Australasian (ACIS)

ACIS 2002 Proceedings

Association for Information Systems *Year* 2002

Meeting Consumer Trust Concerns at the Checkouts of Australian Online Retailers

Mustafa Ally* Mark Toleman†

*University of Southern Queensland

†University of Southern Queensland

Meeting Consumer Trust Concerns at the Checkouts of Australian Online Retailers

Mustafa A. Ally

Mark Toleman

Department of Information Systems
Faculty of Business
University of Southern Queensland
Toowoomba, Australia
Mustafa.Ally@usq.edu.au

Abstract

Lack of security and consumer trust has been repeatedly reported as one of the most important factors hindering the development of e-Commerce. This paper is a preliminary analysis of the types of trust building mechanisms available to merchants and the extent to which a selection of Australian online retailers have incorporated them in their websites. The assessment of security in the trustworthiness evaluation process typically takes place just before placing an order. The focus here, therefore, is specifically on those measures most likely to enhance confidence in the payment processing phase. We study some of the tools, over and above technical security infrastructure solutions, that could help mitigate consumer concerns over trust and security issues arising out of this stage of the business process chain.

Keywords

Electronic Commerce, Trust, Security, Payment Systems

INTRODUCTION

For users to adopt Business-to-Consumer (B2C) e-Commerce, it is imperative that the benefits of using this medium (convenience, decreased transaction costs, etc.) significantly outweigh potential and perceived risks. However, lack of trust of online payment systems has been found to constitute a real psychological barrier to e-Commerce (Egger 2000b). In the physical marketplace, the transacting partners in a face-to-face environment rely on a number of mechanisms to build security and trust. From the perspective of the consumer the physical presence of the commercial location, the appearance of goods and personnel, the possibility of touching and feeling the goods, the ability to identify entities towards which eventual complaints can be addressed, etc., inspire trust and serve the need to authenticate the merchant.

In the virtual marketplace, merchant authentication is a building block for this trust building process. In order to maintain an acceptable level of security and trust when trading on open networks, it is necessary not only to replace traditional “face-to-face” mechanisms by new digital ones but also to create new tools (digital, legal, procedural) to manage the specific risks of the open network environment where e-Commerce is conducted. It is a widely held view that public key cryptography, public key infrastructure, digital signatures and secure Internet Payment Systems will lead to a secure and trustworthy environment for e-Commerce (Centeno 2001).

These tools are in the process of being developed and refined, and will go a long way to overcoming the requirements concerned with data confidentiality and integrity, mutual consumer and merchant authentication and non-repudiation. However, while these are generally agreed to be key components of a security solution, they are not sufficient on their own, in building security, trust and confidence over the Internet between two transacting parties who do not know each other (merchant and consumer). Since the average consumer is unlikely to be able to assess the objective security of, say, an encryption algorithm, the central issue becomes one of trust built around the availability and credibility of information sources.

This paper is a preliminary analysis of a selection of those trust building measures (over and above technical security infrastructure solutions) that are likely to enhance confidence in the payment phase of a purchase and the degree to which Australian e-Commerce retailers have applied them in their business strategies.

The next section reviews literature on the theoretical concepts, classifications and nature of trust and its relation to the risks inherent in paying over the Internet from a consumer perspective. The third section operationalises these concepts and discusses a range of potential trust and security building measures. We then report on the data collection and analyse the results obtained therein. Conclusions and directions for further empirical study are also presented.

CONSUMER TRUST IN A WEB MERCHANT

Regardless of the type of payment system the seller and buyer rely on two fundamental principles to initiate and maintain purchasing over the Internet – trust and security. The parties of a transaction have to trust each other. The buyer must believe that the seller is legitimate and will actually deliver the goods. The buyer must believe that the goods are as represented and actually worth the price. The seller must believe that the buyer is legitimate and will provide valuable payment in exchange for the goods (GPayments 2001). Trust in an Internet store has been defined as a consumer's willingness to rely on the seller and to take action in circumstances where such action makes the consumer vulnerable to the seller (Jarvenpaa & Tractinsky 1999). This reliance is based on beliefs that the consumer has formed on the basis of the information the consumer has about the merchant. The Theory of Reasoned Action (Fishbein & Ajzen 1975) and the Theory of Planned Behaviour (Ajzen 1991) contend that beliefs affect a person's attitudes and that attitudes in turn influence behavioural intention, which is a good predictor of actual behaviour. A consumer's willingness to buy from an Internet seller (i.e. behavioural intention) is contingent on the consumer's attitude towards the store (i.e. the consumer's favourable or unfavourable evaluations of the merchant and the site), which, in turn, is affected by the seller's ability to evoke the consumer's trust (i.e. belief). Consumers are less likely to patronise stores that fail to create a sense of trustworthiness. Higher trust, on the other hand, will not only directly improve attitudes towards a store, but might also have an influence indirectly by way of reducing the perceived level of risk associated with buying from that particular store (Jarvenpaa & Tractinsky 1999).

As regards security, the parties need a secure environment in which to conduct the transaction. In an online payment transaction, the buyer and seller want to protect the details of the order and payment. Buyers want to be certain that their account information is not stolen and used inappropriately. Sellers need to ensure that their sites, and the data they hold, are protected from external and internal attack and abuse.

Buying on the Internet involves a number of risks for consumers: information asymmetries, lack of personal interaction, limited ability to inspect the desired product and the fear the company they are doing business with today may not be there tomorrow. The perceived and real risks of purchasing from an Internet company are initially relatively high and the level of trust is often not high enough to accept this risk. Thus, the aim must be to reduce the risk of a negative outcome in order to engender trust in the process.

Categorisation of trust factors

Trust enhancing tools can be incorporated throughout the whole shopping experience – from the product presentation step to the negotiation, ordering, payment initiation, order fulfilment, payment fulfilment and after sales phases. A model for e-Commerce trust developed by (Egger 2000a) categorises and analyses factors, likely to influence the development and maintenance of trust, into the following components:

- Interface properties (e.g. usability, aesthetic appeal).
- Relationship management (e.g. customer service, clear terms and conditions, contractual framework).
- Pre-interactional filters (e.g. reputation).

- Informational content (e.g. product and service information, transparency through security and privacy policies, financial risk and guarantees).

Another categorisation chronicles the trust building factors into pre-interaction, user interface, site information and purchase interaction factors (Centeno 2002). Several mechanisms related to payment and security are identified from the latter two categories and are used in developing our checklist in the following section. (Einweller, Geissler, & Will 2001) describe a framework based on trust-signals classified under the categories of experience, familiarity, affiliation and belonging, transparency, and factual signals and heuristic cues. While trust-signals cover different factors relevant for the development of trust they are not independent from each other. The elicitation of trust through transparency and factual signals has particular import to this study. They are company inherent factors that take place on the company's side. Transparent, accessible and open communication concerning company details can lead to a reduction in real or perceived information asymmetry. Furthermore, transparency of the transaction process can be achieved by keeping the consumer updated on its status. Facts signalling objective security measures such as certificates, guarantees or security statements are effective trust-signals to enhance the feeling of security and to generate trust.

The risks in transacting online

Risk is defined as a consumer's perceptions of the uncertainty and adverse consequences of engaging in an activity (Dowling & Staelin 1994). Consumers face a number of risks, when transacting through unsecured open networks. Consumers face the risk of transacting with a fake or fraudulent merchant who may bill the transaction and never deliver the goods purchased; or may receive recurrent or unauthorised debits for a service subscription they never agreed to; or may face the risk of having card or account data stolen and re-used for another purpose.

Consumer confidence in Internet transactions fell in the first quarter of 2002 over increased concern of the security of credit card information and the level of trust of regarding use of personal information (Yahoo!/ACNielsen 2002). Payment scheme statistics (Europay International, May 2001, quoted in (Centeno 2001) show that Internet fraud with credit cards mainly takes place either at the transactional sites that collect payment data and then disappear after fraudulently charging the cardholder (e.g. adult sites), or through unauthorised access to payment data stored at merchant servers that were insufficiently protected.

All of this has exacerbated the fear of purchasing over the Internet. When risk is present, trust is needed to make transactions possible. That is, consumer trust toward a merchant reduces the perceived riskiness of a specific webstore (Jarvenpaa & Tractinsky 1999). To allay some of this fear it is necessary for merchants to implement a variety of mechanisms to overcome any perceived apprehension that customers may harbour while purchasing online.

The Australian experience

Australia is well positioned for online retailing success. The country has high levels of Internet penetration, a strong Internet infrastructure, a progressive policy environment for e-Commerce, and a population that is ready and willing to adopt new technologies. However, although Australians are rapidly adopting the Internet, they are not adopting online retailing as aggressively as their U.S. counterparts (ACNielsen 2000). The lower incidence of online purchasing is in part the result of higher sensitivity among Australians about privacy and security. A survey conducted by Jupiter Communications revealed that as many as 58% of Australian consumers believed that using a credit card online was unsafe. This ranked among the highest of any national consumer group and was the primary inhibitor to more exponential growth in Internet commerce in the country (Jupiter Research Centre 2000).

It is therefore essential that online retailers in Australia address this problem. Only companies that manage to engender trust in their business by fully satisfying consumer needs have a chance of flourishing (Einweller, Geissler, & Will 2001). Lessons can be learned from leading retail sites that have adopted strategies to alleviate these concerns (Boston Consulting Group 2000). The following section identifies some of the main elements of trust building as they relate to payment and transaction processing.

MEASURES FOR BUILDING CONSUMER TRUST

The utility derived from the purchase of goods in B2C e-Commerce depends on the quality attribute of the product (e.g. book, CD) and of various complementary goods (e.g. consumer and privacy protection, transparency of information, delivery service, payment procedure). While quality attributes of a particular book and CD can be assumed to be homogenous across B2C e-Commerce companies, there is considerable heterogeneity with respect to the quality attributes of the complementary goods. A positive shopping experience with regard to the price/ quality ratio of the product will reduce the likelihood of a shopper purchasing at another store (Latzer & Schmitz).

In user tests of e-Commerce websites it has been found that the assessment of the site's security happens very late in the trustworthiness evaluation process, and in particular at the order placement stage of the chain. It is usually when a transaction is ready to be initiated that the consumer begins to explore the terms and conditions, and the privacy and security policies of the company. This risk assessment phase goes much further than merely assessing the security of online payments – it covers the handling of confidential data by the company, warrantees and after-sales service, as well as the customer's liability in cases of fraud (Egger 2001).

A recent study by Consumers International (www.consumersinternational.org) and discussed in (Klasen 2001) revealed that 28% of merchants surveyed failed to mention privacy policies, 20% did not describe their payment security practices, 50% of traders failed to give information on rights of withdrawal, 12% had no returns procedure and 13% left the customer without any information about the total price.

Merchants wanting to trade fairly need to adopt business strategies that raise consumer confidence and avoid conflicts or solve these conflicts in a mutually satisfying manner. In this regard, they have access to several guidelines developed by government and consumer bodies. The *Guidelines for Consumer Protection in the Context of Electronic Commerce* by the OECD countries (www.oecd.org/dsti/sti/it/consumer), the *Global Business Dialogue on E-Commerce*, the *Transatlantic Consumer Dialogue* of the European Union and U.S. consumer organisations (www.gbd.org/nn/index.html), the *Model Code of Conduct for Electronic Commerce* arising out of the Dutch *Electronic Commerce Platform*, and the German industry initiative *D21* (www.initiatived21.de) provide quality criteria for online B2C transactions involving consumers. In Australia a group of experts chaired by the government has developed a *Best Practice Model for Business* that is supported by the Australian Consumers' Association (www.choice.com.au).

While not legally binding, these guidelines suggest a number of self-regulatory trust building measures (over and above technical solutions) that can be incorporated within a merchant's website to help allay consumer concerns over trust and security.

Table 1 identifies a selected list of such measures, in particular, those related to the security and payment component of the business. While many of the mechanisms are self-explanatory some of them require further clarification.

- Provision of alternative payment methods with different risk levels for consumers (COD, credit card, etc.).
- Detailed step-by-step payment procedures.
- Clearly stated information on payment types, return and refund policies, handling of suspect order, and the consumer's right of withdrawal.
- Provision for limitation consumer liability in the case of fraud.
- Consumers right and ability to withdraw from a transaction.
- Presentation of terms and conditions.
- Limitation of consumer liability and provision of guarantees.
- Availability of redress mechanisms and provision of alternate dispute resolution schemes.
- Use of trusted third parties (e.g. security seals of approvals, credit card logos).

- Privacy Policy Statements including the way confidential information is handled.
- Adoption of anti-fraud mechanisms and strategies.
- Security Policy Statements on transactional data.
- Employment of high standard technological means to ensure authenticity and confidentiality of financial transactions and payments.
- Communication of information on security and authentication systems employed.
- Provision of online access to an in-house complaint system that is fair, effective, transparent and confidential.

Table 1: Checklist of Consumer Trust Building Methods

Payment options

The payment options offered should cater for the diverse requirements of consumers. This should include both online and offline methods. However, there is increasing expectation on the part of consumers that they will be able to pay directly over the Internet and it is therefore essential that such an option be provided and that the payment process be seamless, secure and reliable. Any barriers placed in the way of their usage will prove a disincentive to electronic commerce.

Security policies

To engineer a certain level of trust in terms of perceived security a clear and prominent policy of security should be provided. A Cheskin Research study on identifying the specific elements that communicate trustworthiness in e-Commerce sites recommends that merchants clearly spell out the security technology and practices their business was employing (Cheskin Research 2000). The security techniques employed should be clearly visible and explained to the end-user with a minimum of technical jargon and in relatively simple terms. Textual information describing security solutions implemented and logos of reputed institutions or solution providers could be used. Security measures employed in the management and storage of the data should be explained and a support system on security related issues should be established. Changes and upgrades to the security features of the site should be provided regularly.

Data protection and data privacy policies

On December 21, 2001, the Australian Federal Government introduced amendments to the Privacy Act 1988 to cover private sector organisations. Prior to this, privacy legislation was only applicable to government organisations, but now all organisations, private and public sector, with an annual turnover of more than $3 million need policies and procedures in place to protect the privacy of all individuals with whom they do business (Baltimore Technologies 2002). This protection includes securing personal data from deliberate or accidental access misuse or modification, ensuring the accuracy of the information and providing opportunity for correction. The use of technical solutions like firewalls, and authorisation and authentication security technologies can reduce the risk of privacy breaches. Any use of such security strategies should be clearly and unambiguously articulated on the website together with explicit explanations of the merchant's use of customer's information and an assurance that personal information will not be used for marketing or other purposes without the permission of the customer.

Anti-fraud technology

A major concern of merchants using credit card payment methods is the reported relatively high incidence of online fraud. Due to the impact of fraud on consumer trust and to the complexity of legal prosecution, fraud prevention is seen as the first line of defence (Centeno 2002). Merchants can play an important role in fraud prevention by screening fraudulent transactions. The lack of consumer authentication by issuing banks combined with merchants' liability for fraudulent credit card transactions has motivated the development of

merchant-based authentication solutions, with a view to reducing the level of online fraud. These solutions sometimes combine both “hard” technology based techniques with “soft” measures and include:

- Address validation.
- Online authorisation.
- Customer follow-up (email conformation, etc.).
- Customer history database consultation.
- Fraud scoring systems.
- Customer data format and content editing, rejecting orders with incomplete information.
- Proof of delivery to the verified billing address.
- Domain site check.
- Application of additional measures for high risk purchases (call customer, ask for issuer bank and phone number, exact name on credit card).
- Website statement that anti-fraud measures have been put in place.

Trusted third parties

Experienced trustworthiness can be increased with the involvement of trusted third parties (Egger 2000b). Consumer organisations regard trustmarks as a suitable instrument for providing assurance for consumers (Klasen 2001). Seals of approval from third party companies like VeriSign or TRUSTe provide consumer reassurance that high security standards have been established. Some seal programs read the privacy statement from the business and allow the site to post its seal to communicate to consumers that the website they are visiting posts a comprehensive policy. Policies are read and compared to a standard. The use of icons that symbolise the security of the network as a whole such as VeriSign and TRUSTe, and those that symbolise the reputation of the payment method such as MasterCard, Visa and Amex has been suggested as one way of increasing trust in the payment process.

Limitations of consumer liability

Consumers should be provided with information about their legal rights and liability for any losses should a fraudulent transaction occur. Limiting consumer liability in this regard can play an important part in building consumer confidence. This limitation, of course, depends on the payment instrument used and the legal contracts between the consumer and the payment instrument provider. Clearly pronounced return policies as well as guaranteed security of payment are crucial factors for reducing the perceived risk (Einweller, Geissler, & Will 2001).

Terms and conditions

Terms and conditions contain essential information such as cancellation and cooling-off rights, payment and delivery terms, and dispute resolution, so it is essential that they be presented to the consumer before purchase is completed (Consumers International 1999). Presented as a legally binding contract, the terms and conditions can provide the consumers with information on their rights and obligations and a means of assessing the extent of risks they might face in continuing with the transaction.

Redress mechanisms

In the event of unauthorised charges through fraud, billing errors or undelivered or defective purchases, effective redress measures should be in place to resolve the problem. The merchant should also explore and support alternate dispute resolution mechanisms. The redress steps and options should be clearly elucidated to promote further trust in the payment system. Consumers also need clear information about how to contact the retailer other than through the Internet in the case of queries or disputes (Consumers International 1999).

Despite the obvious importance of these mechanisms many sites lacked transparency on these matters. A 1999 study by IMSN, which examined 700 e-Commerce sites globally, found that online shopping sites were particularly lacking in information on privacy, security and customer rights. In addition, more than 50% had no security information on payment methods (IMSN 1999). Three years down the track our study attempts to examine the extent to which Australian merchants have addressed these trust building mechanisms.

RESEARCH DESIGN AND DATA COLLECTION

This research sought to gain insight into the extent to which trust mechanisms have been incorporated into e-Commerce websites. Existing literature and consumer research was used to determine the key factors for consumers wanting to make a purchase online. As described in the previous section those trust-signals directly related to facilitating the transaction processing leg of the purchasing decision were investigated.

In an attempt to provide an experience-based snapshot of what is essentially a very fast-changing situation, a sample of seventy-nine Australian companies, dealing in the sale of books, was chosen for this study. An analysis of the online bookselling industry is particularly instructive, because books have been one of the first commodities to be traded over the Internet, and consequently book sites have had the longest period to mature and develop over the years. In addition, sites like Amazon.com have often served over the years as the benchmark in e-Commerce trading and the innovative development and design of their sites sets out the potential for conducting business on the Internet.

The sites were chosen from search engines and e-Business “yellow pages” and catalogues. Those that were offline, under re-construction or had technical problems were not included in the analysis. The research process involved visiting each of the selected sites as a potential buyer and identifying and noting the trust signals of this study in the course of making a purchase. A descriptive analysis of the results follows.

RESULTS

A descriptive analysis of the results of this study, grouped under the broad categorisation of trust and security-building mechanisms, follows:

Provision of alternate payment methods

- A little over 50% had provision for secure forms for online submission of credit card details. Three merchants provided insecure forms that requested the submission of credit card details.
- 49% made provision for alternate non-Internet payment methods. These included cheque, COD, direct bank deposit, money order and payment over phone and fax.
- 18% provided for online submission of payment details as well as non-Internet methods.
- One seller offered BPay (an online bill payment and presentment method) and three supported PayPal.
- 7% allowed for payment via pre-established accounts.
- 17% offered order forms for offline printing, completion and submission via fax and post.
- 13% provided for orders via email requesting users to submit order details (including credit card numbers) via their email client.

During the ordering process

- As little as 20% of the sites provided detailed step-by-step ordering and payment procedures.
- 60% provided a shopping cart facility, most of these offering the user the option to review the order or cancel it altogether.

- 19% provided customers with the “one-click”, express checkout option requiring initial registration of details and access via a username and password.
- 14% of the sites supplied customers with the terms and conditions of transacting with the business.
- 10% provided online instant card processing capabilities through payment system providers and/ or payment gateways.
- 24% provided information on their refunds and returns policies.
- Only one site provided a formal guarantee to customers in the event of fraudulent use of credit card details arising out of dealing with the business.
- Fourteen of the sites required compulsory registration before any order would be processed.
- Two sites had online order tracking systems.

Trustmarks and seals of approval

- 30% displayed logos of certification authorities of which Thawte appeared to predominate
- 23% displayed logos of the credit card organisations
- Those sites that offered online authorisation of payments displayed the logos or provided links to their payment system providers

Privacy Policy Statements

- 35% of the sites made reference to privacy issues and the statements varied in content from a few lines to fairly comprehensive ones
- One of the guidelines provided by the Office of the Federal Privacy Commission of Australia recommends that websites should incorporate a prominently display Privacy Statement. In many cases these statements were found to be in a variety of links such as Help, Contact Info, FAQ, Shopping Services etc.
- Of the sites that had any reference to the issue of privacy only 18% alluded to the compliance with the Commonwealth Privacy Act of 1988 and only one to the amended 2001 Act
- 37% made explicit reference to specific mechanisms for customers to view and amend details held about them

Anti-fraud mechanisms

- Three sites indicated their recording of IP addresses for handling suspected fraudulent use of credit cards
- 40% of the sites that provided a secure order form did not carry out even rudimentary credit card number checks such as tests for reasonableness, length, range or valid expiry dates
- Two sites made use of the three digit security code found on the two major credit cards for validation

Security Policies

- 13% provided detailed explanations about how personal data and credit card numbers were being secured at the site
- 25% of the sites detailed the security measures they were using to protect the transactions and personal information

Other observations

- As regards Australian law we found only one site which made specific reference to compliance with the guidelines of the Trade Practices Act 1974, the Fair Trading Act and Sales Good Act, the Consumer Credit Code and the Electronic Transactions Act of 1999

- Also, none had any explicit statements about complaints procedures and alternate dispute resolution arrangements

DISCUSSION OF RESULTS

The results suggest that much can be done by these merchants to exploit some of the trust-building mechanisms described in this research and, in doing so, improve the overall trust and confidence in their sites. Their limited use can be attributed to one or more of several possible reasons: possible lack of awareness, on the part of these organisations, of the role that these trust mechanism can play in encouraging sales; an understanding of available trust building mechanisms and the skill to implement them; and a lack of awareness of the factors that influence trust.

As the marketplace grows in terms of the number of participants, the size of transactions and other elements, more trust enhancers are need to maintain user confidence and willingness to participate. It is evident from these results that the websites in the study have not succeeded in keeping pace with the available technologies and the demands of an increasingly sophisticated purchaser. For example, many sites in the study have not fully exploited readily available security and payment technologies which have succeeded in alleviating many consumer concerns. The absence of third-party trust mechanisms and comprehensive privacy policies, too, was evident in many of the sites studied.

Ultimately, the most effective way for e-Commerce to grow is by developing profitable sites that engender trust. On-line shoppers need to be re-assured that it is safe to conduct on-line transactions and that security, privacy and integrity issues have been adequately addressed. To this end, merchants must embed appropriate technology within their systems to protect their customers. Payment protocols, encryption and digital signature technologies need to be adopted more widely. Organisations need to demonstrate that they adhere to the strictest standards of privacy, security and encryption and incorporate seals of approval to offer assurance that these controls are in place.

LIMITATIONS

The research was designed to provide a snapshot picture of the state of a selection of Australian businesses at the time of the study. It was not designed to give a statistically representative result for the B2C e-Commerce industry. Also, no attempt was made to determine the completeness, validity or efficacy of the mechanisms investigated in this study.

CONCLUSION

The nature of the Internet and the rapid growth in e-Commerce transactions makes it an imperative for Internet companies to concentrate a greater effort on engendering consumer trust. This study was centred on some of the suggested methods that have the potential to stimulate trust in the transaction processing and payment leg of the purchasing chain. The results show that retailers have much work still to do before they can offer consumers a reliable environment in which they can shop with confidence. There are several indicators that Australian online booksellers have the potential to further increase trust and security in their sites through the adoption of a wide range of confidence building mechanisms.

Because the adherence to many aspects of best practice guidelines is voluntary, consumers need a way of recognising Internet stores that offer high standards of consumer protection with ease. The development of an internationally recognised certification or labelling scheme, which indicates that stores meet agreed minimum standards on a range of key issues, would go a long way to offering this reassurance.

FURTHER RESEARCH

A further longitudinal study will be conducted to evaluate the level of maturation of the companies studied over a period of time. There is also a need to further explore the nature of trust and to construct new trust models in the light of the manifest demands of online transacting. Empirical results can be used to validate these models as well as determine the efficacy of the trust mechanisms identified in this study. The relative importance of these

trust elements and the manner in which they interact with each other should then be determined.

REFERENCES

ACNielsen (2000) *Australian online shoppers browse US, e-tail local* [Online], Available: http://eratings.com/news/2000/20000614.htm, [Accessed 19 April 2002].

Ajzen, I. (1991) 'The theory of planned behaviour', *Organisational Behaviour and Human Decision Processes*, vol. 50, pp. 179-211.

Baltimore Technologies (2002) *Security Holds the Key to Privacy* [Online], Available: www.baltimore.com, [Accessed 4 March 2002].

Boston Consulting Group (2000) The Canadian Online Retailing Report, Retail Council of Canada.

Centeno, C. (2001) Securing Internet Payments, Background Paper No. 6 (Electronic Payment Systems Observatory) edn., Institute for Prospective Technological Studies.

Centeno, C. (2002) Building Security and Consumer Trust in Internet Payments, Background Paper No. 7 (Electronic Payment Systems Observatory) edn., Institute for Prospective Technological Studies.

Cheskin Research (2000) Trust in the Wired Americas.

Consumers International (1999) 'Consumers@shopping: An international comparative study of electronic commerce', [Online], Available:www.consumersinternational.org, [Accessed 18 April 2002]

Dowling, G.R. & Staelin, R. (1994) 'A model of perceived risk and intended risk-handling activity', *Journal of Consumer Research*, vol. 21, pp. 119-34.

Egger, F. N. (2000a) *Towards a Model of Trust for E-Commerce System Design* [Online], Available: http://www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html, [Accessed 15 April 2002a].

Egger, F. N. (2000b) '"Trust Me, I'm an Online Vendor": Towards a Model of Trust for E-Commerce System Design', In: G. Szwillus & T. Turner (Eds.), CHI2000 Extended Abstracts: *Conference on Human Factors in Computing Systems,* The Hague (The Netherlands) , April 1-6, 2000: 101-102.

Egger, F. N. (2001) Security & Trust: Taking Care of the Human Factor, ePSO-Newsletter No. 9.

Einwiller, S., Geissler, U. & Will, M. (2001) Engendering Trust in Internet Business using Elements of Corporate Branding, Institute for Media and Communications Management, University of St. Gallen, Switzerland.

Fishbein, M. & Ajzen, I. (1975) *Belief, attitude, intention and behaviour: An introduction to theory and research ,* Addison-Wesley, Reading, MA.

GPayments (2001) *Authentication: the missing element in online payment security* [Online], Available: www.gpayments.com, [Accessed 4 December 2002].

IMSN (1999) *Study on Privacy, Security and Customer Rights* [Online], Available: www.imsnricc.org/imsn/activities.htm, [Accessed 27 November 1999].

Jarvenpaa, S.L. & Tractinsky, N. (1999) 'Consumer Trust in an Internet Store: A Cross-Cultural Validation ', *Journal of Computer-Mediated Communication*, vol. 5, 2.

Jupiter Research Centre (2000) *Online Commerce Down Under: Despite Growth, Credit Card Security Remains a Major Issue* [Online], Available: www.jup.com/sps/research, [Accessed 26 April 2002].

Klasen, D. (2001) Creating Consumer Confidence: Current Efforts towards International Quality Criteria for E-Commerce, ePSO-Newsletter No. 9.

Latzer, M. & Schmitz, S.W. (2001) 'B2C eCommerce: A Frictionless Market is Not in Sight. Arguments and Policy Implications', in Innovations for an e-Society. Challenges for Technology Assessment.

Yahoo!/ACNielsen (2002) *The Yahoo!/ACNielsen Internet Confidence Index* [Online], Available: http://docs.yahoo.com/docs/info/yici/, [Accessed 19 April 2002].

COPYRIGHT