 2015 fraudulent CNP transactions cost a total of £249.9 million [23].

Fraudsters often use stolen account information to reach others accounts. There are some signs that could be found or noticed in fraud transactions [24] such as:

• Before the cardholder notices that her card has been compromised, fraudsters try to make large transactions to maximize their opportunity.

• Fraudsters often try to purchase large quantities of the same item such as jewelry.

• International shipping, fraudulent transactions are generally shipped outside (i.e. to another country).

• Run multiple transactions on a single card in a short period of time in order to gain as much as possible of the card's value.

• Multiple card accounts are used to buy something from the same IP.

Payment fraud is a serious assault that causes billions of dollar loss each year. Furthermore, fraudsters use recently developed techniques and methods for obtaining cardholder's personal and financial information. A report released in May 2016 by AiteGroup indicates that card fraud cost in US is about $4.5 billion [25].

The authors of [26] described an overview of the various types of payment frauds and provided suggestions to reduce the probability of fraud occurrence. Those frauds could be summarized as the following:

• **Lost or Stolen Wallet:** Credit/debit cards are generally carried in wallets. Most fraud is often a result of this type.

• Shoulder Surfing: This fraud is used specially in crowded places in which it is easier to observe someone while accomplishing payment transaction.

• **Mail Theft:** Fraudsters obstruct mail to steal new credit/debit cards.

• **Data Breaches:** Hacking is a popular technological method used by fraudsters to get access to databases in which sensitive data about consumers and their bank account are stored.

• **Inside Sources:** Personal data can be obtained from dishonest employees in some cases.

• **Skimming:** One of the most commonly known type of payment card frauds in which fraudsters try to copy or capture the data from the magnetic tape of the card.

• **Phishing:** This fraud involves creating emails that appear as if it is from legitimate existing businesses. These emails are sent to consumers and then consumers are directed to fake websites that require them to enter sensitive data.

• **Social Networking:** Hackers and fraudsters use social media websites in order to obtain some useful information.

On the other hand, the transaction of the data between merchant and acquirer is also an important concern for payments. In CP payments, it is easier to secure the communication, since there is generally a placed device (e.g. POS device) for reading card data. Communication between acquirer and POS device is encrypted with the embedded keys in this device. However, securing CNP payments are not this easy, since there isn't any pre-placed device in the environment. Some methods to ensure the security of CNP payments are as follows:

• **Fingerprint:** In order to authenticate the user, Smartphone scans the fingerprint.

• **SSL/TLS:** SSL/TLS is commonly used for securing the transaction between host computer and the server.

• **Multi-factor authentication:** An additional secure code is sent over the consumer's registered mobile number or mail address, and this code is required to accomplish the transaction. If the right code is used, then transaction is authenticated otherwise it will be aborted.

In [27], authors emphasize an important subject: "It is important to bear in mind that fraudsters have no scope; they will try to attack your payment system from any angle". In the same work, authors also recommend three principles for secure mobile payment systems:

• **Protect (PT) from attacks:** Several measures can be applied in order to increase the difficulty of attacking the mobile payment system.

• **Detect (DT) fraud:** No matter how secure the payment architecture is, there will still be fraud attempts; measures have to be applied for fraud detection.

• **Prevent (PV) fraud:** Detection shall be accompanied by valid fraud prevention measures.

In another study on mobile payment systems' security [14]; authors state that malware, vulnerabilities of SSL/TLS, and data breaches are the main threads to mobile payment systems. Malware on mobile devices includes activities such as instant messaging, recording calls, GSP locating, forwarding call logs and many others. The data obtained from the aforementioned activities can be used later to attack mobile payment systems.

After analyzing the existing studies in the literature; following security requirements are identified for the targeted payment facilitator model:

• **Authentication:** Authentication will assure that the communicating entity is the one that it claims to be.

• **Confidentiality:** Since sensitive data is involved in payment transaction data must be protected against unauthorized access. Confidentiality is used as a measure to see our model's ability to protect consumer's sensitive and important data.

• **Integrity:** The model must make sure that the received data is identical to the originally sent one; no modification takes place during the transmission.

• **Non-repudiation:** The model must be able to prove that the consumer is authenticated securely at the time of transaction, and the data is not modified. Thus, a consumer will not be able to deny the payment transaction that she performed. Additionally; two-factor authentication mechanism must be used to make it not possible for consumers to deny transactions accomplished by them, and also to support regulations.

Within a payment system, a number of connections and data transmissions between different parties take place, so end-to-end security is a must. The communication should be secure enough so that no one can actively or passively affect the communication at any stage. Cryptography techniques played a great role in satisfying the model's security requirements. Further, key exchange protocol between the different entities is very important to ensure the security of the whole system.

3.2 Risks

Payment transactions involve many steps from the point where consumers start providing their information until receiving the voucher. Payment systems must be robust and secure enough to protect and prevent sensitive data from any attacks or attempts at any step. The most obvious point is that at some steps, data is transmitted over unsecure networks so much more attentions should be paid to such situations.

In [28], authors stated that GSM protocol has weakness in the security of its identifiers, which makes it possible for cloning. Cloning is one of the serious attacks in which attackers try to copy a consumer's SIM, and then uses it for financial transactions. Cloning could be performed either physical operation in which a SIM should be read by a kind of SIM reader, or over the air by exploiting weakness of standard GSM communication. The SIM card contains several unique identifier keys used to subscribe to the GSM network and these keys include secret individual subscriber authentication key (Ki) of the SIM, along with the International Mobile Subscriber Identity (IMSI) and Integrated Circuit Card Identifier (ICCID). SIM cloning involves extracting SIM identifier values and programming them into another chip card, creating a duplicate of the original SIM.

Many other risks could be occurred during Over-the-Air transmission such as identity theft, information disclosure, and replay attacks. A solution to OTA weakness and vulnerabilities is to use a trusted platform module (TPM) along with secure protocols [29].

Absence of two-factor authentication is another problem, which leads to fraudulent transactions. On one hand, transaction orders could be accomplished without knowledge of the consumer. One the other hand, in some cases consumers conduct a transaction and then claim the transaction is not accomplished by them, thus companies are not able to get the value of such transactions.

4. Discussion And Conclusion

Mobile communication continues to evolve and improve, leading to introduction of new technologies which offer attractive business opportunities. At the same time consumers are seeking for a good implementation which is secure enough to get

benefits from the newly introduced technologies.

There are several challenges related to payment systems [30]:

• **Cloud Computing**: Cloud technologies enable to store credentials about consumers somewhere in the cloud. Both consumers and merchants must download the cloud-based application and subscribe to the service in order to be able to use it. Despite the benefits obtained from clouds, there are some security issues remains with no answers.

• **Wireless connections:** End-to-end security solutions adopted by cellular networks are not secure enough to convoy latest technologies. Thus they will not be able to support future secure m-payment systems and applications.

• **Performance:** Since wireless environment is not secure, improving the security of payment systems by increasing or using huge computations will need more performance in host computers and servers.

Consumer's dependence on mobile and associated internet facilities is increasing rapidly. New models are introduced to them especially in mobile payment field. In this study a comprehensive analysis of existing payment systems and their security issues have been analyzed. Performed studies will be used to develop a secure and innovative payment facilitator model are unavoidable.

References

[1] Cucinotta, A., Pardolesi, R., Van den Bergh, R. (EDs.). (2002). Post-Chicago developments in antitrust law. Edward Elgar Publishing.

[2] US retail e-commerce sales forecast, available online at : http://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/

[3] Siau, K., Ee-Peng, L., Shen, Z. (2001). Mobile commerce: promises, challenges, and research agenda. *Journal of Database Management,* 12 (3) 4.K. Elissa, Title of paper if known, unpublished.

[4] Serenko A, Bontis N (2004) A model of user adoption of mobile portals. *Q J Electron Commer* 4 (1) 69–98.

[5] Varshney, U., Vetter, R. (2002). Mobile commerce: framework, applications, and networking support. Mobile networks and Applications, 7(3) 185-198.

[6] What is EMV Chip Technology ? Available online at : https://www.level2kernel.com/emv-guide.html.

[7] A Guide To EMV chip Technology, Available online at : https://www.emvco.com/best_practices.aspx?id=217

[8] Kim, C. (2009) An empirical study of consumer s' perceptions of security and trust in e-payment systems.Electron. Comm.Res. Appl, doi:10.1016/j.elerap.2009.04.014..

[9] What are Pre-paid Cards, Available online at : http://www.maestrocard.com/uk/prepaid/about.html

[10] Card-Not-Present Fraud: A Primer on Trends and Authentication Processes, available online at : http://www.emv-connection.com/downloads/2014/01/CNP-WP-012414.pdf

[11] Banka ve Kredi Karti Ýþlemlerinde Kullanýlan Bilgi Sistemlerinin Yönetimi Hakkýnda Teblið Taslaðý, Available online https://www.bddk.org.tr/websitesi/turkce/Mevzuat/Duzenleme_Taslaklari/13479karttebligi.pdf

[12]The Mobile Economy 2015, available online at : http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf

[13] US Mobile Payments Forecast 2014 To 2019, Available online at : https://www.forrester.com/report/US+Mobile+Payments+Forecast+2014+To+2019/-/E-RES115498

[14] Wang, Y., Hahn, C., Sutrave, K. (2016). Mobile payment security, threats, and challenges. *In*: 2016 Second International Conference on Mobile and Secure Services (MobiSecServ) (p. 1-5). IEEE

[15] Square Register, available online at: https://squareup.com/global/en

[16] PayPal, available online at: https://www.paypal.com/

[17] BKM Express, available online at: https://bkmexpress.com/

[18] Visa Payment Facilitator Model. Available online at: https://usa.visa.com/dam/VCOM/download/merchants/02-MAY-2014-

Visa-Payment-FacilitatorModel.pdf

19] Kadhiwal, S., Zulfiquar, A. U. S. (2007). Analysis of mobile payment security measures and different standards. *Computer Fraud & Security* (6) 12-1.

[20] Froud, D. (2016). The central role of authentication in fighting fraud in mobile commerce. *Journal of Payments Strategy & Systems,* 9 (4) 274-279.

[21] Cimiotti, G., Merschen, T. (2014). Trends in consumer payment fraud: A call for consistent strong authentication across all consumer payments. *Journal of Payments Strategy & Systems*, 8 (1) 43-63.

[22] Anderson, R., Murdoch, S. J. (2014). EMV: Why payment systems fail. *Communications of the ACM*, 57 (6) 24-28.

[23]UK Card Association. http://www.chequeandcredit.co.uk/files/candc/c&ccc/press_releases/2015/2015_h1_fraud_figures_release_-_final.pdf

[24] Mitigating Fraudulent CNP Transactions. Available online at: http://www.quatrroprocessing.com/images/pdf/Whitepaper-CNP-Transactions.pdf

[25] EMV: Issuance Trajectory and Impact on Account Takeover and CNP - Available online at: http://aitegroup.com/report/emv-issuance-trajectory-and-impact-account-takeover-and-cnp

[26] Sakharova, I. (2012). Payment card fraud: Challenges and solutions. In Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on (p. 227-234). IEEE.

[27] Secure Mobile Payment Systems Recommendations for Building, Managing and Deploying, available online at : https://www.visaeurope.com/media/pdf/secure%20mobile%20payment%20systems%20guide.pdf

[28] Singh, J., Ruhl, R., Lindskog, D. (2013). GSM OTA SIM Cloning Attack and Cloning Resistance in EAP-SIM and USIM. *In:* Social Computing (SocialCom), 2013 International Conference on (p. 1005-1010). IEEE.

[29] Mobile Payments: Risk, Security and Assurance Issues, available online at : http://www.isaca.org/groups/professional-english/pci compliance/groupdocuments/mobilepaymentswp.pdf

[30] Isaac, J. T., Zeadally, S. (2014). Secure Mobile Payment Systems. IT Professional, 16 (3) 36-43.