8-7-2011

Are All Commercial Websites Created Equal? Web Vendor Reputation and Security on Third Party Payment Use

Ruth C. King
Fayetteville State University, ruthking@gmail.com

Richard A. M. Schilhavy
University of North Carolina at Greensboro, raschilh@uncg.edu

Are All Commercial Websites Created Equal? Web Vendor Reputation and Security on Third Party Payment Use

Ruth C. King
Fayetteville State University
ruthking@gmail.com

Richard A. M. Schilhavy
University of North Carolina at Greensboro
raschilh@uncg.edu

ABSTRACT

New web vendors emerge daily as business-to-consumer e-commerce grows substantially over the years. However, new web vendors may be regarded with skepticism in an existing marketplace, and may require third party support to reduce uncertainty. This study investigates the effect of consumer's perceived security and reputation of web vendors on consumer's purchase intention and third party payment choice. Our study examines under what condition adopting a reputable third party payment system is beneficial to web vendors. Applying trust transference theory, we found that website with high reputation and high security may not benefit from having a third party payment presence, while website with low reputation and low security will benefit the most for having an alternative financial payment mechanism. Our study also found that online consumers tend not to choose to use third party payment system when the website is perceived as high security regardless of the reputation of the website.

Keywords

Reputation, security, trust, purchase decision, purchase intention, third party payment

INTRODUCTION

Are all B2C websites created equal? Assuming the "location, location, location" marketing imperative is paramount; B2C websites may indeed be equal since no two web vendors have the same relative distance to their potential customers. However, since online consumers and vendors do not "see" each other and only interact with each other through the websites, many factors can become significant barriers for consumers to shop on a particular website such as distrust (McKnight & Choudhury, 2006), security (Yenisey, Ozok, & Salvendy, 2005), and poor website design (Moss, Gunn, & Heller, 2006). Studies have shown that online security concerns have always been major obstacles for e-commerce success (Ahuja, Gupta, & Raman, 2003; Kim, Ferrin, & Rao, 2008). The U.S. Census Bureau (2010) reported that online retail sales has an average annual growth rate of 21 percent from 2002 to 2008, compared with 4 percent for total retail sales. However, in 2008, $21 billion in online sales spending was lost due to consumers' information security and identity theft concerns (Merchant, 2009). To address these concerns about security, web vendors will pursue many different mechanisms to reduce perceived uncertainty and risk of the web vendors, including indicators of security and reputation. Some web vendors may adopt reputable third party payment systems such as Google Checkout, PayPal, or NetPay to provide additional assurance and convenience for online consumers. *This study investigates how web vendor reputation and security influences consumer perceptions and purchasing intentions. Furthermore, do online consumers prefer third party payment platforms when dealing with web vendors that have low reputation and poor security?*

LITERATURE REVIEW AND RESEARCH HYPOTHESES

Online Consumer Perceptions

Based on the theory of reasoned action (TRA) (Ajzen, Fishbein, & Heilbroner, 1980), trusting beliefs in the web vendor form trustworthiness towards the web vendor by the customers. Trusting beliefs are a person's perceptions of the trustworthiness of another object or agent. Trusting beliefs occur when the trustor perceives that the trustee possess characteristics that will benefit the trustor, and those benefits are likely to be realized (McKnight, Choudhury, & Kacmar, 2002). McKnight and others (2002) have proposed three characteristics of trustworthiness perceptions of an agent or object are relevant in forming trusting beliefs. These three characteristics are *competence* (ability of the trustee to do what the truster needs), *benevolence* (trustee caring and motivation to act in the truster's interests), and *integrity* (trustee honesty and promise keeping). Trusting belief is found to be associated with risk perception and willingness to purchase online (Kim, Ferrin, et al., 2008).

People make important buying decisions based in part on their level of trust in the product, salesperson, and/or the company (Hosmer, 1995). However, a customer often does not interact with any physical entity or representative of the web vendor when purchasing similar products online. Therefore, it becomes crucial for web vendors to manage how customers perceive the company, and to cultivate a solid reputation and ensure the utmost security for online consumers. Research has identified

several crucial dimensions of online consumer perceptions towards the web vendor: *perceived trustworthiness* (McKnight, et al., 2002), *perceived reputation* (Jarvenpaa, Tractinsky, & Vitale, 2000), and *perceived security* (Casalo, Flavián, & Guinalíu, 2007; Chang & Chen, 2009; Yenisey, et al., 2005).

Perceived reputation is the extent to which buyers believe that the selling organization is honest and concerned about its customers (Doney & Cannon, 1997). For online vendors entering the market, reputation could be transferred from a variety of mechanisms, such as buzz and word-of-mouth or a vendor's "brick and mortar" existence. For example, companies such as Barnes and Nobles with a strong physical presence prior to introducing online services transfers a higher level of reputation absent for other web vendors who do not have a physical storefront. As perceived reputation of a web vendor has strong impact on the customer's overall perception towards (Jarvenpaa, et al., 2000), a positive perception toward a web vendor's reputation will reduce a consumer's uncertainty and increase assurances and trust about the web vendor (Casalo, et al., 2007). Although some suggested that perceived reputation as the antecedent of and fully mediated by perceived trustworthiness (Pavlou & Dimoka, 2006), it is our assertion that the direct effect of the reputation of the web vendor also requires consideration. Initial formations of trust are crucial in supporting online consumer perceptions and behaviors (McKnight, et al., 2002); however, trust may become less salient as the online consumer continues interacting with the web vendor, or as the web vendor becomes more reputable in the marketplace. In other words, the reputation of web vendor may precede any necessity of formations of trust. Therefore, we hypothesis the following:

Hypothesis 1a: Online consumers are more likely to purchase from websites perceived as having higher reputation.

Web vendors employ multiple security mechanisms to protect against security threats. However, most of these precautions are highly technical and not transparent to online consumers who may not have the expertise to readily comprehend the implications of specific security mechanisms. Moreover, in situations that involve high risk people's subjective, intuitively grounded perceptions are highly variable and may deviate significantly from objective realities (Powell & Leiss, 1997). To provide assurance and develop consumer trust online, it becomes crucial for web vendors to not only incorporate the technology necessary to protect data and consumer information, but also employ mechanisms by which online consumers feel more secure. This aspect, known as *perceived security*, is defined as "the level of security that users feel when they are shopping on e-commerce sites" (Yenisey, et al., 2005, p. 259). Extant research (Dong-Her, Hsiu-Sen, Chun-Yuan, & Lin, 2004; Furnell & Karweni, 1999) identifies the lack of perceived security for online consumers as a primary obstacle to e-commerce growth. It is important for ecommerce companies to deploy technical measures for securing transactions as well as to take steps that will increase customers' perceived security on their web sites. Based on these assertions, we hypothesize that:

Hypothesis 1b: Online consumers are more likely to purchase from websites perceived as having higher security.

Third Party Platforms and Trust Transference

Traditional shopping channels, such as brick-and-mortar stores, have a physical storefront so consumers can make purchase decisions based through a more tangible experience coupled with pre-established notions of brand name and company image, affording a more direct and effective method of forming trust online. Online vendors, especially new vendors on the marketplace, do not have such traditional trust building mechanisms to help build consumer confidence and trust. However, new web vendors may transfer trusting beliefs one trusted entity (e.g. a sponsor website or third party platform) to another unknown entity (e.g. a new web vendor) according to trust transference theory (Stewart, 1999, 2003). The concept of trust transference is based on the cognitive balance theory (Heider, 1958), which focuses on the valence of relations between actors. Balance theory posits that a triad is balanced when there exists "a harmonious state…in which the entities and the feelings about them fit together without stress" (Heider, 1958, p. 180). Whenever a person has dissimilar level of relationships with associated parties, the individual experiences dissonance, which people attempt to reduce over time (Festinger, 1954, 1957). The balance might be achieved in two ways: bringing their relationships into balance either by changing the valence of their relationship to one of the objects or by changing their perception of the relationship between the objects. Given two positive relations (e.g., X trusts Y and Y is associated with Z), balance theory predicts that the third relation will also be positive (i.e., X will trust Z). Stewart (1999, 2003) suggested that in forming this third relation, perceptions of trust may be transferred. As suggested by the transference mechanism, when confronted with a new target, an individual bases trust in the new target on trust in associated targets in a way that balance will exist.

Conducting financial transactions online is a primary reason why online consumers are concerned about privacy and security (Kim, 2008; Kim, Ferrin, et al., 2008). Two popular transaction channels/platforms are marketplace (e.g. Amazon.com) and third party payment systems (e.g. PayPal, Google Checkout). The third party payment systems have been designed specifically to facilitate financial transaction (Latour, 1999) as an alternative payment scheme (Choudhary & Tyagi, 2009). Consistent with trust transference theory (Stewart, 1999, 2003), facilitating financial transactions with a highly trustworthy

third party will positively influence the perception of online customers and increase purchasing intention (Choudhary & Tyagi, 2009). Therefore, web vendors with low reputation may seek these third party payment systems to increase the assurance of online consumers. Reputation have been shown to significantly influence the formation of trust of online financial services (Casalo, et al., 2007). Therefore, online consumers shopping at highly reputable stores will be less likely to use third party platforms because the trust transference mechanisms is not necessary—the reputable vendor is already highly trusted. However, in order to reduce uncertainty and engender trust with less reputable web vendors, consumers will seek more reputable third party platforms. Therefore, the following is hypothesized:

> Hypothesis 2a: Online consumers are more likely to use third party checkout to purchase from websites that are less reputable.

But interestingly almost none of this existing literature has taken into account the fact that security features may play different role based on the company profile. For example, indicators of security features (Yenisey, et al., 2005) may have a more meaningful impact to consumers for a new company that is less known or less reputable in the marketplace in comparison to a well-established renowned company. However, the effectiveness of these security feature indicators, such as third party security seals, has been inconsistent (Belanger, Hiller, & Smith, 2002; Kim, Steinfield, & Lai, 2008; McKnight, Kacmar, & Choudhury, 2004). Nevertheless, some authors have reported that online consumers who perceived the website as more secure are more satisfied and loyal (Chang & Chen, 2009), and have stronger purchasing intentions and commitment to the web vendor (Casalo, et al., 2007). Therefore, considering that security feature indicators are inconsistent in improving online consumer's perceptions, but perceptions of security seem to have a strong influence, web vendors may actively seek third parties to create a perception of security that the website itself does not provide. By extension, these web vendors will be more likely to offer and promote third party platforms, and online consumers in these environments will be more likely to use them to due to the lack of security assurances. Therefore, we hypothesis the following:

> Hypothesis 2b: Online consumers are more likely to use third party platforms to purchase from websites that are less secure.

RESEARCH DESIGN AND METHODOLOGY

Our research question and hypotheses necessitated additional control over an online customer's shopping experience; therefore, an experimental methodology couple with a structured questionnaire was chosen to address the research problem. The hypotheses proposed were tested through a laboratory experiment using a 2×2 factorial design (i.e., two levels of reputation, and two levels of security). A collection of web vendors that used third party payment systems were selected and evaluated using objective measures of reputation and security to properly categorizing them into the four treatment conditions. Figure 1 details the experimental design, vendor websites used, sample sizes in each treatment group, and hypothesized levels of purchasing intention and preference for third party payment platforms.

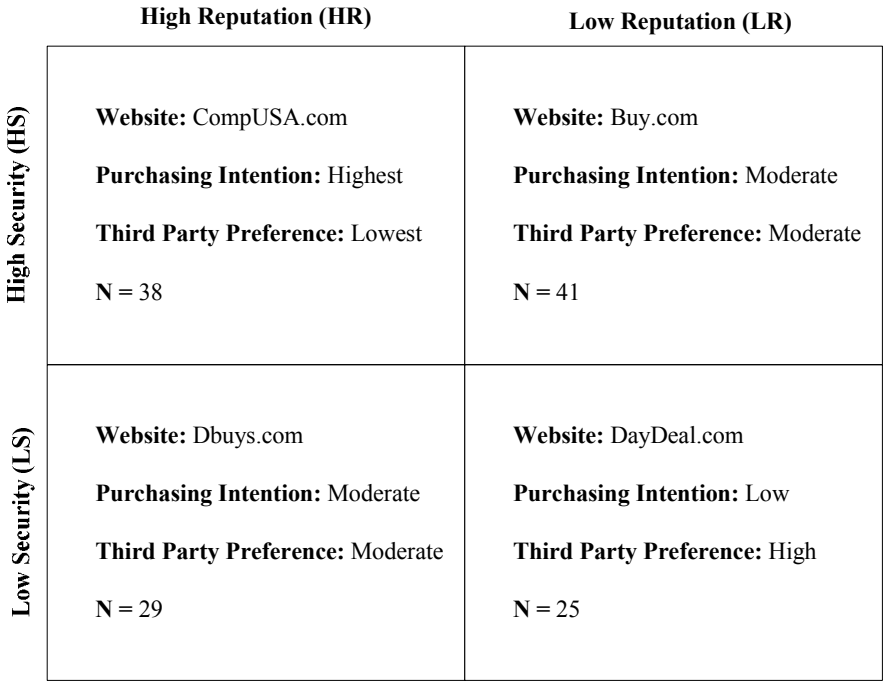

Figure 1: Research design of experimental conditions

The reputation levels of the web vendor are high reputation (HR) and low reputation (LR). The categorization of web vendor's reputation is based upon: (1) annual sales, (2) appearance in the trade journals and popular magazines, and (3) how long the company has been in the business. The categorization of web vendors as high or low reputation was validated using a small sample from the population, as well as other information systems researchers to ensure the categorization achieved face validity.

The security levels of the web vendor are classified as high security (HS) and low security (LS) based on the existence of security features indicators on the web vendor's website. These criteria have been identified based on the existing literature and a content analysis of more than 100 websites. The most widespread methods that web vendors use to increase the perceived security of the customers are (1) third party security seal or web assurance seal (Belanger, et al., 2002; Kim, Sivasailam, & Rao, 2004; Kim, Steinfield, et al., 2008), (2) top management's endorsement (Yenisey, et al., 2005), (3) login and password authentications are used extensively to provide secure transaction environments (Yenisey, et al., 2005), (4) security features are distributed consistently within the site (Yenisey, et al., 2005), and all file transfers are made over secure internet communication lines (Chellappa & Pavlou, 2002; Yenisey, et al., 2005). These indicators of security features designed for increasing perceived security of online consumers.

Several third party payment mechanisms exist in the e-commerce market, including PayPal, Amazon, and Google Checkout. Although some of the web vendor implements multiple third party payment options, Google Checkout was the common third party payment mechanism among the websites selected. Therefore, third party payment preferences represent a preference for using Google Checkout over the web vendor's payment mechanism.

The subjects were randomly assigned to one of the four treatment conditions. On average 30 subjects were assigned to each treatment group although there is some variation between treatment conditions. The procedure was as follows:

1. The subject was requested to visit the particular website (based upon the treatment group assigned) to purchase a gift for a significant member in their life.
2. Once a subject has finished browsing the website and found the product to purchase, s/he has to add that product to the shopping cart and proceed to the checkout point.
3. The subjects were asked to stop and close the browser upon directly before providing payment information.
4. Subjects were asked to complete a survey based on the perception s/he had developed towards the web vendor and the vendor's website during their shopping experience.

Measurement and Sample

The instrument—a structured questionnaire—consists of several sections. Each section was designed to investigate the factors described the aforementioned factors in the research design. Almost all of the items of the instrument have been collected from the existing literature (see Table 1). The third party checkout preference, or Google Checkout preference, is measured using two items: one assessing the subject's preference for Google Checkout over the web vendor's option, and the second measuring checkout preference assuming identical pricing.

Construct/Factor	Sub-factor	Reference	Operationalization
Security Features Indicators	Perceived Security	Chellappa & Pavlou (2002) Flavián & Guinalíu (2006)	Chellappa & Pavlou (2002) Flavián & Guinalíu (2006)
	Third Party Seal	Belenger, et al. (2002) Kim, et al. (2004) Kim, et al. (2008)	Belenger, et al. (2002) Kim, et al. (2004) Kim, et al. (2008)
	Top Management Endorsement	Yeinsey, et al. (2005)	Yeinsey, et al. (2005)
	Login Authentication	Yeinsey, et al. (2005)	Yeinsey, et al. (2005)
	Security Feature Distribution	Yeinsey, et al. (2005)	Yeinsey, et al. (2005)
	Secured Socket Layer (SSL)	Chellappa & Pavlou (2002)	Chellappa & Pavlou (2002)
Transaction Channel/Platform	Third Party Checkout Preference	Latour (1999) Choudhary & Tyagi (2009)	Latour (1999) Choudhary & Tyagi (2009)

Table 1: Summary of Constructs, Definitions, and Operationalizations

A chi-square analysis revealed no significant differences in gender, level of study, experience with internet, or online purchase experience among the groups. A one-way ANOVA further revealed no significant differences between the groups in terms of age, number of years in education, or average time spent on the Internet. A demographic profile of the sample may be found in Table 2.

Measure	Value	Frequency	Percentage
Gender	Male	66	50.4
	Female	65	49.6
Age	18-22	95	74.2
	23-30	14	10.9
	>30	19	14.8
Education	High School	6	4.6
	Some college	84	64.1
	Bachelor	25	19.1
	Master & Above	16	12.3
Internet Use (Hours/Day)	1-2 hours	28	21.4
	2-4 years	53	40.2
	4-6 hours	26	19.8
	More than 6 Hours	24	18.2
Internet Purchases (Monthly)	< $100	110	87.3
	$101 -$300	14	11.1
	>$300	2	1.6
Occupation	Full-time Employee	27	20.6
	Part-time Employee	35	26.7
	Full-time Student	68	51.9
	Other	1	0.8

Table 2: Demographic statistics of sample

ANALYSIS AND RESULTS

A factor analysis of the measurement items was performed to confirm construct validity. Cronbach's α was calculated for each construct to assess the reliability of each measure. Table 3 outlines the means, standard deviations, and Cronbach's α of each major construct in the study. With the exception of checkout preference, all reliabilities exceed suitable criteria for

exploratory research *(α > 0.7)*, while trust, security, and intention match criteria for predictive conclusions *(α > 0.95)* (Nunnally, 1967).

	Construct	Mean	SD	1	2	3	4	5
1	Purchase Intention	3.90	1.57	**(0.95)**				
2	Checkout Preference	0.46	0.42	-0.315 **	**(0.61)**			
3	Trust	4.88	0.96	0.422 **	-0.260 **	**(0.93)**		
4	Reputation	3.85	1.09	0.509 **	-0.164	0.533 **	**(0.74)**	
5	Security	4.61	1.04	0.555 **	-0.252 **	0.642 **	0.584 **	**(0.94)**

Table 3: Construct means, standard deviations, reliabilities, and cross correlations

Hypothesis Tests

Using a one-way ANOVA analysis and F-test (shown in Table 4), the results indicate that there are significant differences between the four treatment groups (high and low reputation and security) with regards to all dependent (checkout preference and buying intention) and control variables (trust, reputation, and security). A further breakdown comparing specific group differences may be found in Table 5.

Construct	F	Sig
Purchase Intention	9.991	< 0.001
Checkout Preference	8.674	< 0.001
Trust	3.971	< 0.01
Reputation	16.807	< 0.001
Security	7.711	< 0.001

Table 4: One-way ANOVA results for checkout preference, trust, reputation, security, and buying intention

Hypothesis H1a states that websites of higher reputation (HRHS and HRLS) will demonstrate a higher buying intention than websites of comparably lower security (LRHS and (LRLS). The results from Table 5 indicate that for the HRHS website there is significantly higher purchasing intention than either the LRHS *(Δx̄ = 0.91, p < 0.05)* or LRLS *(Δx̄ = 1.93, p < 0.001)* websites. Unsurprisingly, the difference is much greater for the low security websites than the high security website. However, when comparing the purchasing intentions of the HRLS website, we find no evidence supporting a difference of buying intentions for the LRHS website *(Δx̄ = 0.51)*, but substantial evidence for the LRLS website *(Δx̄ = 1.53, p < 0.001)*. Therefore, hypothesis H1a is partially supported, with only the HRLS-LRHS relationship being an exception.

Hypothesis H1b states that websites with higher security (HRHS and LRHS) will have a demonstrably higher buying intention than websites with comparatively lower security (HRLS and LRLS). The results from Table 5 indicate a significantly higher buying intention for the HRHS website than the LRLS website *(Δx̄ = 1.93, p < 0.001)*, but not the HRLS website *(Δx̄ = 0.40)*. This suggests that a higher observed security, when combined with a stronger reputation, translates into strong buying intention; however, a higher security alone may not account for a stronger purchasing intention. There is no evidence of a difference of purchasing intention between the HRLS and LRHS websites *(Δx̄ = 0.51)*. These results perpetuate the ambiguity between the "middle cases," such as the HRLS and LRHS websites, and further demonstrate an interaction between reputation and security. Finally, comparing the difference between the low reputation treatments, there is some evidence a difference between the LRHS and LRLS websites *(Δx̄ = 1.02, p < 0.05)*. Ultimately, hypothesis H1b is partially supported, but only for websites of low reputation.

		Mean Difference (I - J)				
Category (I)	**Category (J)**	**Google**	**Intention**	**Trust**	**Reputation**	**Security**
HRHS	HRLS	−0.20 *	0.40	0.24	0.45 *	0.13
	LRHS	−0.14	0.91 *	0.77 **	1.47 ***	1.05 ***
	LRLS	−0.50 ***	1.93 ***	0.36	1.19 ***	0.49 *
HRLS	LRHS	0.06	0.51	0.53 *	1.01 ***	0.92 ***

	LRLS	−0.30 **	1.53 ***	0.12	0.73 **	0.36
LRHS	LRLS	−0.37 **	1.02 *	0.41	−0.28	−0.56 *

** $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$*

Table 5: One-way ANOVA results for checkout preference, trust, reputation, security, and buying intention

Hypothesis H2a states that websites of high reputation (HRHS and HRLS) will show lower preferences for using third party platforms compared with other websites of lower reputation (LRHS and LRLS). The results in Table 5 indicate that the HRHS website has significantly lower preferences for Google checkout when compared with the LRLS website *(Δx = −0.50, $p < 0.001$)*, but not compared with the LRHS website *(Δx = −0.14)*. Comparing the HRLS website shows similarly conflicting results. While there is strong evidence of a checkout preference difference between the HRLS and LRLS websites *(Δx = −0.30, $p < 0.01$)*, there is no evidence of a difference between the HRLS and LRHS websites *(Δx = 0.06)*. Therefore, hypothesis H2a is partially supported with the LRHS website being the exception.

Hypothesis H2b states that websites of high security (HRHS and LRHS) will show lower preferences for using third party platforms. The results indicate that the HRHS website has a significantly lower preference to use a Google checkout over the vendor's checkout compared with the HRLS *(Δx = −0.20, $p < 0.05$)* and LRLS *(Δx = −0.50, $p < 0.001$)*. In addition, the LRHS website also showed a significantly lower preference for using Google checkout *(Δx = −0.37, $p < 0.01$)* compared with the LRLS website. However, there is no evidence of checkout preference differences between the HRLS and LRHS websites *(Δx = 0.06)*. Therefore, hypothesis H2b is partially supported, where the LRHS website, again, is the exception.

Interestingly, although there was no evidence of differences of checkout preference and purchasing intentions between the HRLS and LRHS websites, substantial evidence respondents perceived the HRLS website as not only *more reputable (Δx = 1.01, $p < 0.001$)*, but also *more secure (Δx = 0.92, $p < 0.001$)*, than the LRHS website. These results further suggest that perceptions of high reputation and high security interact when buyers are choosing between checkout and purchasing options. Furthermore, vendors may supplement a low reputation in the market for a higher observed security, through the use of security statements, third party seals, etc. Finally, the results may also suggest perceived security may deviate from observed security, possibly due to a higher perceived reputation.

DISCUSSION AND CONCLUSION

Although third party payments systems have gained prominence in the past decade, scholarly research in the area remains relatively recent (Choudhary & Tyagi, 2009) and deserves further examination. Our study investigates consumer's decision to use third party payment systems, and how this decision changes between websites of different reputation and security.

Two explanations are posited as to these inconsistent findings. First, these studies may not have accounted for other characteristics of web vendor perceived by the consumer, particularly reputation and trustworthiness. Second, these inconsistent findings may be due to a gulf between indicators of security

Two clear cases resulted from the study. First, consumer's using websites of high reputation and high observed security were much less likely to prefer a third party payment platform and more likely to purchase from the vendor. Second, consumer's using websites of low reputation and security were more likely to prefer the third party payment system. This suggests that when consumers are dealing with markedly different websites on the basis of reputation and security, third party payment systems are an effective and preferred means of mitigating the uncertainty of new web vendors, who may not have sufficient brand recognition and security features to entrust consumers. Our findings are consistent with trust transference theory (Stewart, 1999, 2003), where the well-known and highly reputable third party payment system was preferred in low reputation and low security situations.

However, online consumer's decision to purchase or preference towards third party payments were not particularly influenced by web vendors demonstrating high security features if the vendor was not also reputable. Many of the original hypotheses predicting clear differences between high and low reputation and security were only partially supported. The "moderate" cases (high reputation and low security, low reputation and high security) showed little or no difference in terms of checkout preference and purchasing intention when compared with their counterparts. As previously discussed in the literature review, perceptions of reputation and trust of web vendors are undoubtedly related (Pavlou & Dimoka, 2006), and no doubt perceptions of security and assurances (Yenisey, et al., 2005) are also linked with a company's reputation. The interaction between a web vendor's reputation and perceptions of security deserves further investigation, as evidenced in particular by the perceptions of security between the high reputation, low security and low reputation, high security.

One limitation of our study concerns the apparent failed manipulation check of highly secure website resulting in low perceptions of overall security. There are several plausible explanations for this limitation. First, web vendors with low

reputation may be negatively affected by the low reputation, creating perceptions of poor security despite an abundance of visible security features. Second, visible security features may not be an effective method of engendering perceptions of a highly secure website. Other features such as a well designed websites (legitimation), strong brand name (reputation), or third party promotion (status) (Bitektine, 2011) may be more consistent with perceptions that the website is more secure. Consumers may suffer from a cognitive dissonance where perceptions of security are inconsistent with observed security features of the website.

In conclusion, our study demonstrates that online consumer's preference for the use of third party payment systems is heavily influenced by the web vendor's reputation, but only partially influenced by the prevalence of security features. Consistent with trust transference theory, online consumer's sought out a more reputable third party when using websites that were both less secure and less reputable. Conversely, consumer's buying intentions were much higher for websites that were both more reputable and more secure. Future research should investigate the interaction between reputation and security in relation to third party platform preference, and the cognitive disassociation between reputation, security features, and perceived security.

REFERENCES

Ahuja, M., Gupta, B., & Raman, P. (2003). An Empirical Investigation of Online Consumer Purchasing Behavior. *Communications of the ACM, 46*(12), 145-151.

Ajzen, I., Fishbein, M., & Heilbroner, R. L. (1980). *Understanding attitudes and predicting social behavior* (Vol. 278): Prentice-Hall Englewood Cliffs, NJ.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

Bitektine, A. (2011). Toward a theory of social judgments of organizations: The case of legitimacy, reputation, and status. *Academy of Management Review, 36*(1), 151-179.

Bureau, U. S. C. (2010). E-commerce 2008 E-Stats. Retrieved February 17, 2011, from http://www.census.gov/econ/estats/2008/2008reportfinal.pdf

Casalo, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability, and reputation in the development of online banking. *Online Information review, 31*(5), 583-603.

Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electric commerce. *Information & Management, 46*, 411-417.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368.

Choudhary, V., & Tyagi, R. (2009). Economic incentives to adopt electronic payment schemes under competition. *Decision Support Systems, 46*, 552-561.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *the Journal of Marketing, 61*(2), 35-51.

Dong-Her, S., Hsiu-Sen, C., Chun-Yuan, C., & Lin, B. (2004). Internet security: malicious e-mails detection and protection. *Industrial Management & Data Systems, 104*(7), 613-623.

Festinger, L. (1954). A theory of social comparison processes. *Human Relations, 7*, 117-140.

Festinger, L. (1957). *A theory of cognitive dissonance*. Evanston, IL: Row, Peterson.

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management, 43*(1), 1-14.

Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet research, 9*(5), 372-382.

Heider, F. (1958). *The Psychology of Interpersonal Relations*. John Wiley & Sons: New York.

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of management review, 20*(2), 379-403.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1), 45-71.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13-45.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.

Kim, D. J., Sivasailam, N., & Rao, H. R. (2004). Information assurance in B2C websites for information goods/services. *Electronic Markets, 14*(4), 344-359.

Kim, D. J., Steinfield, C., & Lai, Y. J. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44*(4), 1000-1015.

Latour, A. (1999, November 2009?). PayPal electronic plan may by on the money in years to come. *The Wall Street Journal Interactive Edition*.

McKnight, D. H., & Choudhury, V. (2006). *Distrust and trust in B2C e-commerce: Do they differ?* Paper presented at the International Conference on Electronic Commerce, New York, NY.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *Journal of Strategic Information Systems, 11*(3-4), 297-323.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business. *Electronic Markets, 14*(3), 252-266.

Merchant, M. (2009). Survey says: $21 Billion Lost Last Year in Online Sales. Retrieved February 17, 2011, from http://www.multichanelmerchant.com/ecommerce/news/0324-online-sales-survey/

Moss, G., Gunn, R., & Heller, J. (2006). Some men like it black, some women like it pink: consumer implications of differences in male and female website design. *Journal of Consumer Behaviour, 5*, 326-341.

Nunnally, J. C. (1967). *Psychometric Theory*. New York, NY: McGraw Hill.

Pavlou, P. A., & Dimoka, A. (2006). The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research, 17*(4), 392.

Powell, D. A., & Leiss, W. (1997). *Mad cows and mother's milk: the perils of poor risk communication*: McGill Queens Univ Press.

Stewart, K. J. (1999). *Transference as a means of building trust in World Wide Web sites.* Paper presented at the International Conference on Information Systems.

Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science, 14*(1), 5-17.

Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology, 24*(4), 259-274.