Trust in e-Commerce: Evaluating the Impact of Third-Party Seals

Milena M. Head*
headm@mcmaster.ca
905-525-9140 ext. 24435

Khaled Hassanein
hassank@mcmaster.ca
905-525-9140 ext. 23956

DeGroote School of Business,
McMaster University,
1280 Main Street West
Hamilton, Ont., L8S 4M4
Canada

Head, M., and Hassanein, K. (2002). "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals", *Quarterly Journal of Electronic Commerce*, 3(3), 307-325.

Acknowledgement
This work was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

*** corresponding author**

Trust in e-Commerce: Evaluating the Impact of Third-Party Seals

Milena Head and Khaled Hassanein

Abstract

In an electronic commerce environment, trust is more difficult to build and even more critical for success than in traditional commerce. Trust is a long-term proposition that may be tough to build and easy to lose. This paper presents a new conceptual model for online trust, which illustrates the phases of building online consumer trust and outlines the necessary interactions between consumers, vendors and referees to progress from one trust phase to another. This model can help to further our understanding of online trust, provide online vendors with methods for building consumer trust, and direct future research in this new and critical field. Subsequently, a survey is conducted to validate our model and investigate the impacts of seals-of-approval provided by trusted third parties as a mediating factor in building and maintaining online trust. We found that the general awareness and influence of such seals was still relatively low. However respondents agreed that the influence and impact of third-party referees varies according to the phases of the trust lifecycle. Additionally, we confirmed that a breech of trust will cause most consumers to revert back to the chaos state of trust where it may be more difficult to re-establish online trust. Conclusions from this research are discussed and areas for future research are proposed.

Keywords: electronic commerce; trust; trusted third-party; seal-of-approval; lifecycle, security, privacy, reliability

1. Introduction

Everyday we place our trust in people and the services those people provide. We trust that our friends will not betray our confidences, that the water we drink will not make us ill, that the building we work in will not collapse, that the vendor we buy from will not overcharge us, and so forth. In order to be productive and comfortable in our lives, we must routinely place our trust in these familiar environments. By and large, the Internet, and electronic commerce (e-Commerce) in particular, is not a familiar environment where we blindly place our trust. When compared with traditional commerce, e-Commerce is more impersonal, more automated, provides fewer direct sensory cues, has less immediate gratification, entails more legal uncertainties, and presents more opportunities for fraud and abuse (Görsch 2001; Head et al. 2001; Roy et al. 2001; Yoon 2002). Therefore trust is more difficult to build in this online environment (Hoffman et al. 1999).

In order for e-Commerce to flourish, consumers must not be fearful that they will be cheated, defrauded, have their credit card numbers stolen, or receive poor quality goods or service. Vendors envision the Web as a viable alternative to traditional channels and a new arena for developing personalized relationships with consumers (Dreze & Zufryden, 1998). Within this context, trust becomes a critical component for fostering and improving this customer relationship (Speier et al., 1998). However, recent surveys have shown that a lack of trust is still one of the biggest concerns for Internet consumers (Cox, 1999; Levin, 2000; Westin and Maurici, 1998). Without trust, development of e-commerce cannot reach its full potential (Cheskin/Sapient 1999).

This paper is structured as follows: the concept of trust is discussed from several perspectives in Section 2. Section 3 specifically examines trust in an electronic commerce environment. A new online trust building model is presented and discussed in Section 4. From this model, focus is placed on referee trust, which is examined in more detail in Section 5. Various propositions for examination are also outlined in this section. Sections 6 and 7 present the methodology and the data analysis of a survey sampling experiment designed to validate our model and test our propositions. Finally, conclusions and areas for future research are presented in Section 8.

2. The Concept of Trust

Trust is a complex concept that has been studied by many disciplines, such as sociology, psychology, business, among others. Sociological research tends to examine trust from the perspective of social relationships (Barber 1983; Good 1988). Trust can be held by individuals, social relationships and social systems. It is a concept that is difficult to capture and study, thus, sociological research presents many varied definitions and propositions of trust. However, certain elements appear to be common across these sociological views. Many sociologists argue that without trust, modern society would not be possible (Barber 1983; Macy and Skvoretz 1998). To build trust, most researchers agree that experience is critical and information about past behaviour, goals and reputation are required (Barber 1983; Good 1988; Buskens 1998; Seligman 1998). Additionally, trust is commonly viewed as a dynamic process which must be built over time and is dependent on situational context (Lewis and Weigert 1985; Good 1988;

Buskens 1998; Macy and Skvoretz 1998). Some sociologists also believe that trust cannot exist in the absence of risk (Seligman 1998).

From a psychological perspective, trust research tends to focus on individual personality differences and development throughout life (for example, see Erickson 1963) or interpersonal relationships (for example, see Rotter 1980; Lewicki and Bunker 1995). As with the sociological view, the body of trust research in psychology is fragmented and varied (Lewicki and Bunker 1995). It is difficult to define trust since it can apply to many different types of relationships, varies across contexts, and is multi-dimensional (Deutsch 1958; Rotter 1980). Interpersonal trust has been extensively examined from a game theory perspective, where communication, experience and motivation are major trust determinants (Deutsch 1958; Kee and Knox 1970). In particular, Deutsch (1958) identified three motivational inclinations: (i) cooperative; (ii) individualistic; and (iii) competitive. As with the sociological view, psychologists have also considered trust to entail elements of risk and vulnerability (Zand 1972).

As with other disciplines, business-related literature presents several views and definitions of trust. Shapiro (1987) has gone so far as to say that definitions of trust have become a "confusing potpourri". Trust has been defined as the willingness to depend on an exchanging partner in whom one has confidence (Moorman et al. 1993), the willingness to be vulnerable to the actions of another party (Mayer et al. 1995), the expectation of ethically justifiable behavior (Hosmer 1995; Baba 1999), among others. Several studies have recognized credibility and benevolence as critical components

underlying trust (Ganesan 1994; Doney and Cannon 1997; Ambrose and Johnson 1998; Roy et al. 2001). Credibility is the belief that the vendor has the necessary expertise to complete the task effectively and reliably, whereas benevolence is the belief that the vendor has positive intensions and will act in a favorable manner even when there is no existing commitment between the two parties. Risk also reoccurs as a topic in business-related literature. Risk is defined as a consumer's perceptions of the uncertainty and adverse consequences of engaging in an activity (Dowling and Staelin 1994). Researchers agree that there must be risk and uncertainty for trust to occur (Lewicki and Bunker 1996, Mayer et al. 1995). The level of trust requested or needed has an approximate inverse relationship to the degree of risk with respect to business transactions (Konrad et al. 1999; Povey 1999).

In this paper, we adopt the definition proposed by Geyskens et al. (1996), where trust is the belief or expectation that the vendor's word or promise can be relied upon and the vendor will not take advantage of the consumer's vulnerability. Trust can be increased by a reputation for reliable, fair and consistent behaviour (Ganesan 1994). Vendor size has been shown to positively influence consumer trust (Doney and Cannon 1997) as well as the consumer's previous experience with the vendor (Anderson and Weitz 1989). Trust is also increased when the consumer believes the vendor has made investments on his or her behalf, such as customization of products (Ganesan 1994; Doney and Cannon 1997). From a vendor's perspective, the development of consumer trust is highly desirable, since it leads to the establishment of long-term exchange relationships (Ganesan 1994). Trust also affects a consumer's continuing intention of doing business

with a vendor (Doney and Cannon 1997). From a more macro level, trust is a valuable asset which is firmly linked with economic success (Fukuyama 1996).

3. Trust in e-Commerce

Trust is more difficult to build and more critical in online, versus offline, business environments (Hodges 1997; Ratnasingham 1998; Hoffman et al. 1999; Roy et al. 2001). For example, most people do not hesitate to order merchandise over the telephone or pass a credit card to an unknown salesperson. If an error occurs in these types of transactions, we trust the service provider to correct the error. However, we do not observe the same levels of trust in online environments, as we do in our everyday lives (Head et al. 2001). We are far more skeptical and cautious about passing personal information through Internet channels. Online transactions are more impersonal, anonymous and automated than offline transactions (Head et al. 2001). This de-humanization of business relations is also accompanied by an increase in the technical means and opportunity for fraud and abuse.

Trust in business-to-consumer (B2C) e-Commerce is established very differently than in business-to-business (B2B) e-Commerce environments because relationships are often shorter in term and more transaction-oriented (Roy et al. 2001). In this paper, we focus on the B2C e-Commerce environment. In this context, Head et al. (2001) distinguish between "hard" and "soft" trust, where "hard trust" includes issues of security whereas "soft trust" encompasses privacy and quality of service dimensions. "Hard trust" centers on technical solutions to provide secure interactions, so that consumers feel confident that

the information they transmit during a transaction will arrive uncorrupted and will not be improperly leaked to others (Stratford 1999). For example, encryption techniques can protect information during transmission, and firewalls and encryption can protect private customer information once it is stored (Head 2000).

Issues of "soft trust" cannot be as easily resolved through the application of technology solutions. "Soft trust" includes trust in the privacy of personal information and trust in the vendor's quality of service (Head et al. 2001). To conduct business and provide valuable services, it is often necessary for online vendors to collect information from customers. This personal information, which can be gathered explicitly or through more covert implicit actions while the customer is interacting with a vendor's Web site, may have great monetary value to a vendor. Consumers need to trust that their personal information will not be abused by the vendor or even sold to the highest direct marketing bidder. Concerns about information practices will lead to consumers guarding their personal information or falsifying information, which deprives the online vendor of valuable information that could be used to tailor their services/product to individual customers. Milne and Boza (1999) found that consumer trust levels vary by industry, depending on how much information is captured and whether it is shared. Additionally, what is regarded as private varies across organizations, cultures, and even individuals (Simmons 1993). It has been recommended that online trust can be increased through honest and full disclosure of information practices (Milne and Boza 1999).

Trusting the quality of an online vendor's service may also be a challenge for consumers. After all, the store down the block will likely be there tomorrow, but the store that exists in cyberspace is often not "real" in the customer's eyes. Online vendors may be considered "fly-by-night" as there are fewer assurances for consumers that the online merchant will stay in business for some time (Jarvenpaa et al., 1999). Doney & Cannon (1997) found that in traditional environments, consumer trust is affected by the seller's investments in physical buildings, facilities, and personnel. An online vendor may even be in another country, which has a different legal system. Customers need assurance that businesses are accurately representing themselves (authenticity) and that their transactions will be honored as agreed (non-repudiability) (Head et al 2001). Branding has been shown to be important in overcoming some e-commerce obstacles (Davis 2000; de Groote and Egger 2000). Without contact with "real", physical elements (such as salespeople, buildings, products, etc.), online consumers heavily rely on brands, which are symbols of quality that can evoke trust. Positive past experiences and feelings of control also help to build trust in quality of service (Frazier et al. 1988; Jarvenpaa et al. 1999; Sisson 2000). Other online trust engenders may include well-designed websites (Sisson 2000; Egger 2000; Nielsen et al 2001) and assurances from independent third parties (Resnick et al. 2000; Head et al. 2001).

4. A Model to Understand e-Commerce Trust

In the B2C e-Commerce environment, three main parties interact to determine consumer trust levels. These trust parties are:

- ***Consumers***: Consumers seek trust before interacting with a vendor to acquire their products or services. They have significant experience in the traditional market, but may not be as familiar with or comfortable in the online marketplace. Individual consumers will differ in their "trusting" personality traits (Erickson 1963; Bowlby 1973) and the pace at which they attain the trust required to start transacting with an online vendor.

- ***Vendors***: Vendors seek to build trust among consumer in order to sell their product or services. They may have both a physical and an online presence, or solely operate in the electronic marketplace. Vendors with a physical presence that have an established, commonly recognized brand with a built-in trust factor are proving to be more successful in the electronic marketplace compared to their pure online counterparts (Head et al. 2001). Consumers who recognize the Web storefront as an extension of an existing business may perceive it to be more legitimate, and have more trust in the store (Steinfield and Whitten, 1999).

- ***Referees***: Referees are third-parties who provide independent recommendations on the trustworthiness of vendors. Trust referees may come in many forms, from individual recommendations to privacy and security trust "seals" to media representatives/watchdogs. Referee types are discussed in more detail in the next subsection. In particular, this paper focuses on trust seals as a mediating factor in building online consumer trust.

Trust is a dynamic process that may deepen or retreat over time and with experience (Ravald and Grönroos 1996; Roy et al. 2001). Lewicki and Bunker (1995) proposed that types of trust fall into phases which are linked, sequential, interactive and evolve over time. Marcella (1999) extended this work to an online environment, where he suggested that trust in e-Commerce vendors is deepened by passing through stages of building, confirmation and maintenance. Cheskin/Sapient (1999) propose that online trust is built, confirmed and maintained over time as consumers move through an untrust phase, an extrinsic level of trust phase and an intrinsic level of trust phase. Head et al. (2001) further this research by presenting a more detailed four phase lifecycle (chaos; establish; enhance; and maintain) for developing online consumer trust.

We use the lifecycle phases proposed by Head et al (2001) as the basis for our Online Trust Building Model, presented in Figure 1. In addition to outlining the phases of consumer online trust, this model integrates the necessary interactions between consumers, vendors and referees to progress from one trust phase to another. Consumers may at first feel a sense of chaos in the e-Commerce market, as they fear that their personal information may be stolen due to unreliable security and that online businesses may be fraudulent. They are untrusting of online vendors and do not seek the recommendations of referees. With appropriate motivation, trust can be established over time, as consumers become more familiar with the new technology and the marketplace. However, before customers are willing to register or transact through a Web site, they must build trust to a certain level or threshold. Specifically, consumers start to compare and assess online vendors while seeking recommendations from referees. If trust is

established and initial vendor transactions successfully meet consumer expectations, then consumer trust is reinforced and further enhanced (Roy et al. 2001). Referees continue to play an important role in strengthening consumer trust in online vendors. As consumers continue to experience successful transactions, trust is maintained. Although consumers may no longer be swayed by positive referee recommendations, negative reviews or remarks may still influence consumer perceptions of vendor trust.

Trust also involves vulnerability. When people trust, they expose themselves to risk. If consumers experience a breech or violation of trust, they may easily revert back to the chaos state where trust may be more difficult to reestablish (Head et al. 2001). Lewicki and Bunker (1995) propose that breeches or violations of trust will have different outcomes in different phases of the trust lifecycle. Although a trust violation will likely end a relationship in earlier phases of the lifecycle, in later phases, relationships may continue if the trustor (consumer) perceived the violation circumstances to have been beyond the control of the trustees (vendor). In our Online Trust Building Model, we show that a breech of trust will most often send a consumer back to a state of chaos. This is particularly true if the consumer perceives the vendor to have knowingly executed the violation. However, if the relationship between the consumer and vendor is strong (at the maintain stage) and the violation is not perceived to be intentional, then trust violation consequences may be less severe, possibly reverting to a previous phase (such as establish or enhance).

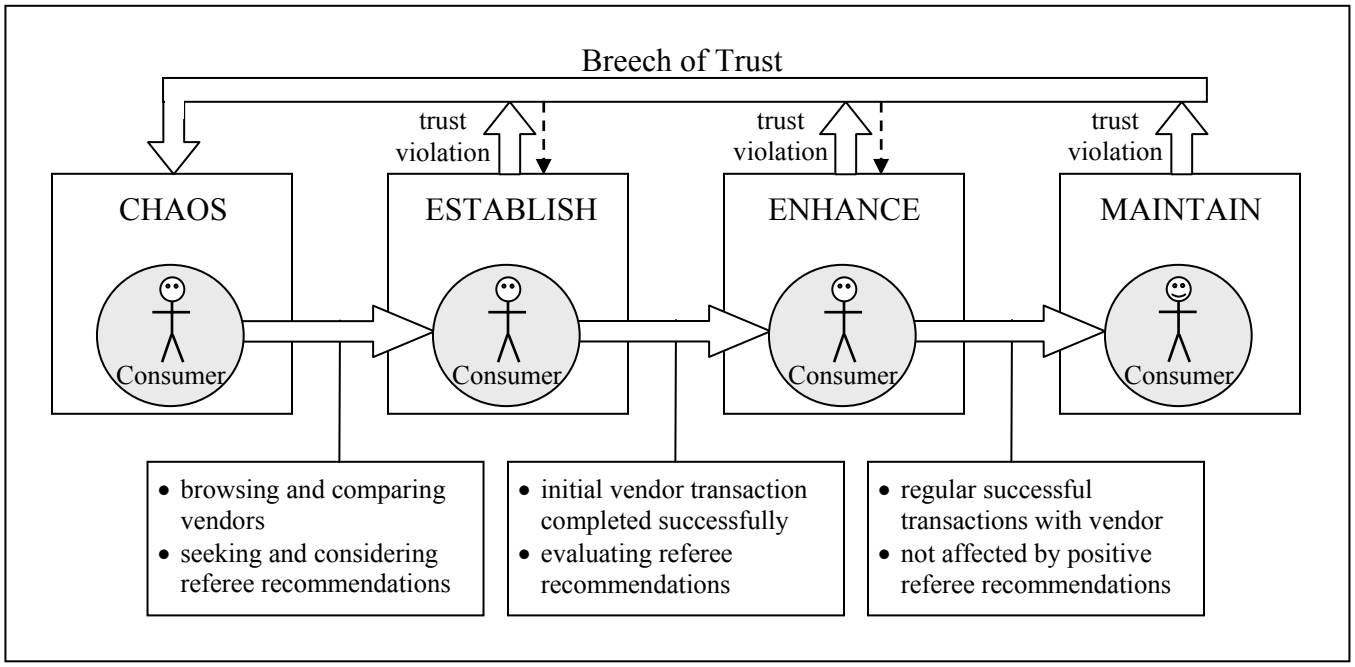

Figure 1: Online Trust Building Model

The Online Trust Building Model introduced above focuses on the consumer's position and activities at the different phases of the trust lifecycle. It is important to note, however, that the consumer trust level in an online vendor and consequently his/her position within the trust lifecycle is highly dependent on the interactions between the three trust parties identified in our model (consumer, vendor, referee). Table 1 outlines a more detailed description of the party-to-party interactions at each of the trust lifecycle stages. By examining these interactions, it is possible to gain an understanding of the roles and responsibilities of each of the parties during the different stages in the trust lifecycle.

Table 1: Party-to-Party Interactions within the Online Trust Life Cycle

	Consumer	Vendor	Referee
Consumer	N/A	**C**: does not seek vendor because of being unaware or untrusting **Es**: becomes aware of vendor through browsing and comparison **En**: registers/completes initial transaction to her/his satisfaction **M**: performs regular satisfactory transactions	**C**: does not seek or is unaware of referee; focuses on negative referee comments **Es**: seeks and considers referee recommendations **En**: continues to consider referee recommendations in light of their personal experience **M**: no longer affected by positive recommendations; may continue to be influenced by negative recommendations
Vendor	**C**: attempts to attract consumer's attention or rebuild consumer trust **Es**: tries to instill trust through first impressions **En**: strives to enhance trust by fulfilling consumer expectations **M**: maintains trust through repeated satisfactory experiences	N/A	**C**: does not seek/have positive referee recommendations; negative referee comments may be publicized **Es**: seeks positive referee recommendations **En**: receives and advertises positive referee recommendations **M**: consistently complies with referee standards
Referee	**C**: attempts to inform consumer about their value **Es**: provides recommendations to consumer **En**: continues to provide recommendations to consumer, possibly incorporating their opinions; investigates consumer complaints **M**: continues to provide recommendations to consumer, possibly incorporating their opinions; investigates consumer complaints	**C**: attempts to inform vendor about their value **Es**: evaluates vendor **En**: issues vendor recommendations **M**: continues to issue vendor recommendations based on regular audits	N/A

Note: C = Chaos Phase; Es = Establish Phase; En = Enhance Phase; M = Maintain Phase

5. Referee Trust

For consumers to trust a transaction partner, they must have a degree of knowledge about them. This knowledge can be gained through previous experiences (Doney and Cannon 1997) or by gaining information from a third party (Strub and Priest 1976). Needham

(1998) agrees that one way vendors can win the trust of potential customers is to secure recommendations and referrals from credible third parties. This is particularly important in online environments (Siyal and Barkat 2002). Since time and experience are needed to deepen trust and the Internet is still relatively new (Cheskin/Sapient 1999), online transactions require very explicit guarantees up front (Nielsen 1999). Clearly, the degree to which a consumer's opinions and purchasing behavior is influenced by a referee is directly dependent on the consumer-perceived reliability and trust of that referee. We classify four types of referees (word-of-mouth; watchdogs; certificate authorities; seals-of-approval), which are examined in more detail below.

5.1 Word-of-mouth

Word of mouth, spread through individual experiences, can have a powerful influence on the level of trust consumers have in vendors. Consumers may find it difficult, however, to judge the trustworthiness of information. Friends are generally trusted and the information / opinions they provide often form the basis for decision making. Trust in people can be transformed into online trust (Karvonen 1999). Additionally, consumers may not be motivated to spend the time and effort required to investigate the technical details of security and privacy policies. Therefore, it may be easier for consumers to find out through trusted referees whether adequate security and privacy procedures are in place, rather than having to establish this on their own (Adams and Sasse 1999).

The online environment can facilitate word-of-mouth communication through virtual communities. Bagozzi and Dholakia (2002) define virtual communities as "mediated

social spaces in the digital environment that allow groups to form and be sustained primarily through ongoing communication processes". Members of virtual communities may share recommendations, reviews, overviews, tips, advice, etc. Community members demonstrate trust in other members by virtue of their membership in the community (Fukuyama 1996). These communities can be valuable resources for promoting vendor trust and encouraging website "stickiness". By developing and promoting an "imagined community", consumers may perceive vendors as a trusted part of the virtual community rather than merely an institution (Anderson 1991). For example, Amazon.com has been very successful at building trust through the promotion of its open community of reviewers. Similarly, eBay's Feedback Forum community, where users leave comments about their experiences and their evaluations of buyers and sellers with whom they transact, has fostered a more trusting environment for online auctions (Ba and Pavlou 2002). In these cases, building trust may heavily depend on the credibility assessment of the early customers (Mahadevan and Venkatesh 2000).

5.2 Watchdogs

Watchdogs are independent organizations, centers or media representatives that identify vendors' violations or breeches of trust and publicize their actions to alert consumers (Head and Yuan 2001). For example, EPIC (Electronic Privacy Information Center) and CDT (Center of Democracy and Technology) act as privacy watchdogs that continuously monitor the privacy practices of online vendors and provide a forum for consumers to communicate their privacy concerns. The vigilance of these watchdogs can help to quickly halt and correct the improper practices of vendors. For example, on

November 1, 1999, The New York Times printed a story about RealNetworks' alleged privacy leaks. This created such a public embarrassment for the company that its privacy policy was amended the very same day (Head et al. 2001).

5.3 Certificate Authorities

Cryptography is essential to transactional security on the Internet. Most cryptographic protocols for secure electronic transactions require the presence of a trusted third party, such as a bank or certificate authority (CA). The CA verifies the link between the identities of individuals or vendors and their corresponding public keys, through the use of digital certificates. The CA does not vouch for the trustworthiness of the vendor, but simply authenticates the vendor's identity (Grandison and Sloman 2000). For example, VeriSign (http://www.verisign.com) and Entrust (http://www.entrust.com/) are leading Certification Authorities that authenticate, issue and manage digital certificates on the Internet.

A web-of-trust is an extension to certificate authorities, which blurs the distinction between CAs and users. Every participant in a web-of-trust system is able to issue notices about whom they know and trust. For example, the Thawte web-of-trust system (http://www.thawte.com/) is a peer-to-peer community-driven certification system. Individuals can be notarized, and can in turn act as notaries to certify others. This system may be compared to a "bottom-up" CA, compared to the traditional "top-down" CA (Froomkin 1996). Webs-of trust are also closely linked to virtual communities.

5.4 Seals of Approval

Trust in interactive spaces is not only determined by providing measures for security (D'Hertefelt 2000). To promote trust in electronic markets, researchers suggest providing credible signals to differentiate among vendors (Ba and Pavlou 2002). While certificate authorities simply authenticate a vendor's identity, seals of approval aim to assure consumers that a vendor's site is a reliable and credible place to do business. Vendors may convey this information by placing the sign, logo, or seal of a trusted third-party (TTP) on their website. Consumers may click on the seals of approval displayed on vendor sites to obtain detailed disclosures of the TTP. The seals and their disclosures are designed to assure consumers that the transactions of the online vendor reflect the high standards set forth by the TTP (Benassi 1999).

TTPs can serve as privacy, security or business credibility/reliability validators (Greenstein and Feinman 2000). Vendors that display a privacy seal convey a message to consumers that they openly disclose and adhere to certain standards for conducting business, and that this disclosure/adherence is assured by a credible third-party regulator. For example, the TRUSTe privacy seal (http://www.truste.com) is awarded to online vendors that adhere to established privacy principles and are willing to comply with oversight and consumer resolution procedures. Online vendors that display the TRUSTe privacy seal include AOL, eBay and AltaVista. Vendors that display a safety seal, such as VeriSign (http://www.verisign.com), assure users that they are really doing business with the intended vendor (acting as a certificate authority), and that the information sent is protected from interception and alteration over the Internet. Additionally,

credibility/reliability seals may be granted to vendors that comply with the TTP's standards along these dimensions. For example, the BBBOnline reliability seal (http://www.bbbonline.com/reliability/) may be used by vendors that are at least one year old and have joined their local Better Business Bureau (BBB). This means that vendors must abide by BBB guidelines for prompt and satisfactory responses to customer complaints; commitment to problem resolution; and adherence to publicized programs (Greenspan 2002). Online vendors that display the BBBOnline reliability seal include Lexmark and Liberty Mutual.

It is important to note that within the various privacy, security and business credibility/reliability validations, some TTPs only focus on the vendor's proper disclosure of policies and practices, while others also monitor the vendor's compliance with those policies and practices (Steer 1999). For example, WebAssured provides online vendors with the opportunity to become members in their web assurance program. By becoming a member (and displaying the WebAssured certification seal), a vendor agrees to conduct their online business in conformance with a Universal Standard of Ethics, established by WebAssured. WebAssured, however, does not actively seek to verify vendor compliance to their standards of ethics. Instead, they rely on consumers to report any deviations by vendors from this standard. Escrow.ca is an example of an online vendor that displays the WebAssured seal. In contrast, WebTrust (http://cpawebstruct.org) is a TTP that also regularly monitors for vendor compliance with stated policies and practices. WebTrust assurance services, which are backed up by the American Institute of Certified Public Accountants (AICPA) and the Canadian

Institute of Chartered Accountants (CICA), convey information about the vendor's identity and quality (Srivastava and Mock 2000). Online vendors that display the WebTrust seal include American Airlines, Bell Canada and VeriSign. Increasingly more TTPs are providing compliance assurances in addition to disclosure guarantees.

Third party authentication seals are another way for e-Commerce sites to demonstrate their trustworthiness. The Cheskin/Sapient e-Commerce Trust Study (1999) found that web-based seals of approval, when recognized, do communicate trustworthiness. They seek to re-assure the consumer that control has been established. In contrast, the presence of credit card symbols does not add to the trustworthiness of websites, even though they are more universally recognized. The Cheskin/Sapient study (1999) claimed that seals of approval are one of six primary components that communicate e-Commerce trust. However, during the time of the Cheskin/Sapient study, the awareness of such seals was relatively low. VeriSign was recognized by 36% of respondents, TRUSTe by 23% and BBBOnline by only 18% (Cheskin/Sapient 1999). More current evidence suggests that consumer's awareness of online seal programs may have increased during the last few years. For example, a more recent study from Princeton Survey Research Associates (2002) reports that 60% of respondents thought that a website's display of seals of approval from third parties was at least somewhat important. Therefore, we propose the following:

P1: Online consumers are aware of seals-of-approval programs.

Some research has suggested that seals-of-approval may impact a consumer's decision to purchase from an online vendor. For example, Kover et al. (2000) conducted a study on the WebTrust seal, where they found that consumers who paid more attention to the seals and disclosures of web sites had a stronger intent to purchase online than their counterparts. Cashell (1999) proposed that online vendors that display a seal-of-approval on their websites may boost consumer confidence and increase sales. Interestingly, a study by Nöteberg (1999) found there were no significant differences between the effects that different seal types had on the likelihood of purchase. As long as it was a TTP that was providing the assurance, they were significantly more likely to make a purchase than a vendor that did not display a seal. Therefore, we propose the following:

P2: Seals-of-approval positively influence consumers' online purchasing decisions.

Our Online Trust Building Model presented above proposes that trust is developed over time and can be characterized as passing through phases of a lifecycle. This concept is supported by various other researchers (for example, Lewicki and Bunker 1995; Marcella 1999; Cheskin/Sapient 1999). Our model also suggests that the influence of referee recommendations varies according to the consumer's location in the trust lifecycle. Findings from the Princeton Survey Research Associates (2002) also suggests that the importance of seals-of-approval declines somewhat with experience. Therefore, we propose the following:

P3: The influence of seals-of-approval will vary according to the phases of the trust lifecycle.

The above proposition (P3) seeks to validate the referee influence component within our Online Trust Building Model. Another component of our model that requires further validation is the effect of a breech of trust. There is evidence to suggest that a breech of trust may cause consumers to revert back to an earlier phase (often the chaos phase) within the trust lifecycle (Lewicki and Bunker 1995; Cheskin/Sapient 1999). However, more recent evidence of this phenomenon is lacking. Therefore, we propose:

P4: A breech of trust will cause consumers to revert back to the chaos phase within the trust lifecycle.

6. Methodology

To test the four propositions outlined above and validate our proposed Online Trust Building Model, we conducted a questionnaire with 223 subjects. The questionnaire consisted of three main parts: (i) basic demographic information; (ii) online familiarity and attitudes; (iii) TTP familiarity and attitudes. The purpose of this questionnaire was not to provide a comprehensive examination of our outlined propositions, but to serve as an initial validation of our model and to help direct and warrant future research in this area.

6.1 Subjects

From the 223 subjects that participated in this study, 58% were female and 42% were male. The majority of respondents fell between the ages of 18 and 24 (70%) and were either completing or had completed a university degree (67%). While many professions were represented among the respondents, education and banking were the most common work/study industries encountered in this sample. On average, the participants in this study spent between five and nine hours online per week. This is consistent with findings from a recent PricewaterhouseCoopers study, which showed Canadians as spending an average of 5.1 hours per week on the Internet (Pastore 2000). Table 2 summarizes the familiarity with the online environment of the 223 subjects. Generally, this group was Internet-savy, where males were more likely to purchase online than females ($p<.05$), and respondents with higher education were also more likely to shop online ($p<.001$).

Table 2: Subjects' Prior Online Experience

Question	Total (%)	Female (%)	Male (%)
Hours online/week			
< 1	2	2	2
1 – 4	23	15	29
5 – 9	37	34	39
10 – 19	22	23	22
> 20	16	26	8
Online Activities			
Check e-mail	100	100	100
Banking	37	28	49
Perform research	92	89	97
Entertainment	68	65	72
Chat/Newsgroups	35	35	34
Trading	15	5	29
Job Search	51	51	51
Other	16	12	23
Previously purchased online	41	31	54
Online Purchases			

Books/Magazines	25	27	31
Collectibles	4	0	10
Videos	6	3	11
CDs	17	12	28
Clothing	9	7	15
Food	1	2	1
Computer hardware	8	5	14
Computer software	10	3	20
Information	8	4	15
Other	12	16	11
Reasons for NOT buying online			
Shipping expense	25	37	19
Delivery time	25	35	23
Security concerns	42	67	29
Privacy concerns	32	53	19
Lack of online vendor trust	29	48	18
Inability to experience product	43	70	29
Appeal of shopping offline	44	65	35
Other	8	10	9

Respondents were also asked whether they were loyal to any websites and if so, for them to list these websites. More than half (57%) of the respondents were loyal and many listed 4 or 5 sites they returned to repeatedly. The most loyal sites included Chapters.ca, Google.com, Amazon.com, Hotmail, hmv.com, globeinvestor.com, stockhouse.com, ticketmaster.ca and Yahoo! It is interesting to note that the vast majority of these sites displayed a trust seal-of-approval on their homepage.

7. Data Analysis

Validation of our model and propositions was based on analyzing subjective measurements collected from our questionnaire. Both closed-ended and open-ended questions were used to evaluate our propositions. Closed-ended questions collected either ordinal data on a 5-point Likert scale or binary data (yes/no) where no quantitative magnitudes were gathered. One sample t-test were employed where appropriate, since we could assume the underlying population of the sample means was normally

distributed due to our large sample size (n=223). We particularly found the open-ended questions provided richer insights for an exploratory study such as this.

When asked what factors made them trust vendor Web sites, respondents provided varied answers. However, a recurring theme among their comments was reputation. Remarks included: "reputation is the only real means to trust a site"; "a name, something that I recognize is critical. I trust that they value their reputation and will not disappoint me"; and "I would trust Ford or GM's website much more than I would a used car sales website that I had never heard of before". Along these lines, respondents felt that a "physical presence is a major bonus" since they are "hesitant to trust something that [they] really don't know exists". Access to "real people" was also an important physical marker. Some respondents mentioned that they "must be able to phone human employee anytime of day if problems occur" and one even stated that he "calls the phone number to make sure it is in service". Other studies have agreed that a vendor's trustworthiness often depends upon the strength of its reputation or brand name (de Groot and Egger, 2000; Jarvenpaa et al., 1999).

Another common trust engenderer was website design. Respondents commented that the "appearance of the site is critical" and it must "feel and look professional" since "a highly professional site looks less like a scam". At a minimum, to help establish trust, a website should have "proper English with no spelling or grammar mistakes" and should be "frequently updated to show the vendor cares enough to keep the content fresh". Respondents were skeptical of sites that "make too many promises" and "badgered

[them] with mailings and notices". A few subjects also mentioned the importance of an "automatic email reply after a purchase" and the "availability of a courier tracking number". Previous research supports these observations. The growth of trust has been suggested to strongly be affected by one's first impression of a system (Egger, 2000), and interface design factors have predicted user perceptions of trust (Laberge and Caird, 2000).

A third common trust engendered was referee recommendations. Respondents expressed a need to "hear good things about the website from friends and family", be involved in a "consumer environment, where discussions with customers are possible along different topics", and see "some sort of seal or sign that shows the site is secure and reliable". We further explore the influence of referees on consumer trust of online vendors through the analysis of our propositions.

P1: Online consumers are aware of seals-of-approval programs.

We asked participants how important it was to trust a vendor when purchasing a product or service online. As expected, almost all of the respondents (95%; $p<.001$) agreed that trust plays a very important role in the online vendor-customer relationship. The survey then provided definitions and examples of TTPs and seals-of-approval, followed by a question inquiring about their awareness of such seals. Interestingly, the awareness of seals-of-approval was still relatively low, with only 52% ($p>.05$) of respondents recognizing these seals. Comments made by the respondents indicated a need for TTP assurances, without realizing such seals already exist. For example, subjects stated that

"it would be great if sites could be approved by some sort of legal or government agency", "some sort of guarantee or warranty is needed if something goes wrong", and they "would like some concrete evidence of technical security". Many respondents relied on a "secure site indicator" which was described as the "little pad lock icon". This icon is automatically generated by a Web browser when entering a site that uses encryption security. Although security seals provided by TTPs, such as VeriSign, provide richer and more accurate assurances for website security, these respondents did not mention a need to view such security seals. Therefore, the proposition that most online consumers are aware of seals-of-approval programs was not supported in our findings.

P2: Seals-of-approval positively influence consumers' online purchasing decisions.

From those respondents that were aware of TTP's seals, 45% ($p>.05$) felt that seals-of-approval influenced their purchasing decisions. They commented that knowing a seal was present on a website, helped them to confirm the legitimacy of the vendor. Respondents stated that "third party regulators are important", "a guarantee given by the vendor is not enough" and they required guarantees to be "backed up by an official, physical and trustable organization".

In contrast, other respondents commented that they "rarely or never spend the time to check seal certificates", "trust lies more in the vendor" and they doubted if "the third parties would check the sites they verify very often – especially as they become larger". One subject went so far as to say "you never hear of a story whereby a site could not be hacked into due to a VeriSign seal". A subset of respondents did not trust the TTPs,

stating that they did "not know if they are real" and "perhaps the company just paid the regulator money to put the seal on their website". Such subjects tended to rely more on the recommendations of friends and family. Comments included: "if a friend refers it, then I can trust it"; "I trust all websites I've heard of through friends as being safe; and "only when family and friends have used the site OFTEN, will I trust it". "Magazine reviews", "good publicity" and "news programs that compare sites" were also mentioned as trust engenderers. Therefore, the proposition that seals-of-approval positively influence the purchasing decision of most online consumers that are aware of such seals was not supported by our findings.

P3: The influence of seals-of-approval will vary according to the phases of the trust lifecycle.

Trust can be built over time by passing through the four lifecycle phases outlined in our Online Trust Building Model. This lifecycle and its phases were clearly described in our survey. Following this description, respondents were asked which phase of the lifecycle best described their current online trust level, where most indicated the first two phases of chaos (29%) and establish (40%). As expected, we found that individual's position within the trust lifecycle was influenced by the amount of time they spent online. Respondents that spent less than 10 hours a week on the Internet tended to fall into the first two phases of the lifecycle (chaos and establish) ($p<.001$). Those respondents that spent between 10 to 19 hours online a week predominantly fell into the middle two lifecycle phases (establish and enhance) ($p<.05$). Lastly, 57% of respondents that spent more than 20 hours online a week fell in the last two lifecycle phases (enhance and

maintain). This was not statistically significant ($p>.05$), but this may be due to the relatively small sample ($n=35$) of respondents that spent more than 20 hours online per week.

Subjects were also asked which phases of the life cycle they thought seals-of-approval would influence them the most and the least. These results are summarized in Table 3. As proposed in our model, referees were significantly more influential in the establish and enhance stages of the trust lifecycle ($p<.001$), while their presence was not as important in the chaos and maintain stages ($p<.001$).

Table 3: Influence of Seals-of-Approval in Trust Lifecycle Phases

Trust Lifecycle Phase	Seals-of-Approval Influence the MOST	Seals-of-Approval Influence the LEAST
Chaos	20%	42%
Establish	32%	7%
Enhance	32%	7%
Maintain	16%	44%

Respondents indicated the need to build trust before they could consider buying from an online vendor, and seals-of-approval are "useful in the initial trust building process". Comments included: "ratings are important when you are thinking about buying from a new site"; "to buy from a site, I need a good reference from people I regard as 'experts' … not just buddies"; and "I don't buy things online and I have never heard of third party regulators, therefore they do not influence my decision. If I were to start purchasing online, I'm sure the fact that such groups exist would make me feel more confident in my purchase". Interestingly, one trusting respondent stated: "I start with trust and wait for a retailer to betray my trust. I do not start with suspicion and then ask someone to win my

trust". Therefore, the proposition that the influence of seals-of-approval will vary according to trust lifecycle phases was supported by our findings.

P4: A breech of trust will cause consumers to revert back to the chaos phase within the trust lifecycle.

The majority of respondents (62%; $p<.001$) believed that if they were to experience a breech of trust in any phase of the trust lifecycle, they would revert back to a chaos state where trust would be more difficult to re-establish. It was interesting to discover that 10% of the respondents did experience a violation of trust through their online experiences. From this group, 64% stated their personal online violation made them feel angry, 24% felt threatened, 8% felt unsafe, and 4% expressed no feelings towards this breech of trust. Therefore, the proposition that a breech of trust will cause most consumers to revert back to the chaos state was supported by our findings.

8. Conclusion

Researchers warn that a lack of trust may be the most significant long-term barrier for realizing the full potential of electronic commerce (Keen 1997; Hoffman et al. 1999; Roy et al. 2001). Trust is a dynamic process that must be built over time. Since business-to-consumer electronic commerce is still in its infancy, trust in this new market is still relatively scarce. However, various approaches have been suggested to help accelerate the trust building process for the online consumer. For example, emphasizing existing branding or an established offline presence, designing websites that induce customer confidence through professionalism and usability, assuring transaction security, privacy

and reliability through third-party recommendations, and fulfilling online promises can go a long way to engender consumer trust in online vendors.

This paper present a new conceptual model for online trust, which illustrates the phases of consumer online trust and outlines the necessary interactions between consumers, vendors and referees to progress from one trust phase to another. This model can help to further our understanding of online trust, provide online vendors with methods for building consumer trust, and direct future research in this new promising field. From this model, this paper focused on the impact and influence of trusted third-party referees and their seals-of-approval as mediators for building online consumer trust. A survey was conducted as an initial investigation into validating our conceptual model and testing our seals-of-approval propositions. We were surprised to find that the general awareness of seals-of-approval was still relatively low, with just over half of our respondents being aware of such seals. Similarly, from those that were aware of trust seal programs, less than half of our respondents felt that these recommendations influence their online purchasing behavior. These results are similar to earlier studies (Cheskin/Sapient 1999), but it was interesting to find that the awareness and influence of seals-of-approval has not noticeably increased the last few years. Both online vendors and trusted third-party referees need to work together to help increase the visibility and awareness of seals-of-approval. However our model was supported in that respondents agreed that the influence and impact of third-party referees varies according to the phases of the trust lifecycle. Additionally, we found that a breech of trust will cause most consumers to revert back to the chaos state where it may be more difficult to re-establish online trust.

Some limitations of this study must be considered when interpreting our findings. Since this was designed to be an initial investigation in this area, robust constructs were not painstakingly developed and utilized. Additionally, there are some inherent limitations with survey experiments. Turner and Martin (1984) caution that people's self-reported preferences often do not match their real world behavior. Representative samples may also be difficult to obtain, especially with online questionnaires.

Future research in this area may include the following:

- Seals-of-approval address issues of security, privacy and reliability. To what degree do these issues address the concerns of the online consumer? What other concerns can be alleviated by trusted third-parties? Future research is needed to match consumer concerns with trusted third-party offerings and more fully explore any potential gaps.

- This research examined the online consumer trust lifecycle from a holistic point of view. Respondents to our survey were asked to indicate their opinions and perceptions of online vendors and seals-of-approval in general, rather than focusing on a certain product or industry type. It seems likely that consumers' opinions and location within the lifecycle will depend on the types of products or services being examined. Further research is needed to investigate this more fully.

- Our study showed that consumers are still relatively unaware of trusted third-parties and their seals-of-approval. Future research could focus on providing solutions to increase this awareness level, such as modifying where and how these seals are displayed.

- This study focused on authenticating online vendors for consumers. However, vendors may also need consumer authentication to conduct online transactions. Future research could examine how trust in the consumer can be built and communicated for the online vendor.

- Jarvenpaa et al. (1999) propose that consumers in different cultures might have different expectations of what makes an online vendor trustworthy. Although some trusted third-parties provide seals-of-approval for various parts of the world, the perceptions of these seals in different cultures is largely unknown.

Trust is a long-term proposition that may be tough to build and easy to lose. However, there are many methods that can be employed to help engender this trust among online consumers. Assurances provided by trusted third-parties is just one such method. Nevertheless, no matter how much an online vendor strives to attract customers through trust-building techniques, it is all for naught if the vendor can not fulfill the promises made.

References

Adams, A., and Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), December, 41-46.

Anderson, E., and Weitz, B.A. (1989). Determinants of continuity in conventional industrial channel dyads. Marketing Science, 8, 310-323.

Anderson, B. (1991). *Imagined Communities: Reflections on the Origin and Spread of Nationalism*, New York: Verso.

Ambrose, P.J. and Johnson, G.J. (1998). A Trust Based Model of Buying Behaviour in Electronic Retailing. Proceedings of the *Fourth Conference of the Association for Information Systems*, August, 263-265.

Ba, S. and Pavlou, P.A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, to appear.

Baba, M.L. (1999). Dangerous liaisons: Trust, distrust, and information technology in American work organizations. *Human Organization*, 58(3), 331-346.

Bagozzi, R.P. and Dholakia, U.M. (2002). Intentional social action in virtual communities. *Journal of Interactive Marketing*, 16(2), Spring, 2-21.

Barber, D. (1983). *The Logic and Limits of Trust*. New Jersey: Rutgers University Press.

Benassi, P. (1999). TRUSTe: An Online Privacy Seal Program, *Communications of the ACM*, February, 42(2), pp. 56-57.

Bowlby, J. (1973). *Attachment and Loss: Vol. 2. Separations: Anxiety and Anger*. London: Hogarth Press.

Buskens, V. (1998). The social structure of trust. *Social Networks*, 20(3), 265-289.

Cashell, J.D. (1999). WebTrust: A seal of approval. *The Internal Auditor*, 56(3), 50-53.

Cheskin Research and Studio Archetype/Sapient (1999). *eCommerce Trust Study*, http://www.studioarchetype.com/cheskin/, accessed August 2001.

Cox, B. (1999). Security, privacy remain top consumer concerns. InternetNews.com, April 9, http://www.internetnews.com/ec-news/article/0,1087,4_95031,00.html

Davis, S.M. (2000). The Power of the Brand. *Journal of Strategy and Leadership*, 28(4), 4-9.

De Groote, B. and Egger, F.N. (2000). Designing for Trustworthiness: The Case of www.euroclix.nl. Proceedings of the *CHI 2000 Workshop: Designing Interactive Systems for 1-to-1 E-Commerce*, April.

Deutsch, M. (1958). Trust and suspicion. *Conflict Resolution*, 11(4), 265-279.

D'Hertefelt, S. (2000). Trust and the perception of security. InteractionArchitect, January, http://www.interactionarchitect.com/research/report20000103shd.htm, accessed June 2001.

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

Dowling, G.R., Staelin R. (1994). A Model of Perceived Risk and Intended Risk-handling Activity. *Journal of Consumer Research*, p.119-134.

Dreze, X., Zufryden, F. (1998). Is Internet advertising ready for prime time? Journal of Advertising Research, 38(3), pp. 7-18.

Egger, F.N. (2000). "Trust Me, I'm an Online Vendor": Towards a Model of Trust for E-Commerce System Design. Proceeding of the *CHI2000 Extended Abstracts: Conference on Human Factors in Computing Systems*, April, 101-102.

Erickson, E.G. (1963). *Childhood and Society*. New York: W.W. Norton.

Frazier, G.L., Speckman, R. and O'Neal, C.R. (1988). Just-In-Time Exchange Relationships in Industrial Markets. *Journal of Marketing*, 52, October, 52-67.

Froomkin, A.M. (1996). *The essential role of trusted third parties in electronic commerce*. http://www.law.miami.edu/~froomkin/articles/trusted.htm, accessed October 2001.

Fukuyama, F. (1996). *Trust: The Social Virtues and the Creation of Prosperity*. Free Press.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing*, 58, 1-19.

Geyskens, I., Steenkamp, J., Scheer, L.K., Kumar, N. (1996). The effects of trust and interdependence on relationship commitment: A transatlantic study. *International Journal of Research in Marketing*, 13, pp. 303-317.

Görsch, D. (2001). Internet limitations, product types, and the future of electronic retailing. In *Proceedings of the 1st Nordic Workshop on Electronic Commerce*, Halmstad, Sweden.

Good, D. (1988). Individuals, interpersonal relations, and trust. In D. Gambetta (ed.), *Trust: Making and breaking Cooperative Relations*. New York: Blackwell.

Grandison, T. and Sloman, M. (2000). A survey of trust in Internet applications. *IEEE Communications Surveys*, Fourth Quarter.

Greenspan, R. (2002). *Seals of Approval*. eCommerce Guide, June 6, http://ecommerce.internet.com/news/insights/ectips/article/0,,10380_1347831,00.html, accessed June 2002.

Greenstein, M. and Feinman T. (2000). *Electronic Commerce: Security, Risk Management and Control*. Boston: Irwin McGraw-Hill.

Head, M.M. (2000), "Trust is a Must in E-Commerce", Hamilton Spectator, July 28, pp. R4.

Head, M.M., Yuan, Y., Archer, N. (2001). Building Trust in E-Commerce: A Theoretical Framework. Proceedings of the *Second World Congress on the Management of Electronic Commerce*, January.

Head, M.M. and Yuan, Y. (2001). Privacy Protection in Electronic Commerce: A Theoretical Framework. *Human Systems Management*, 20, 149-160.

Hodges, M. (1997). Building a bond of trust. *Technology Review*, 100(6), 26-27.

Hoffman, D.L., Novak, T.P., Peralta, M. (1999). Building consumer trust on-line. *Communications of the ACM*, 42(4), April , 80-84.

Hosmer, L.T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review*, 20(2), 379-401.

Jarvenpaa, S., Tractinsky, N., Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer Mediated Communication*, 5(2), December, 1-37.

Kee, H.W. and Knox, R.E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Conflict Resolution*, 14(3), 357-366.

Karvonen, K. (1999). Creating trust. In *Proceedings of the Fourth Nordic Workshop on Secure IT Systems*, Kista, Sweden, 21-36.

Keen, P.G.W (1997). Are you ready for "trust" economy? *ComputerWorld*, April 21, pp. 80.

Konrad, K., Fuchs, G. and Bathel, J. (1999). Trust and electronic commerce – More than a technical problem. *The 18th Symposium on Reliable Distributed Systems*, Lausanne, Switzerland.

Kovar, S.E., Gladden Burke, K. and Kovar, B.R. (2000). Consumer Responses to the CPA WebTrust™ Assurance. *Journal of Information Systems*, 14(1), Spring, 17-35.

Laberge, J., Caird, J.K. (2000). Trusting the Online Banking Interface: Development of a Conceptual Model Relevant to E-commerce Transactions. Proceedings of the CHI 2000 Workshop: Designing Interactive Systems for 1-to-1 E-commerce, April.

Levin, C. (2000). Web Dropouts : Concerns About Online Privacy Send Some Consumers Off-Line, *PC Magazine*, January 19, http://www.zdnet.com/pcmag/stories/trends/ 0,7607,2423811,00.html.

Lewis, D. and Weigert, A. (1985). Trust is a social reality. *Social Forces*, 63(4), 967-985.

Lewicki, R.J. and Bunker, B.B. (1995). Trust in relationships: A model of development and decline. In B.B. Bunker and J.Z. Zubin (eds.), *Conflict, Cooperation, and Justice: Essays Inspired by the Work of Morton Deutsch.* San Francisco: Jossey-Bass.

Macy, M.W. and Skvoretx, J. (1998). The evolution of trust and cooperation between strangers: A computational model. *American Sociological Review*, 63(10), 638-660.

Marcella, A.J. (1999). *Establishing Trust in Virtual Markets*. Altamonte Springs, FL: The Institute of Internal Auditors.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734.

Mehadevan, B. and Venkatesh, N.S. (2000). A framework for building on-line trust for business to business e-commerce. In *Proceedings of The IT Asia Millennium Conference*, Bombay, India.

Milne, G.R. and Boza, M. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13(1), 5-24.

Moorman, C., Deshpande, R. and Zaltman, G. (1993). Factors Affecting Trust in Market Research Relationships. *Journal of Marketing*, 57, January, 81-101.

Needham, P. (1998). Developing trust and credibility, *TICG Newsletter*, http://www.intercongroup.com/aug98news.html, Accessed July 2000.

Nielsen, J. (1999). Trustworthiness in web design. *Alertbox*, March, http://www.useit.com/alertbox/990307.html

Nielsen, J., Molich, R., Snyder, C. and Farrell, S. (2001). *E-Commerce User Experience*, Nielsen Norman Group: Fremont, CA.

Nöteberg, A. (1999). *Trusting the Web? Web assurance seals for an improved electronic commerce environment*. MA Thesis, University of Amsterdam.

Pastore, M. (2000). Canadians Going Online and Going at High Speeds, *CyberAtlas*, November 17, http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_514861,00.html

Princeton Survey Research Associates (2002). A matter of trust: What users want form web sites. Results of a national survey of Internet users for *Consumer WebWatch*.

Povey, D. (1999). Developing Electronic Trust Policies Using a Risk Management Model. In *Proceedings of the 1999 CQRE (Secure) Congress*, Düsseldorf, Germany.

Ratnasinghan, P. (1998). The importance of trust in electronic commerce. *Internet Research*, 8(4), 313-321.

Ravald, A. and Grönroos, C. (1996). The Value Concept and Relationship Marketing. *European Journal of Marketing*, 30(2), 19-30.

Resnick, P., Zeckhauser, R., Friedman, E., Kuwabara, K. (2000). Reputation Systems. *Communications of the ACM*, 43(12), December, 45-48.

Rotter, J.B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1), 1-7.

Roy, M.C., Dewit, O., Aubert, B.A. (2001). The Impact of Interface Usability on Trust in Web Retailers. *Internet Research: Electronic Networking Applications and Policy*, 11(5), 388-398.

Seligman, A.B. (1998). Trust and sociability: On the limits of confidence and role expectations. *The American Journal of Economics and Sociology*, 57(4), 391-404.

Shapiro, S.P. (1987). The social control of impersonal trust. *American Journal of Sociology*, 93(3), 623-658.

Simmons, G.J. (1993). An introduction to the mathematics of trust in security protocols. In *Proceedings of Computer Security Foundations Workshop IV*, 121-127.

Sisson, D. (2000). *Ecommerce: Trust and Trustworthiness*. http://www.philosphe.com/commerce/trust.html, accessed March 2002.

Siyal, M.Y. and Barkat, B. (2002). A novel trust service provider for Internet based commerce applications. *Internet Research*, 12(1), 55-65.

Speier, C., Harvey, M., and Palmer, J.W. (1998). Virtual management of global marketing relationships. Journal of World Business, 33(3), pp.263-276.

Srivastava, R.P. and Mock, T.J. (2000). Evidential reasoning for WebTrust assurance services. *Journal of Management Information Systems*, Winter 1999-2000, 16(3), 11-32.

Steer, D. (1999). Privacy practices help build trust, get and retain web customers. *EC Management*, 1(10), http://ecmgt.com/Nov1999/feature.article.htm.

Steinfield, C., Whitten, P. (1999). Community Level Socio-Economic Impacts of Electronic Commerce. Journal of Computer-Mediated Communication, 5(2), December.

Stratford, T. (1999). eTrust: Building Trust Online. *Journal of Integrated Communications*, May.

Strub, P.J. and Priest, T.B. (1976). Two patterns of establishing trust: The marijuana user. *Sociological Focus*, 9(4), 399-411.

Turner, C., and Martin, E., eds. (1984). *Surveying Subjective Phenomena*. New York: Russell Sage Foundation.

Westin, A., Maurici, D. (1998). E-Commerce & Privacy: What Net Users Want, *Louis Harris & Associates Survey*, June.

Yoon, S. (2002). The Antecedents and Consequences of Trust in Online-Purchase Decision. *Journal of Interactive Marketing*, 16(2), Spring, 47-63.

Zand, D. (1972). Trust and managerial problem solving. *Administrative Science Quarterly*, 17, 142-152.