Routledge
Taylor & Francis Group

Economic Research-Ekonomska Istraživanja

ISSN: 1331-677X (Print) 1848-9664 (Online) Journal homepage: http://www.tandfonline.com/loi/rero20

The determinants of electronic payment systems usage from consumers' perspective

Emrah Oney, Gizem Oksuzoglu Guven & Wajid Hussain Rizvi

To cite this article: Emrah Oney, Gizem Oksuzoglu Guven & Wajid Hussain Rizvi (2017) The determinants of electronic payment systems usage from consumers' perspective, Economic Research-Ekonomska Istraživanja, 30:1, 394-415, DOI: 10.1080/1331677X.2017.1305791

To link to this article: http://dx.doi.org/10.1080/1331677X.2017.1305791

Published online: 12 Apr 2017.

ECONOMIC RESEARCH–EKONOMSKA ISTRAŽIVANJA, 2017
VOL. 30, NO. 1, 394–415
http://dx.doi.org/10.1080/1331677X.2017.1305791

Routledge
Taylor & Francis Group

The determinants of electronic payment systems usage from consumers' perspective

Emrah Oney[a], Gizem Oksuzoglu Guven[b] and Wajid Hussain Rizvi[c]

[a]Faculty of Business and Economics, Eastern Mediterranean University, Famagusta, Turkey; [b]Faculty of Business Administration, University of Mediterranean Karpasia, Nicosia, Turkey; [c]Department of Marketing, Institute of Business Administration (IBA), Karachi, Pakistan

ABSTRACT

Electronic Payment Systems (EPS) have been improving individuals' quality of life through providing ease of payment for online transactions. The effects of trust and security on the use of EPS have long been recognised in e-commerce literature. However, very few studies have examined these two concepts from the viewpoint of users. This study has developed a conceptual model to examine the determinants of perceived security and trust as well as the impact of perceived security and trust on the use of EPS. A sample of 299 respondents was analysed through structural equation modelling (SEM); the findings indicate that both perceived security and trust have a significant influence on EPS use. Technical protection and past experience have been found to be the common determinants of perceived security and trust. Managerial implications of the findings are discussed in light of the study's limitations and suggestions for further research indicated.

ARTICLE HISTORY
Received 30 October 2014
Accepted 10 June 2016

KEYWORDS
Perceived trust; perceived security; past experience; electronic payment systems (EPS); structural equation modelling; SEM analysis

JEL CLASSIFICATIONS
M10; M15; M30; M39

1. Introduction

This paper examines individual users' personal experience of electronic payment systems (EPS). Due to its widely accepted benefits, many businesses are accepting electronic payment systems for commercial transactions. EPS have been researched with increasing interest, North Cyprus specifically provides an interesting case for the investigation individuals' experience of EPS as it is currently integrating its governmental organisations to an online system and, more importantly, an increasing number of Cypriot businesses are integrating EPS systems to their daily transactions. The individual experiences of customers in North Cyprus are essential as they provide insights which, besides enriching the relevant literature, offer a clear perspective for practitioners such as businesses, advertising, marketing agencies and financial institutions that are currently using EPS services. Unlike the majority of the existing literature, current research investigates the security and trust from the viewpoint of consumers and their effect on EPS usage and attempts to comprehend the antecedents of perceived security and perceived trust in EPS.

CONTACT Emrah Oney emrah.oney@emu.edu.tr

In the next section, EPS has been reviewed and prior research on security and trust issues in EPS are examined. Following this section, a conceptual framework is presented with the developed hypotheses. Subsequently, the research methodology and results are discussed. Finally, conclusion and research implications are provided in the last section.

2. Literature review

2.1. Theoretical background of EPS

The extensive use and commercialisation of the Internet have created a dynamic electronic commerce world. Lee, Yu, and Ku (2001) stated that electronic commerce (EC) provides numerous advantages over traditional commerce such as openness, speed, anonymity and global accessibility, which simplify life and increase individuals' quality of life. These advantages boost the popularity of EC and enhance the competitive edge of the companies which adopt it. Due to its popularity, EC has been defined in various ways; however the best definition for the purpose of this article suggests that EC is 'the sharing of business information, maintaining business relationships and conducting business transactions by the means of telecommunication networks' (Zwass, 1996, p. 3).

EC is built upon electronic payment systems (EPS) and with the increasing volume of electronic commerce, EPS is becoming more crucial for both businesses and consumers (Kim, Tao, Shin, & Kim, 2010). EPS are used for the completion of electronic commerce transactions and have been defined as 'any payment system that facilitates secure electronic commerce transactions between organisations and individuals' (Lim, Lee, & Kurnia, 2007, p. 231). Linck, Pousttchi, and Wiedemann (2006) stated that for businesses which operate electronically, EPS are one of the most essential determinants of success. As a result, EPS have attracted much attention by researchers and practitioners since the emergence of EC.

Although EPS have improved significantly over the last decade, security and trust issues were still matter of concern for users back in the 2000s, and such concerns still exist (Shon & Swatman, 1998). Within the context of EPS, both security and trust are essential; security has been defined as 'a set of procedures, mechanisms and computer programmes to authenticate the source of information and guarantee the integrity and privacy of the information (data) to abstain this circumstance to lead to a hardship (economic) of data or network resources' (Tsiakis & Sthephanides, 2005, p. 10). Trust is defined as a form of confidence in a partner as a whole and his/her reliability and integrity Liao, Liu, & Chen, 2011; Moorman, Deshpande, & Zaltman, 1993). According to Reichheld and Schefter (2000), trust is vital in transactional relationships, especially those containing high risk such as online transactions. In other words, trust is as crucial as security for the success of EPS. Thus, identifying and comprehending the factors affecting trust and security is essential for practitioners who deal with EPS.

The lack of perceived security and trust has been identified as one of the most vital factors slowing the development of e-commerce (Centeno, 2002). The majority of trust theories are built upon personal contact and conventional relationships (Tsiakis & Sthephanides, 2005). However, e-commerce lacks these two mandatory elements in its nature; thus it is problematic to establish and retain trust for this particular system. This is why it is particularly important to have secure EPS and inspect technical protections that are developed to reduce the risk of e-commerce before addressing the issue of user trust.

Previous research has indicated that the lack of human contact or social relation during the electronic payment process creates a threat for the security of EPS (Kim et al., 2010; Tsiakis & Sthephanides, 2005). According to researchers such as Van Dyke, Midha, and Nemati (2007) and Eastlick, Lotz, and Warrington (2006), trust and privacy concerns are the two particular reasons that prevent individuals engaging in e-commerce transactions. Likewise, findings of the survey by Gartner Group (2001) stated that when shopping online, trust and privacy issues were the main concern of 95% of the participants (Gartner Group, 2001). Thus, security is of utmost importance for EPS usage. Before anything else, the first and foremost an EPS should provide security to its users (Kim et al., 2010; Linck et al., 2006; Tsiakis & Sthephanides, 2005).

The existing literature mainly focuses on security and trust in EPS from the perspective of service providers (Linck et al., 2006) and not enough attention has been given to consumers' perception of security and trust. As a consequence, theoretical and empirical researches are lacking in this crucial area. A notable exception is the study of Kim et al. (2010). Their research examined the determinants of consumers' EPS usage. They have concluded that both perceived security and trust have a positive and significant impact on EPS use. In order to address the above mentioned deficiency in the literature, the present study examines security and trust in EPS from the viewpoint of consumers in a small island economy (North Cyprus). Additionally, factors affecting consumers' perceived trust and security have also been examined in order to provide a deeper understanding of the research phenomenon.

Although, EPS have been employed all around the world, the present research uses North Cyprus for the empirical investigation for two main reasons. First, electronic commerce and EPS provide opportunities to developing countries that can potentially enhance their economic growth (Molla, Taylor, & Licker, 2006). Second, consumers in small economies as in North Cyprus cannot benefit from the advantages of economies of scale and competitive market opportunities of traditional market places. Thus, EC opens a window of opportunity that enhances interest in adoption of EPS in North Cyprus. Since the late-1990s, Cypriot consumers have purchased products and services through the internet. Over the years, the engagement in EC amplified when Cypriot consumers realised that prices of numerous products and services are considerably cheaper on the internet than in traditional marketplaces (Thrassou, Vrontis, & Kokkinaki, 2010). Consequently, EC has become an important part of life for consumers especially for the younger generations. Several different EPS brands are already used in North Cyprus such as PayPal, eCredit and Smartpay and more is projected to be established in the future. The EC in North Cyprus is expected to grow with high speed in the following years, thus EPS will become more important for consumers, businesses and researchers.

With the emergence of EC, EPS became one of the most crucial and practical monetary tools of transaction for consumers and businesses. Concurrently, new intermediaries such as PayPal managed to fulfil the fresh and novel needs of EC users (i.e. consumers and merchants) (Dahlberg, Dahlberg, & Nyström, 2008); such as electronic payment (e-payment) which is an imperative requirement to complete an electronic commerce transaction. According to Kim et al. (2010), e-payment is the transfer of an electronic value from a payer to a payee via an electronic mechanism. E-payment services assist and allow individuals to manage their financial transactions remotely (Lim, 2008). According to Tsiakis and Sthephanides (2005), EPS achieve two things in particular: (a) the emulation of existing payment frameworks from the real world and/or (b) the systematisation of new ways to

execute payment transactions (Tsiakis & Sthephanides, 2005). EPS can be classified into five categories (Kim et al., 2010).

These categories are;

Electronic cash: Electronic cash is a method of payment in which a specific identification number is associated with a specific amount of money (Kim et al., 2010). This method was developed as an alternative of credit card and debit card for e-commerce. Electronic cash is the informational equivalent of physical banknotes and coins (Zwass, 1996). Individuals have to purchase electronic digital cash from the issuing company in order to be able to use this system (Abrazhevich, 2004). The purchased digital cash can be transferred through electronic telecommunication channels (Hsieh, 2001; Kim et al., 2010). Electronic cash can offer such benefits as buyer anonymity, global validity, and divisibility that can go beyond real cash in the case of so-called micropayments cost-effectively, for instance to pay an amount of US$0.02 (Zwass, 1996).

Pre-paid cards: Pre-paid cards are generated for a particular value by a specific merchant and are used for in-store or online transactions (Kim et al., 2010; Kniberg, 2002). Although, in practice the pre-paid cards are given as 'gift cards' where a giftee can select goods or services up to the amount pre-loaded on the card, it is also common where they are used by an individual who pre-loaded the card for personal use. Alternatively, companies provide pre-paid cards as part of their customer relationship management strategies in the form of corporate gifts or compensation of individual customers who experienced dissatisfaction. The person, who would like to use pre-paid cards online, enters the unique card number on the seller's website to pay for the goods or services during check-out process. The amount to be paid to the seller is deducted from the value of the card. Most of the pre-paid cards are one-time use only and they expire after a given time period if not used; a number of businesses started to allow customers to use pre-paid cards without an expiration date and on more than one transaction within a certain time period (e.g.: within a month's time from its first use). The reason why pre-paid cards are preferred by consumers is their ease of use and convenience (Kim et al., 2010).

Credit cards: Credit cards are plastic payment cards issued to the users to make online or offline financial transactions. Credit cards are the most frequently used form of e-payment (Hsieh, 2001; Kim et al., 2010). Visa, which is one of the biggest credit card companies, reported that e-purchases reached $350 billion this year. Credit cards involve highly complex transaction structure and provide a secure medium for its users (Wright, 2002). Compared to other EPS, credit cards are not appropriate for micro payments (i.e., payments smaller than $1) unlike electronic cash.

Debit cards: Debit cards (also known as bank cards or check cards) are a plastic card which allows individuals to withdraw cash from their bank accounts via automated teller machines (ATMs) without face-to-face interaction in a bank, as well as to pay for goods and services both online and offline. Debit cards are issued by banks (public/private) and financial service providers. Unlike credit cards, once an individual pays with a debit card, the amount is automatically deducted from his/her bank account. Debit card is one of the most frequently used e-payment methods (Kim et al., 2010).

Electronic cheques: Electronic cheque is a form of e-payment, which is designed to work in the same way with a traditional/paper check. The main difference between electronic cheque and paper cheque is that actual funds are debited or credited electronically with the use of electronic check. Compared to other e-payment methods, the electronic cheque is the least popular (Yahid, Shahbahrami, & Nobakht, 2013).

Based on the above review, it is apparent that pre-paid, credit and debit cards are the most frequently used e-payment methods, whereas the electronic cash method has been operating as a complement to them. Electronic cash has been mostly used for small-value transactions while pre-paid, credit and debit cards have been employed for most types of transactions except small-value transactions. The reason for not using pre-paid, credit and debit cards for small-value transactions is that it can be disproportionally expensive to employ these methods for small amounts. Since no single e-payment method predominates the sector, all the methods can be seen as an alternative to each other. Furthermore, security, security mechanisms, and ease of use are important elements for individuals while deciding on the type of EPS to use. Importance should be given appropriately to these elements in order to reduce transaction risk and increase the use of EPS. The next section will review the literature in order to identify the factors affecting consumers' perceived security and perceived trust in the use of EPS.

2.2. Security and trust issues in EPS

The lack of perceived security and trust has been identified as one of the most vital factors slowing the development of e-commerce (Centeno, 2002). In order to build trust and security in EPS, it is important to provide technical protection to users (Kim et al., 2010). Similarly, Kalakota and Whinston (1997) found out that technical reliability and the resistance of the EPS against security attacks are two factors affecting the security of EPS. Furthermore, technical infrastructure, implementation, well-defined transaction rules, and legal factors (e.g. legal framework) have been found to be important factors for EPS security and trust. Finally, Romdhane (2005) reviewed the existing literature and stated that a secure EP system must exhibit nine elements. These elements are authentication, fraud prevention, confidentiality, divisibility, transferability, duplicate spending prevention, payment privacy, payment anonymity, and payer traceability.

Moreover, transaction procedure has also been identified as a factor influencing the security and trust in EPS (Hwang, Li, & Hsiao, 2006; Kim et al., 2010). As mentioned earlier, EPS differ from the traditional payment methods in their nature and, thus, are faced with a wide range of novel security issues (Lim, 2008). Some of these security issues include unauthorised use of the EPS and transaction status (Kim et al., 2010; Linck et al., 2006). According to Laudon and Traver (2001), Kim et al. (2010) and Lawrence, Newton, Corbitt, Braithwaite, and Parker (2002) sophisticated transaction procedures and process interactions should be developed in order to minimise and/or eliminate consumers' perceived security and trust concerns. The importance of security and trust in EPS has been mentioned previously, hence an upsurge in these elements will boost the use of EPS.

Security statements have also been found to be an important factor affecting consumers' perceived security and trust (Mukherjee & Nath, 2003). The term 'security statement' is defined as the information delivered to the users (consumers) for EPS processes and security solutions. According to Miyazaki and Fernandez (2000b), security statements posted on websites are likely to increase intention to purchase over the internet. This particular finding is also supported by the concept of information asymmetry. Information asymmetry refers to 'situations in which one of the parties involved in a transaction does not have access to all the information needed for decision making' (Kim et al., 2010, p. 86). The problem of information asymmetry has been an ongoing issue for EPS since its emergence (Mukherjee,

& Nath, 2003). Friedman, Howe, and Felten (2002) and Mukherjee and Nath (2003) stated that descriptive contents concerning security and privacy issues (e.g. security statements) should influence consumer perceptions of trust and security in EPS. Moreover, descriptive contents also assist consumers to construct a more accurate interpretation of EPS security (Friedman et al., 2002).

Previous research has correspondingly discovered that protection of information is a vital element influencing the use of EPS (Kim et al., 2010; Linck et al., 2006). The majority of the researches focused on the technical details of protection such as privacy and integrity. However, according to Kim et al. (2010) and Mukherjee and Nath (2003), the methods used for authentication, confirmation, and modification are also essential in the use of EPS and should be examined when the use of EPS is a matter of protection.

Finally, past experience is recognised as another influencing factor for the use of EPS. According To Wu and Wang (2005), past-experience will increase the chance of adoption and use of new technologies and systems (e.g. EPS). Furthermore, Patton and Jøsang (2004) and Pichler (2000) stated that trust is based on experience over time and deepens as a function of past-experience. Similarly, Miyazaki and Fernandez (2001) found out that past-experience is negatively related with the existence of concerns regarding the security of EC. Thus, it is expected that past experience should influence customer perception of security and trust in EPS.

Based on the literature review, four factors that influence consumers' perception of security and trust in EPS have been identified. These factors are security statements; transaction procedures; technical protection and personal past experience with EPS.

3. Research model and hypotheses

3.1. Research model

Few studies have explored the relationship between perceived security, perceived trust and the use of EPS. Notable exceptions are the studies of Kim et al. (2010) and Theodosios and George (2005). They concluded that perceived security and perceived trust have a significant, positive effect on the use of EPS. Correspondingly, Theodosios and George (2005) claimed that EPS providers should take into account trust and security as important determinants of consumer use of EPS.

This study borrows Kim et al.'s (2010) research model, which is designed to test the influence of perceived security and trust on consumer EPS use. As mentioned previously, both perceived security and trust are important concerns for EPS use. Lack of perceived security and trust may erode consumers' willingness to use EPS (Linck et al., 2006; Mukherjee & Nath, 2003). Thus, it is vital to study the factors influencing perceived security and trust. Figure 1 summarises the research model, based on the research hypotheses developed. Although, some of the factors identified in this model have been used in previous studies (e.g. Kim et al., 2010), our research model a identifies new determinant which is considered to be important for consumers' perceived security and trust. As shown in the model, technical protection, transaction procedures, security statements and past experience with EPS are the principal factors for consumer perceptions of security and trust in the use of EPS. These factors are believed to have a significant effect on consumers' perceived security and trust in EPS.

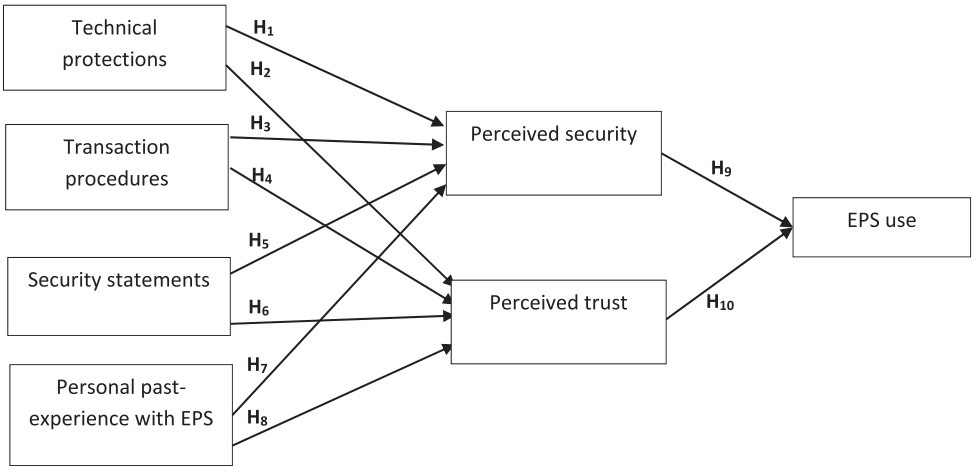

Figure 1. The conceptual model of perceived security and perceived trust in EPS use. Source: Created by authors.

3.2. Technical protections in EPS

Technical protections have been accepted as important antecedents for EPS security (Kim et al., 2010). Numerous technical protections have been developed and utilised in order to ensure the safety of electronic payment (Linck et al., 2006). Likewise, Kim et al. (2010) and Chellappa and Pavlou (2002) mentioned that technical protections (including privacy, integrity and stability) have a positive effect on perceived security and trust. In other words, providing sufficient technical protection will enhance consumers' perceived security and trust in EPS. Based on these findings, it is proposed that:

Hypothesis 1. Technical protections have a significant and positive effect on consumers' perceived security in EPS.

Hypothesis 2. Technical protections have a significant and positive effect on consumers' perceived trust in EPS.

3.3. Transaction procedures in EPS

Transaction procedures are critical for individuals to be able to use EPS safely and efficiently. According to Hwang, Shiau, and Jan (2007) and Kim et al. (2010), well-defined transaction procedures assist individuals to eliminate their security concerns. Generally, three main transaction procedures are employed during the electronic monetary transactions. These procedures are: (1) authenticating each participant prior to the transaction; (2) providing consumers with several separate steps toward the completion of the payment; (3) sending acknowledgement messages to each participant after the completion of the payment (Hwang et al., 2007). It is believed that transaction procedures will have an effect on perceived security and trust. It has been hypothesised that:

Hypothesis 3. Transaction procedures have a significant and positive effect on consumers' perceived security in EPS.

Hypothesis 4. Transaction procedures have a significant and positive effect on consumers' perceived trust in EPS.

3.4. Security statements in EPS

Security statements on EPS have been found to be a vital factor influencing consumers' perceived trust in EPS (Kim et al., 2010; Mukherjee & Nath, 2003). According to Kim et al. (2010), consumers' decision to use an EPS will heavily depend on the security statements posted since these statements can boost the consumers' perceived security and trust in EPS. Similarly, Miyazaki and Fernandez (2000a) stated that security statements posted on EPS will increase the likelihood of consumers purchase over the Internet. Based on these findings, it has been hypothesised that:

Hypothesis 5. Security statements have a significant and positive effect on consumers' perceived security in EPS.

Hypothesis 6. Security statements have a significant and positive effect on consumers' perceived trust in EPS.

3.5. Personal past experience with EPS

Past experience will lead to the faster adoption and consumption of new technologies (i.e. EPS) (Wu & Wang, 2005). Similarly, Hackbarth, Grover, and Yi (2003) mentioned that individuals are more comfortable using new technology innovations when they have prior experience. The reason for this happening is that past experience builds trust (Eastin, 2002) and is negatively related with the existence of concerns regarding the security of EC (Miyazaki & Fernandez, 2001). Thus, consumers with EPS past-experience will trust these systems and perceive them as a secure way of completing transactions. Hence, it has been hypothesised that;

Hypothesis 7. Past experience with EPS has a significant and positive effect on consumers' perceived security in EPS.

Hypothesis 8. Past experience with EPS has a significant and positive effect on consumers' perceived trust in EPS.

3.6. Perceived security in EPS

Kim et al. (2010) have defined perceived security as the consumer's subjective evaluation of the e-payment system's security. Consumers can analyse and judge the security of EPS differently. Thus, the perceived security of EPS may vary across individuals. The level of perceived security has a great impact on consumers' decisions regarding the use of EPS. If the level of perceived security in an EPS is too low, consumers are unlikely to engage in a

transaction (Kim et al., 2010; Tsiakis & Sthephanides, 2005). Security is one of the important triggers of EPS use. Thus, it has been hypothesised that:

Hypothesis 9. Perceived security in EPS has a significant and positive effect on consumers' use of EPS.

3.7. Perceived trust in EPS

Earle (2009, p. 786) described trust as 'the willingness, in the expectation of beneficial outcomes, to make oneself vulnerable to another based on judgement of similarity of intentions or values'. Correspondingly, Tsiakis and Sthephanides (2005) have defined perceived trust as consumers' belief that electronic payment transactions will be proceed in accordance with their expectations. Trust has been identified as one of the most important factors influencing consumers' use of EPS and consumers with higher levels of trust have been found to be more prone to use EPS (Kim et al., 2010; Tsiakis & Sthephanides, 2005). Similarly, Kim et al. (2010) mentioned that it is impossible for an EPS to gain widespread usage without trust. Furthermore, it has been found out that trust is more important than security and without trust consumers will not use EPS to complete their transactions (Mallat, 2007). Thus, it has been hypothesised that:

Hypothesis 10. Perceived trust in EPS has a significant and positive effect on consumers' use of EPS.

4. Method and data analysis

4.1. Data collection and sample profile

Using personally administered questionnaires, data were collected from a sample of 329 students at Eastern Mediterranean University. Rigorous pre-testing ensured readability, understanding and comprehension of all questions. 30 out of 329 questionnaires were non-usable due to the vast amount of missing information. Thus, the final sample size comprised 299 respondents. According to Lightner, Yenisey, Ozok, and Salvendy (2002), university students are representative groups of typical online shoppers in the electronic commerce world, mainly due to their familiarity with computers and e-commerce.

A structured, paper-based questionnaire and a convenience sampling technique were used for data collection. Convenience sampling provides a relatively quick and economical way to collect data and although it is not appropriate for theory testing (i.e., it generalises the findings), it is acceptable for theory building (i.e., revealing the impact of selected factors on EPS use). The questionnaire had eight sections: technical protections, transaction protections, security statements, personal past experience, perceived security in EPS, perceived trust in EPS, EPS use and demographics.

Questionnaires were collected immediately after completion. The data collection was completed in 27 days. The final sample comprised 181 males (60.5%), and 118 females (39.5%) with a mean age of 24. A total of 245 respondents (81.9%) were single or divorced and 43 respondents (14.4%) were married (11 missing values, comprising 3.7% of the sample).

4.2. Measures

Technical protections (6 items), transaction procedures (6 items), security statements (6 items), perceived trust (4 items), perceived security (4 items) and EPS use (3 items) were measured with scales borrowed from Kim et al. (2010). Personal experience with EPS was measured with a five item scale, which was developed by authors for the purpose of this study. Seven-point Likert-type response categories (i.e., 1=strongly disagree; 7=strongly agree) were used for all of the employed scales. This research measures technical protections via privacy; integrity; and confidentiality; transaction procedures via authentication; modification; and confirmation and security statements through availability; accessibility; and comprehensibility (Kim et al., 2010).

4.3. Descriptive statistics

The averaged summated mean scores and the corresponding standard deviations of all the constructs in the current study are presented in Table 1. Along a 7-point measurement scale, the reported mean of EPS use score was 5.38, showing that the majority of the sample frequently uses EPS in order to complete online transactions. This result demonstrates that the selected sample is familiar with the use of EPS and, thus, will provide valuable insight information regarding the present research questions. Moreover, the respondents exhibited high security and trust in EPS (respectively 5.47 and 5.14) despite there being plentiful threats on the internet for users. Finally, along a 7-point measurement scale, the mean personal past experience score was 5.06, showing that respondents have a considerable amount of experience, knowledge and information about EPS.

4.4. Data analysis

A two-step approach that included confirmatory factor analysis (CFA) and structural equation modelling (SEM) was used in this study (Anderson & Gerbing, 1988). CFA is used to assess the overall measurement quality and employed SEM through AMOS 21 for testing the proposed hypotheses (Jöreskog & Sörborn, 1996).

4.5. Confirmatory factor analysis

CFA is mainly used to assess interrelationship among latent constructs, unlike the structural model confirmatory measurement model which does not assume specific directional path among constructs (Hair, Anderson, Tatham, & Black, 1995). Based on CFA analysis,

Table 1. Descriptive Statistics of the Constructs under Study ($N = 299$).

	Mean	Standard Deviation
Transaction Procedures	5.99	0.67
Technical Protections	5.74	0.74
Security Statements	5.57	0.70
Personal Past-experience	5.06	1.32
Perceived Security	5.47	0.78
Perceived Trust	5.14	0.84
EPS Use	5.38	1.19

Source: Created by authors.

items were removed either because of low loadings (less than .5) or non-significant t-values ($p > .05$), more specifically, one item each from the transaction procedures, technical protections, and personal past experience measures were discarded. These items were removed from further analysis. Overall, the analysis indicated a good fit of the measurement model (x2 = 987.590, df = 378; x2/df = 2.613; CFI = 0.908; IFI = 0.909; RMSEA = 0.074). These values all met the threshold requirements suggested by previous researches (Browne & Cudeck, 1993; Byne, 1994; Hair et al., 1995; Kim et al., 2010).

As presented in Table 2, all standardised loading ranging from 0.70 to 0.95 for all items. Confirmatory factor analyses determined that technical protections, transaction procedures, security statements, personal past experience, perceived security, perceived trust, and EPS use are separate variables. The initial component solution was rotated by using the varimax procedure, with components whose Eigen values were greater than one, which is the criterion for factor retention. Based on the Eigen values that were greater than one, seven factors were accepted as interpretable factors. Furthermore, all the cross-loadings were less than .30. These results provide initial evidence that the measures exhibit discriminant validity.

Table 2. Summarised Results of Standardised Factor Loadings, Cronbach's Alpha (α), Composite Reliability (C.R) and Average Variance Explained (A.V.E) ($N = 299$).

Indicator	Tran. Pro.	Tech. Pro.	Sec. Stat.	P. Exp.	Perc. Sec.	Perc. Tru.	EPS Use
TranPro1	0.82						
TranPro2	0.71						
TranPro3	0.83						
TranPro5	0.75						
TranPro6	0.70						
TechPro1		0.78					
TechPro2		0.86					
TechPro3		0.82					
TechPro4		0.77					
TechPro5		0.70					
SecStat1			0.85				
SecStat2			0.84				
SecStat3			0.80				
SecStat4			0.81				
SecStat5			0.82				
SecStat6			0.77				
PastExp1				0.93			
PastExp2				0.93			
PastExp3				0.74			
PastExp4				0.74			
PercSec1					0.90		
PercSec2					0.91		
PercSec3					0.75		
PercSec4					0.73		
PercTru1						0.70	
PercTru2						0.95	
PercTru3						0.80	
EPSUse1							0.92
EPSUse2							0.95
EPSUse3							0.87
Alpha ()	0.87	0.89	0.92	0.90	0.90	0.85	0.94
A.V.E	0.58	0.62	0.66	0.71	0.68	0.67	0.83
C.R	0.87	0.89	0.92	0.90	0.90	0.86	0.94

Notes: Tran. Pro. _ transaction procedures, Tech. Pro. _ technical protections, Sec. Stat. _ security statements, P. Exp. _ personal past experience, Perc. Sec _ perceived security, Perc. Tru. _ perceived trust, and EPS Use _ Use of Electronic Payment System. All the estimated factor loadings are significant at p 0.05.

Source: Created by authors.

The average variance extracted (AVE) by each latent variable was examined. Fornell and Larcker (1981, p. 303) state that 'AVE. is an examination of the amount of variance that is captured by the construct in relation to the amount of variance due to measurement error'. Hair, Anderson, Tatham, and Black (2007) suggests that values over 0.50 are acceptable for the AVE. If the AVE value is less than 0.50, the variance due to measurement error exceeds the variance captured by the construct; in such cases the validity of the instrument may be called into question. As presented in Table 2 all values of AVE are larger than 0.5; thus convergent validity is present for all the scales (Anderson & Gerbing, 1998).

Furthermore, composite reliability (CR) of each latent variable was examined. Composite reliability (CR) measure is used to check how well a construct is captured by its assigned indicators (Hair et al., 2010). Hair et al. (2007) suggest that values over 0.70 are acceptable returns from the composite reliability. As presented in Table 2, the composite reliability (CR) of each latent variable was greater than 0.70. The composite reliability (CR) and Cronbach's Alpha (see Table 2) of each latent variable exceeds the suggested cut-off value of 0.7, indicating that the reliability of all constructs was good (Bagozzi & Yi, 1988; Hair, Anderson, Tatham, & Black, 1998; Hayduk, 1987).

Discriminant validity was established by calculating the shared variance between pairs of constructs and verifying that it was lower than the variances extracted for the individual constructs (Fornell & Larcker, 1981). The shared variances between pairs of all possible scale combinations ranged from 0.06 to 0.48 which is below the AVE for each construct (range: 0.58 to 0.83). Thus, the scales provide evidence for discriminant validity (Anderson & Gerbing, 1998).

Since, no particular problem was detected in the measurement model, structural equation modelling was then employed to examine the overall fit of the proposed model, and to assess all the relevant path coefficients (Anderson & Gerbing, 1998). The major findings are presented in the following section.

4.6. Structural equation modelling – overall model fit

The proposed model in this study contains various latent constructs and each construct has a pre-conceived directional influence on other constructs. According to Hair et al. (1995), one of the main applications of structural model is to represent a proposed theory specifically when proposed constructs in a theory are latent rather than observed. Thus structural model was used to represent proposed hypotheses. The goodness of fit statistics indicates that the proposed model fits the data well (x^2 = 1,068.037 p<.001, df = 386; CMIN = 2.767; CFI = 0.90; IFI = 0.899; RMSEA = 0.077). The suggested goodness of fit threefold for CMIN is 2–3, CFI 90–95, IFI 90–95 and RMSEA .05-.08 (Hair et al., 1995). The values of the indices are within the suggested thresholds representing the model fit (Browne & Cudeck, 1993; Byne, 1994; Kim et al., 2010). It was further observed that the model was able to explain 47% of the variance in perceived security, 32% of the variance in perceived trust and 9% of the variance in EPS use.

Figure 2 shows the estimated standardised regression coefficients of the constructs under investigation. The results of SEM indicated that technical protections had a significant positive effect on perceived security and perceived trust (β=0.356, p<0.01; β=0.481, p<0.01 respectively). Hence, both H1 and H2 are supported. In contrast, the effect of transaction procedures on perceived security and perceived trust were not significant (β = -0.41,

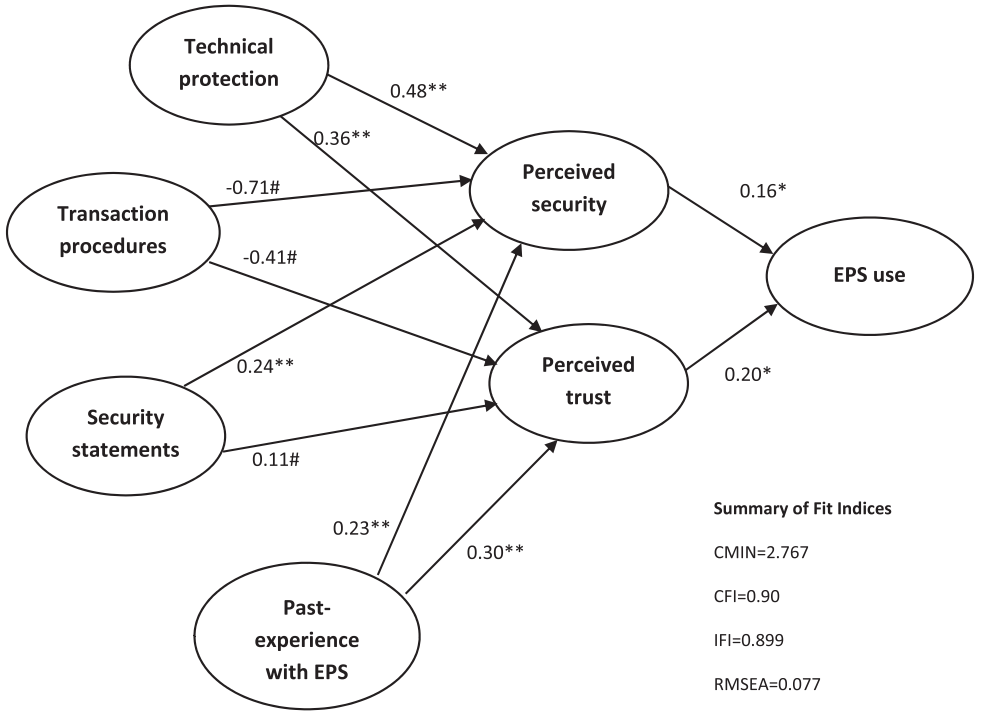

Figure 2. Overall fit of the proposed model and path analysis of the latent constructs.
Notes: * Significant at $p<0.05$; ** Significant at $p<0.01$; # Not significant.

p=0.260; β = -0.71, p=0.557 respectively) and thus, both H3 and H4 were not supported. The results have shown that transaction procedures do not act as an antecedent for both perceived security and perceived trust. Moreover, the findings suggest that security statements have a significant and positive effect on perceived security (β=0.236, p<0.01) but not on perceived trust (β=0.110, p=0.97). These results indicate that in case of H5 the null hypotheses is rejected but we failed to reject the null in case of H6. Hence, security statements can be seen as an antecedent of perceived security but not as an antecedent of perceived trust. Our results have also shown that personal past experience with EPS has a positive and significant effect on both perceived security and perceived trust (β=0.227, p<0.01; β=0.303, p<0.01 respectively) indicating support for the 7 and 8 hypotheses. Finally, the results have shown that perceived security and perceived trust have a positive and significant effect on EPS use (β=0.158, p<0.17; β=0.201, p<0.02 respectively) indicating support for H9 and H10. These findings have revealed that perceived security and perceived trust can be important triggers of EPS use.

The result suggests that both technical protection and past experience with ESP are major determinants of perceived security and perceived trust representing H1, H2, H7 and H8 and in turn both perceived security and perceived trust influence EPS use representing H9 and H10. However, it is important to note that transactional procedure (H3 and H4) is not an antecedent of perceived security and trust, since the coefficient is negative and non-significant. One explanation for this notion could be that some transactional procedures may be recognised as unnecessary or inconvenient actions by users. Thus, the level of perceived

security and perceived trust of users is not affected by transactional procedures. Moreover it was observed that security statements were not a statistically significant antecedent of perceived trust (H6), whereas it was statistically significant antecedent of perceived security (H7). Although this result is not confirmed as it was hypothesised, it is not beyond understanding either. Since perceived security and trust are conceptually different, the former is based on subjective evaluation and the latter on beliefs that formulate certain expectations, therefore security statements were handy to influence just subjective evaluation rather than forming certain beliefs. Finally, the results have shown that both perceived trust and perceived security have a significant effect on EPS use. The effect of perceived trust has been found to be stronger than perceived security on EPS use that is highlighted in the results as regression coefficient of perceive trust is higher than perceived security (H9 and H10). The result consistency of this study with academic literature is further highlighted in the discussion session.

5. Discussion

5.1. Evaluation of findings

In this study, an attempt has been made to identify the determinants of perceived security and perceived trust and their effect on EPS use. The security and trust concepts have been examined from the viewpoint of users of EPS in order to provide a deeper understanding of these constructs as it highlights the extended insights of EPS users. Our findings have shown that both perceived security and perceived trust have a positive and significant effect on EPS use. In other words, when users perceive the EPS as secure and trustworthy, they are more willing to complete their transactions electronically. The results are consistent with the existing literature (Culnan & Armstrong, 1999; Kim et al., 2010). The results have also shown that technical protection is the strongest determinant of both perceived security and trust. This finding is consistent with previous research (Kim et al., 2010). Thus, the evidence suggests that providing technical protection to the users of EPS can increase consumers' feelings of security and trust.

Furthermore, no significant effect of transaction procedures on perceived security and trust has been found. The effect (insignificant) found in this study is also consistent with the finding in Kim et al. (2010) stating that transaction procedure is not a determinant of perceived security and trust. However, the finding in this study and that of Kim et al. (2010) are different from those reported by Romdhane (2005). In Romdhane's (2005) study a significant effect of transaction procedure on perceived security and trust has been identified. Based on this particular finding, it can be stated that it unlikely that transaction procedure is a parameter for the security and trustworthiness of EPS and commonly has been accepted as an excessive practice. Hence, the transaction procedure may cause inconveniences for the users from time to time and degrade users' valuation of the security and trust in the EPS. Finally, personal past experience with EPS has been found to be a common antecedent of perceived security and trust. This finding is in-line with Pavlou and Gefen's (2004) study. According to this result, individuals built their feeling of security and trust based on their past experience. Hence, it is rational to mention that security and trust are based on past experience over time and deepen as a function of past experience.

5.2. Managerial implications

The current study provides several valuable implications for managers in general and it specifically highlights use of EPS and success of a business in North Cyprus. As it is suggested that success rate of a business increases if it engages customers electronically (using EPS), specially when consumers in North Cyprus are increasingly engaging in EPS. However, this engagement is influenced by perceived security and trust. Thus it is essential for mangers to understand the implication of the influencing factors. First, this study shows that that perceived security and perceived trust enhance the use of EPS. Managers should seek ways to trigger users' perceived security and trust. The empirical evidence sought in this study highlights the ways to trigger users' perceived security and trust, as evidence suggests both technical protection and past experience determine perceived security and trust. Thus the managerial focus should be on delivering maximum possible technical protection and providing a secure system to the users. EPS should ensure that users' personal details (name, address, phone number, credit card number etc.) are kept secure and the transfers are fast and reliable. Moreover, the results have also shown that, users require user-friendly, easy-to-use and problem-free systems in order to feel secure and trust the EPS.

Second, the results shows that past experience is an important determinant of perceived security and trust. While users are gaining experience with the EPS over time, managers should make sure that consumers are pleased with their involvement. Positive past experience can strongly trigger consumers' trust and feeling of security towards the EPS. Thus, it is essential for companies to monitor the experiences of the consumers' and to take action if there is a sign of dissatisfaction.

6. Conclusion

The present study proposed and tested a research model that investigated determinants of perceived security and perceived trust and the effect of these two variables on EPS use. The results have shown that both technical protection and personal past experience are important determinants of perceived security and trust. Simultaneously, a security statement is identified as a determinant of perceived security. Finally, and most importantly, perceived security and perceived trust have been found as important determinants of EPS use. These findings are consistent with the previous results (Kim et al., 2010; Miyazaki & Fernandez, 2000; Pavlou & Gefen, 2004).

This study finds no evidence of a statistically significant relationship between transaction procedures and consumers' perceived trust and security in EPS use. One explanation for this result could be that consumers may find transaction procedures complex and timing consuming, thus this inconvenience might negatively affect their perception of security and trust. This finding shows that consumers are not only considering the security of the procedures but also the convenience of the procedures for EPS.

This study is not without limitations. To begin with, the use of a convenient sample limits the results of the research to the specific sample, which means that the findings cannot be generalised to a larger population (Hair et al., 1998). This limitation would have been a problem if the purpose of this study was to test theory. However, as the main aim here was to build theory, lack of external validity becomes less of a problem. Second, the use of student sample may question the representativeness of the study. However, according to Lightner

et al. (2002), university students are representative groups of typical online shoppers in the electronic commerce world, mainly due to their familiarity with computers and e-commerce. Third, the personal past experience scale which has been created by the researchers has not been established using the traditional and more advanced scale development procedures (e.g., focus groups, item generation and purification). Although, the scale has face validity and has been tested for reliability and convergent validity, it will be healthier to develop a scale by using rigorous and advance scale development procedures for future studies.

Finally, this study examined the separate effects of perceived security and perceived trust on EPS use. Future studies may examine the combined effect of these variables on EPS use via polynomial regression analysis. This method will demonstrate how combinations of these two predictor variables (perceived security and perceived trust) relate to EPS use.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Abrazhevich, D. (2004). *Electronic payment systems: A user-centred perspective and interaction design*. Netherlands: Universiteitsdrukkerij Technische Universiteit Eindhoven.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modelling in practice: A review and recommended two steps. *Psychological Bulletin, 103*, 411–423.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of Academy of Marketing Science, 16*, 74–94.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 136–162). Beverly Hills, Ca: Sage.

Byne, B. M. (1994). *Structural equation modelling with EQS and EQS/Windows: Basic concepts, applications, and programming*. Thousand Oaks, CA: Sage.

Centeno, C. (2002). *Building security and consumer trust in internet payments: The potential of "soft" measures- Report EUR20278 EN*. Spain: Institute for Prospective Technological Studies.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*, 358–368.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*, 104–115.

Dahlberg, K., Dahlberg, H., & Nyström, M. (2008). *Reflective lifeworld research* (2nd ed.). Sweden: Studentlitteratur.

Earle, T. C. (2009). Trust, confidence, and the 2008 global financial crisis. *Risk Analysis, 29*, 785–792.

Eastin, M. S. (2002). Diffusion of e-commerce: An analysis of the adoption of four e-commerce activities. *Telematics and Informatics, 19*, 251–267.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*, 877–886.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39–50.

Friedman, B., Howe, D. C., & Felten, E. (2002). *Informed consent in the Mozilla browser: Implementing value-sensitive design*. 35th Annual Hawaii International Conference on System Sciences, HICSS'02, Washington DC, IEEE.

Gartner Group. (2001). On-line fraud prevention white paper for the E-Commerce fraud prevention network. Retrieved August 26, 2013, from http://www.gartner.com

Hackbarth, G., Grover, V., & Yi, M. Y. (2003). Computer playfulness and anxiety: Positive and negative mediators of the system experience effect on perceived ease of use. *Information and Management, 40*, 221–232.
Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis: A global perspective* (7th ed.). Upper Saddle River, NJ: Pearson.
Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate data analysis with readings*. Englewood Cliffs, NJ: Prentice-Hall.
Hair, J., Anderson, R., Tatham, R., & Black, W. (1998). *Multivariate data analysis*. NY: Macmillan.
Hair, J. E., Anderson, R. L., Tatham, W. C., & Black, W. C. (2007). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice-Hall.
Hayduk, L. A. (1987). *Structural equation modeling with LISREL: Essentials and advances*. Baltimore, MD: Johns Hopkins University Press.
Hsieh, C. T. (2001). E-commerce payment systems: Critical issues and management strategies. *Human Systems Management, 20*, 131–138.
Hwang, R. J., Li, J. F., & Hsiao, Y. K. (2006). A wireless-based authentication and anonymous channels for GSM system. *Journal of Computers, 17*, 31–36.
Hwang, R. J., Shiau, S. H., & Jan, D. F. (2007). A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications, 6*, 184–191.
Jöreskog, K. G., & Sörborn, D. (1996). *LISREL 8: User's reerence guide*. Chicago, IL: Scientific Software.
Kalakota, R., & Whinston, A. B. (1997). *Electronic commerce-A manager's guide*. Reading, MA: Addision-Wesley.
Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*, 84–95.
Kniberg, H. (2002). *What makes a micropayment solution succeed* (Master's thesis). Institution for Applied Information Technology, Kungliga Tekniska Högskolan, Kista.
Laudon, K., & Traver, C. (2001). *E-commerce: Business, technology, society*. Boston, MA: Addison-Wesley.
Lawrence, E., Newton, S., Corbitt, B., Braithwaite, R., & Parker, C. (2002) *Technology of internet business*. Milton, QLD: Wiley.
Lee, Z. Y., Yu, H. C., & Ku, P. J. (2001). *An analysis and comparison of different types of electronic payment systems*. Management of Engineering and Technology, 2001. PICMET'01. Portland International Conference on, IEEE, 38–45, Portland.
Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10*, 702–715.
Lightner, N., Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2002). Shopping behavior and preferences in e-commerce of Turkish and American university students: Implications from cross-cultural design. *Behavior and Information Technology, 21*, 373–385
Lim, A. S. (2008). Inter-consortia battles in mobile payments standardization. *Electronic Commerce Research and Application, 7*, 202–213.
Lim, B., Lee, H., & Kurnia, S. (2007). Exploring the reasons for a failure of electronic payment systems: A case study of an Australian company. *Journal of Research and Practice in Information Technology, 39*, 231–244.
Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). *Security issues in mobile payment from the customer viewpoint*. Proceedings of the 14th European Conference on Information Systems, (ECIS 2006), Göteborg, Schweden, 1–11.
Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *Journal of Strategic Information Systems, 16*, 413–432.
Miyazaki, A. D., & Fernandez, A. (2000a). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*, 54–61.
Miyazaki, J., & Fernandez, K. (2000b). The antecedents and consequences of trust in online purchase decisions. *Journal of Interactive marketing, 16*, 47–63.
Miyazaki, J., & Fernandez, K. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs, 35*, 27–44.
Molla, A., Taylor, R., & Licker, P. S. (2006). E-commerce diffusion in small Island countries: The influence of institutions in Barbados. *The Electronic Journal of Information Systems in Developing Countries, 28*, 1–15.

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *The Journal of Marketing, 1*, 81–101.
Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing, 21*, 5–15.
Patton, M. A., & Jøsang, A. (2004). Technologies for trust in electronic commerce. *Electronic Commerce Research, 4*, 9–21.
Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*, 37–59.
Pichler, R. (2000). *Trust and reliance–enforcement and compliance: Enhancing consumer confidence in the electronic marketplace* (Doctoral dissertation). Stanford University, California.
Reichheld, F. F., & Schefter, P. (2000). E-loyalty. *Harvard Business Review, 78*, 105–113.
Romdhane, C. (2005). Security implications of electronic commerce: A survey of consumers and businesses. *Internet Research: Electronic Network Applications and Policy, 9*, 372–382.
Shon, T. H., & Swatman, P. M. (1998). Identifying effectiveness criteria for Internet payment systems. *Internet Research, 8*, 202–218.
Theodosios, T., & George, S. (2005). Concept of security and trust in electronic payment. *Computers and Security, 24*, 10–15.
Thrassou, A., Vrontis, D., & Kokkinaki, A. (2010). Internet consumer behavior in Cyprus. In S. Singh (Ed.), *Handbook of business practices and growth in emerging markets* (pp. 433–453). Singapore: World Scientific , Pte.
Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security, 24*, 10–15.
Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets, 17*, 68–81.
Wright, D. (2002). Comparative evaluation of electronic payment systems. *INFOR, 40*, 71–85.
Wu, J. H., & Wang, S. C. (2005). What drive mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information & Management, 42*, 719–729.
Yahid, B., Shahbahrami, A., & Nobakht, M. B. (2013, April). Providing security for e-wallet using e-cheque. In e-Commerce in Developing Countries: With Focus on e-Security (ECDC), 2013 7th Intenational Conference on (pp. 1–14). IEEE.
Zwass, V. (1996). Electronic commerce: Structures and issues. *International journal of electronic commerce, 1*, 3–24.

Appendix 1: Questionnaire

QUESTIONNAIRE

This academic project is concerned with the relationship between perceptions of security and trust in e-payment systems and use of e-payment systems. Taking the time to complete the questionnaire is vitally important and your contribution is highly appreciated. Your responses will remain anonymous and be treated in the strictest of confidence. There are no right or wrong answers; what really matters is your honest opinion. Thank you very much for your help.

Q1: Please indicate the extent to which you agree or disagree with each of the following statements.
(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) Electronic payment system (EPS) always calls for user name and password when you log-in.	1	2	3	4	5	6	7
b) Various measures are provided by EPS to authenticate.	1	2	3	4	5	6	7
c) The site offers you an opportunity to change any of payment information before completing the final stage of the payment process.	1	2	3	4	5	6	7
d) The site provides a step to verify a payment before the finalization of the actual payment.	1	2	3	4	5	6	7
e) The site typically displays a summary of the payment information (cost, payee…) and the final payment amount.	1	2	3	4	5	6	7
f) A confirmation is sent to you through one of several available methods (online, email, etc.) to assure you that payment has in fact been received.	1	2	3	4	5	6	7

Q2: Please indicate the extent to which you agree or disagree with each of the following statements.
(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) Your personal information, such as contact details or payment details, has never been stolen because of using EPS.	1	2	3	4	5	6	7
b) Your personal information has not been released to other third parties by EPS service providers for any other purposes.	1	2	3	4	5	6	7
c) The payment amount or transaction data displayed on EPS is always accurate.	1	2	3	4	5	6	7
d) You think that the EPS transaction data transferred over the Internet is securely protected.	1	2	3	4	5	6	7
e) Payment services are always available at any time in a day.	1	2	3	4	5	6	7
f) Temporary or sudden errors frequently occur during EPS transaction.	1	2	3	4	5	6	7

Q3: Please indicate the extent to which you agree or disagree with each of the following statements.
(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) The site offers detailed explanations as to how to review, cancel modify or record a payment.	1	2	3	4	5	6	7
b) The site provides security statements on security-policy, contact information under emergency, technical descriptions and functionalities of the EPS.	1	2	3	4	5	6	7
c) You do not need to make any special or extraordinary efforts to find security-related statements.	1	2	3	4	5	6	7
d) Your concerns on security issues can be easily found from frequently asked questions (FAQ) or a help section.	1	2	3	4	5	6	7
e) Security-related statements are drafted in an easily understandable way and largely free from technical words.	1	2	3	4	5	6	7
f) The security-related statements are drafted in a wording that attracts your attention.	1	2	3	4	5	6	7

Q4: Please indicate the extent to which you agree or disagree with each of the following statements.
(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) I perceive EPS as secure.	1	2	3	4	5	6	7
b) I perceive the information relating to user and EPS transactions as secure.	1	2	3	4	5	6	7
c) The information I provided in previous EPS is helpful for secure payment transactions.	1	2	3	4	5	6	7
d) I do not fear hacker invasions into EPS.	1	2	3	4	5	6	7

Q5: Please indicate the extent to which you agree or disagree with each of the following statements.
(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) I trust each participant, such as seller and buyer, involved in EPS.	1	2	3	4	5	6	7
b) I trust the security mechanisms of EPS.	1	2	3	4	5	6	7
c) I trust EPS services.	1	2	3	4	5	6	7
d) I do not fear hacker invasions into EPS	1	2	3	4	5	6	7

Q6: Please indicate the extent to which you agree or disagree with each of the following statements.

(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) I have a considerable experience on ordering a product/service from the web.	1	2	3	4	5	6	7
b) I have a considerable experience in doing payments via credit cards over the internet.	1	2	3	4	5	6	7
c) I have a considerable experience on electronic payment systems other than credit cards (money transfers, PayPal, etc.) on the Internet in general.	1	2	3	4	5	6	7
d) I have started using online transaction and payment systems considerably a long time ago.	1	2	3	4	5	6	7
e) I still frequently benefit from online payment systems.	1	2	3	4	5	6	7

Q7: Please indicate the extent to which you agree or disagree with each of the following statements.

(Please tick /circle only one box per line)

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
a) I use EPS more often than others.	1	2	3	4	5	6	7
b) I am using currently and will continue to use EPS.	1	2	3	4	5	6	7
c) I believe EPS use will increase.	1	2	3	4	5	6	7

Q8. Please specify below your:

(Tick only one box per question)

Q8a) Gender: Male 1

Female 2

Q8b) Age _____

Q8c) Marital Status: Single 1

Married 2

Divorced 3

Other (Please specify): _____

Q8d) What is your occupation? _____

Q8e) Highest Education Level:

Primary School 1

Secondary School 2

High National Diploma (HND) 3

First Degree 4

Masters Degree 5

PhD 6

Other (Please specify): _____

Q8f) Annual Income (optional):

Up to 20,000 1

20,001 - 40,000 2

40,001 - 60,000 3

More than 60,001 4

Thank you very much for your participation