Perceived information security, financial liability and consumer trust in electronic commerce transactions

Ramnath K. Chellappa and Paul A. Pavlou

Introduction

The introduction of new information technologies has always been accompanied by security concerns (Clarke, 1988; Mason, 1986), and the future of electronic commerce (EC) depends on controlling information security threats, enhancing consumer security perceptions (Friedman et al., 2000; Shneiderman, 2000), and building trust (Hoffman et al., 1999; Keen, 2000). According to a study by Business Week (2000), 61 per cent of the survey respondents indicate that they would transact on the Internet if the security and privacy of their personal information could be adequately protected. Likewise, Internet retailers are also subject to security attacks and intrusions by hackers, resulting in high costs for the protection of their systems. These incidents not only result in revenue losses for retailers, but also they project adverse perceptions of transactional security for consumers. Therefore, given the enormous investments to increase security and trust in EC (Lemos, 2001), it is important to understand and measure responses to these efforts better.

Trust has always been an important element in influencing consumer behavior toward merchants (Schurr and Ozanne, 1985) and has been shown to be of high significance in uncertain environments such as Internet-based EC environments (Fung and Lee, 1999). Indeed, Hoffman et al. (1999) have noted that consumers do not trust most Internet marketers enough to engage in “relationship exchanges” involving money and personal information. While a variety of factors such as store reputation and brand names may influence trust, one missing factor is the implicit comfort of face-to-face communication present in physical interactions. In addition, the global and unregulated nature of the Internet further emphasizes the need to build mechanisms for trusting the medium (Chellappa, 2001a). Therefore, it has been argued that trust would be favorably influenced by increase in perceptions of security and privacy in EC transactions (Chellappa, 2001b).

Even if it is feasible to measure objectively the degree of security inherent in every transaction (CERT, 2000; Miyazaki and Fernandez, 2000), it is unclear whether this measurement would readily correspond to the exact consumer perceptions of the security of
their personal information. In situations involving risk, the objective, scientific perspective is usually different from the subjective, intuitively grounded one (Powell et al., 1997) and such a difference can be pronounced in technology environments as shown in analysis of expert and novice perceptions during technology use (Schenk et al., 1998; Spence and Brucks, 1997; Swanson and Falkman, 1997). Thus, even if Internet retailers adhere to a scientific assessment of security based on technological solutions, it is consumer perceptions of security that would influence trust. Given that current research is limited in its understanding of information security perceptions on the Internet (Miyazaki and Fernandez, 2000) it is important to establish measures of perceived information security and its relationship to trust in EC transactions.

This paper identifies antecedents of consumer perceptions of security and hypothesizes its relationship to trust in EC transactions. The antecedents are derived from the set of technology mechanisms that are visible to consumers. Most, if not all EC transactions are conducted through Web browsers that connect to merchant sites. Furthermore, these browsers and Web sites commonly display visible security mechanisms such as an unbroken lock/key (encryption), statements about data protection and firewalls (protection), familiar and verifiable domain names (verification), and digital certificates (authentication) from trusted third parties. Thus it can be proposed that consumer perceptions of security are engendered through these visible mechanisms through processes of encryption, protection, verification and authentication. However, no empirical evidence has shown if these mechanisms have an impact on consumer perceptions of both security and trust, although some mixed evidence exists on the role of trusted third parties (Palmer et al., 2000) and the impact of security-related statements on purchase likelihood (Miyazaki and Fernandez, 2000). In addition to security perceptions, we investigate the role of limited financial liability as a potential surrogate of information security and thus influencing consumer trust. Since trust and risk perceptions are related (Koller, 1988) we can expect that if merchants absorb the monetary risk of a transaction trust perceptions would be significantly enhanced and security concerns would be alleviated.

The proposed hypotheses in this work were tested through an empirical study with 179 participants. While our metrics for the study's principal constructs show excellent measurement properties, further regression analysis provides considerable support for the proposed set of antecedents and consequences of perceived security. While we are able to verify empirically that the mechanisms of encryption, protection, verification and authentication indeed influence perceptions of security, our findings suggested that alleviation of monetary risk through limited liability clauses has only a small impact on consumer trust. Finally we discuss theoretical and practical implications of this study and propose several recommendations for EC research and practice.

Conceptual development

An EC transaction can be considered secure, if the information involved originates from the right entity and reaches the intended party without being observed, altered or destroyed during transit and storage. Historical origins point to why Internet transactions are fundamentally risky. The fact that the Internet was initially created primarily to share information and not to support business processes implies that no security mechanisms were implicitly included (Chellappa, 2001a). Moreover, the global nature of the Internet coupled with its decentralized operation reduces the effect of legal protection. With increasing EC activities, there has also been an increasing number of attacks on corporate networks (CERT, 2000). Therefore, it is now commonly accepted that without adequate mechanisms of control, EC transactions are highly susceptible to security threats.

Perceived information security
Perceived information security is defined as the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations. This definition captures a personal anticipation
rather than an objective measurement and denotes an intuitive perception for assessing risk. For instance, a 128-bit encryption objectively gives the odds of a hacker decrypting a message as one in $2^{128}$. Clearly it is unlikely that an average consumer would exactly perceive this probability. The use of the Internet for conducting transactions is a relatively recent phenomenon as compared with traditional transactions. Consumers implicitly accept certain elements such as the identity of the entities they are transacting with in traditional environments; hence, conventional assumptions are rightfully questioned in electronic transactions.

Literature in computer sciences provides several classifications of security break-in incidents, based upon the type of attack, goal of the attack, place and origin of the incident, etc. In the context of EC transactions, one can identify a topology of security threats at the point of origin, during transit, and at the point of storage or destination. Security threats may also be classified based on how the information is affected such as loss of confidentiality, integrity and availability. Another applicable taxonomy is based on the entities involved in the transaction; for instance, authentication, authorization and non-repudiation. Others have also proposed an action-based (Stallings, 1995) typology that focuses on specific types of compromise such as interruption, interception, modification and fabrication. These classifications very well serve their intended purpose such as to assess incidents and propose technical solutions. However, they are primarily indices for expert assessment of security threats. It has been argued that an information vacuum separates expert assessments and public perceptions of a situation involving risks (Powell and Leiss, 1997; Chellappa, 2001c). Consequently, expert assessment of information security and consumer perceived security should be regarded as two different constructs (Chellappa, 2001b). Therefore, it becomes equally important to investigate the nature and role of perceived information security in EC transactions.

**Perceived information security and trust in electronic transactions**

Practically all relationships require an element of trust, especially those conducted in the uncertain environment of EC (Fung and Lee, 1999). Developing trust between consumers and Internet retailers is critical for the continued growth of EC (Palmer et al., 2000), since trust plays an important role in influencing consumer behavior (Schurr and Ozanne, 1985). Others have also pointed out that trust is an essential element of EC and can be used as a strategic mechanism in EC relationships (Keen, 2000; Speier et al., 1998).

Consumer trust in EC transactions is defined as the subjective probability with which consumers believe that a particular transaction will occur in a manner consistent with their confident expectations. This definition captures two distinct components. First, it involves the traditional view of trust in a specific online entity, and second, it encompasses trust in the reliability and integrity of the communications medium. A particularly important attitude toward a medium is related to its perceived credibility or trustworthiness (Shimp, 1990). Given that the physical distance between consumers and marketers and the technological nature of the communications medium, trust in EC is primarily impersonal in nature compared with the traditional view of interpersonal trust (Culnan and Armstrong, 1999). Others (Doney and Cannon, 1997) maintain that trust can be developed by evaluating an entity’s competence to perform certain tasks. Thus one can argue that consumers subjectively form their own trust perceptions based on the medium’s ability to conduct secure transactions in a manner coherent with their expectations.

Trust also reflects a willingness to assume the risks of disclosure (Mayer et al., 1995). Consumers who provide personal information during transactions assume the risk of having this information endangered. As trust can be represented as a function of the degree of risk of a situation (Koller, 1988), trust in EC transactions may be alternatively viewed as a function of consumer risk. Risk has been defined “the possibility of an adverse outcome, and uncertainty over the occurrence, timing or magnitude of that adverse outcome” (Covello and Merkhofer, 1994). Risk in EC transactions is primarily created by threats to information security; therefore, when consumers perceive the risk of security to be minimal, they would trust in EC transactions:
H1. Perceived information security is positively related to trust in EC transactions.

Antecedents of perceived security
Following the theoretical antecedents of information security, perceived security should be influenced by implicitly perceptible measures that consumers encounter in the process of conducting EC transactions. While perceived information security is a subjective belief, the mechanisms that serve as the antecedents are built upon the self-assessment of various objective technological solutions. Therefore, on the Internet customer perceptions of information security is influenced by the mechanisms of encryption, protection, verification, and authentication.

Encryption
Encryption is defined as the process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called ciphertext). The encryption mechanisms are a combination of complex mathematical algorithms and keys. The process of encryption on the Web is implemented through the use of Web servers and browsers that are built with a technology referred to as secure socket layer (SSL). When such a technology is implemented, the consumer uses the https protocol instead of the traditional http protocol used to communicate with the Web server. The consumer is also introduced to this mechanism when Web sites include statements such as “click here for a secure transaction”, or through dialog boxes that browsers present indicating that the transaction is secure. Moreover, the image of an unbroken key or lock at the bottom of a browser indicates that the transaction is encrypted. Thus the visible nature of this mechanism should influence security perceptions:

H2. Encryption is positively related to perceived information security.

Protection
Protection can be defined as the process through which customers are satisfied with the fact that their personal information is adequately safeguarded by the entity collecting the information. This process is primarily concerned with intrusions at the point of storage or destination. Protection is typically signaled to the consumer in many ways such as through disclosure policies. While these policies are primarily oriented towards privacy protection, they also include assurance about who is collecting the data, how it is stored, and how inaccessible it is. Internet retailers typically employ the use of sophisticated firewall technologies to prevent unauthorized attacks or intrusions. The consumers are further introduced to this process through the media that often carry reports of popular Web sites that have been hacked into. Given that protection is a commonly encountered mechanism for information security, its extent should also influence consumer security perceptions:

H3. Protection is positively related to perceived information security.

Verification
The most important difference between electronic and traditional transactions is the lack of implicit identity verification associated with the transaction. For example, the familiarity of a “Sears” logo is often satisfactory enough for consumers to assure that they are indeed at the actual “Sears” department store. In cases where the consumer is not familiar with the store location, a yellow pages reference often suffices. In contrast, this experiential aspect of the transaction is clearly not present in the online world. It is not only easy for someone to create a phony Web page, but it is also equally possible for a malicious operator to create entirely spurious Web site. For example, do all consumers to know that Citibank is housed at “www.citibank.com” and not at “www.citibank.net” or even that Citibank is spelt with an “i” and not a “y” as in Citybank (Chellappa, 2001a)? Indeed there are numerous examples of sites that have actually benefited from typographical errors (Sullivan, 2000). Thus, when consumers are not aware of the exact domain name, they may rely upon established portals such Yahoo! (www.yahoo.com) to verify the accuracy of the domain name. Given that verification is a commonly met problem, its extent should be expected to influence consumer security perceptions:

H4. Verification is positively related to perceived information security.

Authentication
Authentication is defined as the process through which an Internet retailer can be
established through a trusted third party that guarantees that the retailer is indeed who claims to be. Independent third parties such as Verisign.com (www.verisign.com) provide these guarantees. The consumer is typically introduced to this mechanism through the presence of the authenticator’s seal on the entities’ Web site and through the exchange of a digital certificate when coupled with encryption. Given that authentication is another implicitly perceptible mechanism for information security, it should also influence consumer security perceptions:

\[ H5. \text{Authentication is positively related to perceived information security.} \]

**Limited financial liability**

Assuming that consumers are mostly concerned with the monetary aspect of EC transactions as opposed to the means through which they happen, one could argue that by removing the liability of a transaction (e.g. the monetary loss), consumers will perceive EC transactions as trustworthy. This argument is further strengthened by the fact that consumers are risk averse and more so in uncertain environments (Koller, 1988). There may be a reason why credit cards are the most common means for financial instruments in EC transactions. While consumers were earlier liable to a maximum of $50 on unauthorized credit card transactions, now Visa (www.visa.com) offers zero liability on such transactions, thus completely removing monetary risks from consumers. This shifts the burden of security threats from consumers to Internet merchants who accept credit card payments. It is therefore possible to argue that consumers would perceive that a transaction would occur in accordance with their confident expectations if the risks of disputed transactions were no longer their own responsibility. Although financial liability absorbs the monetary risk, it does not influence how security is maintained or perceived by consumers. Hence, limited financial liability is not an antecedent of perceived security but a potential surrogate, acting as an antecedent of trust:

\[ H6. \text{Limited financial liability is positively related to trust in EC transactions.} \]

**Control variables**

The proposed definition of trust in EC transactions is essentially twofold; trust in Internet retailers and also trust in the security of the underlying medium. To show that perceived security indeed engenders trust in EC transactions, we control for the effect of store reputation that has been shown to be an important antecedent of trust in EC transactions (Jarvenpaa et al., 2000). The complete conceptual framework is shown in Figure 1.

**Research methodology**

A comprehensive approach was used to develop new multi-item scales for perceived security and its antecedents that would have adequate measurement properties and allow us to test the six proposed hypotheses. Our scale development followed the recommendations of Straub (1989) and the standard psychometric scale development procedures (Bagozzi and Philips, 1982). Measures for trust and reputation were adapted from the extant literature (Chellappa, 2001b). The instrument was then reviewed for clearness and comprehensiveness by faculty and doctoral students. Then, the survey was pre-tested by personally administering it to several consumers to verify its appropriateness; these pretests revealed no major problems with any of the items. The anchors for all 23 items were “1 = strongly disagree” to “4 = neither agree nor disagree” and “7 = strongly agree” Likert-scales, and the eight principal constructs were operationalized as shown below:

1. **Perceived security (SEC).** Five new items were introduced based on the components of authentication, authorization, and non-repudiation (CERT, 2000). Authentication was measured by the degree of confidence that information will only reach the
appropriate party. Authorization was assessed by the degree of confidence that inappropriate parties would neither view nor store consumer information, and the retailer will not expose this information to others. Non-repudiation was captured based on beliefs that inappropriate parties will not manipulate consumer information during a transaction. Finally, a global item measured the overall confidence in the transaction’s security.

(2) **Trust (TRUST).** Four items captured this construct based on items by Ganesan (1994). These items were modified to account for the particular details of this study, such as the safety and reliability of the transaction, the possibility of something going wrong, and whether the retailer will promptly take measures in case of a problem.

(3) **Reputation (REP).** Three items on reputation were adapted from Doney and Cannon (1997), reflecting the extent of the retailer’s reliability, dependability, and reputation.

(4) **Encryption (ENCR).** Three items measured the construct of encryption. These items dealt with the risk related to sending private information over insecure transmission media.

(5) **Protection (PROT).** Two new items measured the extent of protection based on the consumers’ confidence in protection of their private information during storage in retailers’ systems.

(6) **Authentication (AUTH).** This construct was captured with two new items that measured the ability of third-party authentication mechanisms to assure the identity of Internet retailers.

(7) **Verification (VERI).** This construct was measured by two new items that captured the importance of validating the accuracy of domain names.

(8) **Monetary liability (LIAB).** This construct was measured by two new items that assessed the consumers’ confidence in financial institutions in terms of protecting consumers in cases of disputed or problematic transactions.

**Research setting**

An empirical study was performed to evaluate the proposed scales and validate the proposed set of interrelationships related to perceived security. Thus, participants were asked to assess the degree of perceived security they would expect from a prospective transaction with particular online retailers with whom they have little experience. We were particularly interested in the properties of perceived security when it is worded in a prospective meaning and is based on limited knowledge of the target retailer. In order to increase the heterogeneity of the sample, both graduate and undergraduate business school students were invited to participate in this survey. Favorable psychometric properties under these conditions would render support for the robustness and generalizability of the new measures. Hence, the sample was chosen to consist of two groups. Given a $200 reward as a raffle prize, 128 graduate and 51 undergraduate students responded to this online questionnaire for a total sample of 179 consumers.

The study controlled for the effect of retailer reputation as an antecedent of trust in buyer-seller relationships (Jarvenpaa et al., 2000). Reputation was manipulated by presenting two different target retailers to the respondents. Our concern was to vary the level of reputation appropriately to achieve high variance in responses. Hence, a pilot study was conducted with a sample of 150 consumers, who rated five different online retailers on two familiarity items adapted from Bruner and Hensel (1992). Based on this study, two retailers emerged: Buy.com (www.buy.com) had a mean value of 4.7 on a seven-point scale (STD = 2.1), while PCNation.com (www.pcnation.com) had a mean of 2.1 (STD = 2.0). Hence, half of the respondents were presented a hypothetical scenario where the target retailer was Buy.com, and the other half was given PCNation.com. Therefore, social desirability bias is limited in this study by not allowing participants to choose their desired merchants. In fact, manipulation check for reputation showed a significant difference ($p < 0.01$) between Buy.com (mean = 5.7, STD = 1.6) and PCNation.com (mean = 4.3, STD = 1.4).

**Data analysis**

A three-step sequence for assessing convergent and discriminant validity was employed:
(1) Exploratory factor analyses were conducted (with rotations) to detect high loadings on hypothesized factors and low cross-loadings.

(2) All eigenvalues were set to greater than unity, and the items were reduced to their principal constructs.

(3) Principal components analysis was used as the extraction method for confirmatory factor analysis with Varimax rotation (see the Appendix, Table AI).

All items tapping the same construct had extremely high correlations, loaded on their hypothesized factors, and their estimates were positive and significant, providing strong evidence of convergent validity (Bagozzi and Yi, 1988). In contrast, items tapping different constructs had very low correlations and low cross-loadings (< 0.4 level), rendering evidence of discriminant validity.

Factorial validity deals with whether the principal variables form distinct constructs. The overall factor solution has an acceptable loading pattern explaining 84 per cent of the variation; the eight-factor solution is acceptable with significant factor loadings ($p < 0.01$) and high comparative fit index ($0.94$), indicating a sufficient fit of the model to the data. Finally, measure validation was also examined for reliability by computing Cronbach’s alpha. As seen in Table I, all measures have excellent reliability levels ($> 0.80$) with an average of 0.87. The perceived security scale achieved a reliability of 0.93.

Results

The effect of perceived security, liability, and reputation on trust were assessed by least-squares regression analysis. The model was tested with normalized data and transformations were applied judiciously in accordance with Cook and Weisberg (1999). The antecedents of trust were tested by estimating the coefficients of the following equation:

$$\text{TRUST} = \alpha_0 + \beta_1 \text{SEC} + \beta_2 \text{LIAB} + \beta_3 \text{REP} + \epsilon.$$  

(1)

The effect of perceived security on trust was significant ($\beta_1 = 0.53$, $p < 0.01$) even after controlling for reputation; hence, the first hypothesis ($H_1$) received strong support by the study’s results. In contrast, the effect of financial liability on trust was non-significant ($\beta_2 = 0.07$), showing that it does not act as a surrogate of perceived security; hence $H_6$ was not supported. Reputation had a substantial effect on trust ($\beta_3 = 0.20$, $p < 0.01$), validating previous research. Even if the predictor variables were correlated, multicollinearity was not shown to cause any concerns for the model’s validity. As shown in Table II, the model coefficient was extremely significant ($F_{3,176} = 38.6$, $p < 0.001$); and the data explained a substantial degree of the variation ($R^2 = 0.37$).

The effect of the four antecedents of perceived security was also assessed by least-squares regression analysis by estimating the following equation:

$$\text{SECURITY} = \alpha_0 + \beta_1 \text{ENCR} + \beta_2 \text{PROT} + \beta_3 \text{VERI} + \beta_4 \text{AUTH} + \epsilon.$$  

(2)

Regression analysis (Table III) indicates that the effect of encryption ($\beta_1 = 0.19$, $p < 0.05$) and protection ($\beta_2 = 0.29$, $p < 0.01$) on perceived security were significant, thus validating $H_2$ and $H_3$. On the other hand, while verification had an influence on perceived security, the effect was non-

<table>
<thead>
<tr>
<th>Construct</th>
<th>Alpha</th>
<th>Mean</th>
<th>STD</th>
<th>SEC</th>
<th>TRUST</th>
<th>REP</th>
<th>ENCR</th>
<th>PROT</th>
<th>VERI</th>
<th>AUTH</th>
<th>LIAB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>0.93</td>
<td>4.44</td>
<td>1.23</td>
<td>1.0</td>
<td>0.63**</td>
<td>0.39**</td>
<td>0.24**</td>
<td>0.38**</td>
<td>0.15</td>
<td>0.18*</td>
<td>0.07</td>
</tr>
<tr>
<td>Trust</td>
<td>0.94</td>
<td>4.76</td>
<td>1.33</td>
<td>1.0</td>
<td>0.55**</td>
<td>0.12</td>
<td>0.32**</td>
<td>0.05</td>
<td>0.15</td>
<td>0.17*</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>0.91</td>
<td>5.33</td>
<td>1.51</td>
<td>1.0</td>
<td>0.33**</td>
<td>0.10</td>
<td>0.06</td>
<td>0.06</td>
<td>0.06</td>
<td>0.39**</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>0.86</td>
<td>6.05</td>
<td>1.17</td>
<td>1.0</td>
<td>0.10</td>
<td>0.43**</td>
<td>0.35**</td>
<td>0.08</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection</td>
<td>0.88</td>
<td>5.33</td>
<td>1.65</td>
<td>1.0</td>
<td>0.04</td>
<td>0.05</td>
<td>0.22**</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>0.83</td>
<td>5.37</td>
<td>1.43</td>
<td>1.0</td>
<td>0.01</td>
<td>0.31**</td>
<td></td>
<td></td>
<td>0.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>0.80</td>
<td>5.85</td>
<td>1.18</td>
<td>1.0</td>
<td>0.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liability</td>
<td>0.87</td>
<td>5.19</td>
<td>1.60</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: **Significant at $p < 0.01$ level; *Significant at $p < 0.05$ level
significant thus not supporting $H_4$. Finally, the impact of authentication was marginally significant ($F_4 = 1.63, p < 0.1$), rendering limited support for $H_5$. The regression coefficient was significant ($F_{4,175} = 7.5, p < 0.001$), and the adjusted $R^2$ was 0.14.

### Discussions and conclusion

The primary contribution of this research is the development and validation of an extensive set of interrelationships related to the construct of perceived information security and the role of financial liability in EC transactions. The constructs allow us to distinguish between objective information security assessment and the subjective consumer perceptions of security in EC transactions. While underlining the importance of consumers’ trust in EC transactions, this research clearly points to the role of perceived security in building this trust. In this work, we propose a set of antecedents to perceived security from technology mechanisms that are visible and therefore perceptible to the consumer. We showed that our hypothesized relationships among the antecedents of perceived security received considerable support, validating the proposed effect of encryption, protection and authentication. In sum, several new insights were engendered regarding the importance of perceived security and its association with consumer trust in EC transactions. Clearly, perceived security is an essential concept in understanding consumer behavior and trust in EC.

A key empirical finding of this research is the relative strength of perceived security on trust in EC transactions as opposed to retailer reputation and financial liability. While limited financial liability has been proposed as a surrogate for information security towards building consumer trust, our results show a weak effect of financial liability, rendering minimal support for our proposed hypothesis ($H_6$). This implies that absorption of financial risk by third parties is not a sufficient predictor of trust in EC transactions. An alternative explanation for this weak effect is that consumer trust in EC transactions involve risks other than monetary. For example, it is possible that privacy concerns are also present in EC transactions. While information security primarily focuses on financial information, private information would also be compromised in case of a security attack. This implies that privacy may be another underlying component that perceived security encompasses. This alternative explanation appears to be consistent with conceptualization of other researchers (Culnan and Armstrong, 1999; Miyazaki and Fernandez, 2000) who noted that privacy is dependent upon information security. Others have also shown this relationship between security and personal information (Chellappa, 2001b).

Among the antecedents of perceived security, protection, which implies consumer perceptions of how securely their information was stored, and encryption, which indicates how their information was handled during transit were unequivocally shown to be important elements of perceived security. This may be attributed to extensive media coverage of hacking incidents that involve retrieval of stored credit card information (Brunker, 2000) and hence a greater awareness for data protection. Moreover, consumers usually encounter pop-up messages whenever encryption is used, thus creating a greater familiarity with this concept. Conversely, since most certificate authorities such as Verisign are pre-bundled into browsers, consumers would rarely view authentication certificates during transactions. This may explain the moderate support for authentication as an antecedent of

---

**Table II** Regression analysis for the antecedents of perceived security

<table>
<thead>
<tr>
<th>Variables</th>
<th>Construct</th>
<th>Security</th>
<th>$t$-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent</td>
<td>Encryption</td>
<td>0.19</td>
<td>2.15**</td>
</tr>
<tr>
<td></td>
<td>Protection</td>
<td>0.29</td>
<td>2.60***</td>
</tr>
<tr>
<td></td>
<td>Accuracy</td>
<td>0.11</td>
<td>1.31</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>0.15</td>
<td>1.63*</td>
</tr>
<tr>
<td></td>
<td>$R^2$</td>
<td>0.15</td>
<td>0.14 (adjusted)</td>
</tr>
<tr>
<td>$F$ ratio</td>
<td>$F_{4,175}=7.5$ ***</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: *Standardized coefficient; * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

**Table III** Regression analysis for the antecedents of trust

<table>
<thead>
<tr>
<th>Variables</th>
<th>Construct</th>
<th>Trust</th>
<th>$t$-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent</td>
<td>Perceived security</td>
<td>0.53</td>
<td>8.44**</td>
</tr>
<tr>
<td>Control</td>
<td>Liability</td>
<td>0.07</td>
<td>1.06</td>
</tr>
<tr>
<td></td>
<td>Reputation</td>
<td>0.20</td>
<td>3.12***</td>
</tr>
<tr>
<td></td>
<td>$R^2$</td>
<td>0.40</td>
<td>0.39 (adjusted)</td>
</tr>
<tr>
<td>$F$ ratio</td>
<td>$F_{3,176}=38.6$ ***</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: *Standardized coefficient; * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
perceived security. Interestingly, we find that verification did not receive significant support as an antecedent element. An explanation is that consumers are familiar with domain names and believe that it cannot be compromised. It may also be possible that if a wrong domain were chosen, it would be easy for an experienced consumer to notice it. Hence, the level of expertise of our participants (who were sampled from university students) could have played a moderating role in this finding.

The role of expertise might have some interesting theoretical implications. Consumer behavior research has argued that novice consumers will rely on reputation and brand, whereas experienced consumers will probably rely on other factors (Ward and Lee, 1999). Further studies in risk perception have argued that due to inadequacy of scientific knowledge, lack of public trust in technology, regulators should be concerned with creating institutional arrangements and mechanisms with credible reassurance in order to foster trust (Pollak, 1996). Therefore, consumer expertise might play a role in altering perceptions of security, possibly bridging the gap between objective assessment and subjective perception. There are also public policy implications such as those suggested in risk management (Chellappa, 2001c; Powell et al., 1997; Powell, 1998) that have called for including non-scientific factors in policy decisions. Our study subtly supports this claim raising potential implications for Internet security policies.

This study also provides significant implications for practice. From the antecedents of perceived security online merchants can clearly assess the effectiveness of their security mechanisms as these are obviously costly technological investments (Lemos, 2001). In addition, retailers may also gain by making specific consumer adaptations to enhance security perceptions. Alliances with third-party institutions such as Verisign and their effectiveness may need to be explored further by online merchants. Once again it would be interesting to explore the role of expertise in assessing the effectiveness of security-building mechanisms. The examination of limited financial liability can be used to evaluate the role of credit card firms in EC. Perhaps, the role of financial liability may be more significant in financial transactions in the business-to-business area due to lessened influence of privacy concerns. Finally, this study provides the required basic framework to explore new service models such as the Amex Blue, PayPal and other financial assurance vendors.

References


Shimp, T.A. (1990), *Promotion Management and Marketing Communications*, Dryden Press, Hinsdale, IL.


### Appendix

**Table A1** Factor analysis solution with varimax rotation for principal constructs

<table>
<thead>
<tr>
<th>Item</th>
<th>SEC</th>
<th>TRUST</th>
<th>REP</th>
<th>ENCR</th>
<th>PROT</th>
<th>VERI</th>
<th>AUTH</th>
<th>LIAB</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC1</td>
<td>0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC2</td>
<td>0.83</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC3</td>
<td>0.88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC4</td>
<td>0.79</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC5</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST1</td>
<td></td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST2</td>
<td></td>
<td>0.88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST3</td>
<td></td>
<td>0.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST4</td>
<td></td>
<td>0.82</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REP1</td>
<td></td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REP2</td>
<td></td>
<td>0.91</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REP3</td>
<td></td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENCR1</td>
<td></td>
<td>0.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENCR2</td>
<td></td>
<td>0.91</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENCR3</td>
<td></td>
<td>0.77</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROT1</td>
<td></td>
<td></td>
<td>0.94</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROT2</td>
<td></td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VERI1</td>
<td></td>
<td></td>
<td></td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VERI2</td>
<td></td>
<td></td>
<td></td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUTH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUTH2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.87</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIAB1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIAB2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.91</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** Variance explained: 84%, Security 30%, TRUST 14%, REP 11%, ENCR 8%, PROT 7%, VERI 5%, AUTH 5%, and LIAB 4%. Only loadings above 0.4 are shown