PACIS 2005 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2005

A Framework for Assessing Payment Security Mechanisms and Security Information on e-Commerce Web Sites

Mustafa Ally
University of Southern Queensland

Mark Toleman
University of Southern Queensland

A Framework for Assessing Payment Security Mechanisms and Security Information on e-Commerce Web Sites

Mustafa Ally
Department of Information Systems
University of Southern Queensland
Toowoomba Qld 4350 Australia
Mustafa.Ally@usq.edu.au

Mark Toleman
Department of Information Systems
University of Southern Queensland
Toowoomba Qld 4350 Australia
Mark.Toleman@usq.edu.au

Abstract

The enthusiasm of many consumers when selecting products for purchase over the Internet is often dampened at the point of payment largely over security and privacy concerns and financial risks. The levels of confidence that exist among potential and existing online purchasers can be influenced significantly by the extent to which merchants inform and reassure their customers over security features and mechanisms that support their e-payment options. This study sets out to establish how online merchants attempt to engender this trust in the payment instrument options on offer to potential customers by indicating technical competence and ability to meet fiduciary obligations. A preliminary assessment of a selected number of Australian web sites was made to determine the extent to which they realize security solutions and other trust mechanisms in practice, and the level and the quality of information they provide to consumers on the technical security solutions in place.

Keywords: Trust, e-Commerce, Electronic Payment Systems, Security

1. Introduction

When making decisions about which electronic payment methods are most appropriate for them, online consumers would have to consider, in addition to the methods being cost-effective and appropriate for their purposes, two important factors, namely, whether sufficient security was in place to protect them against fraudulent activity and whether their privacy would be protected (Shaw 1999). A study of European consumers (Hegarty et al. 2003) showed that these security concerns were raised more frequently ahead of the more generic ones concerning the usability, functionality and added value of a given Electronic Payment Instrument (EPI) or electronic payment application. As a result of this there is a widely held perception that, despite strong growth in e-commerce and especially in electronic banking and commerce, the general public lacks confidence in the security aspects of conducting transactions electronically, particularly those that involve a payment of some kind, i.e. using Electronic Payment Instruments (Hegarty et al. 2003). VeriSign (www.verisign.com.au) quotes various market research studies conducted in 2004 that demonstrate that consumer concerns about online security have been deterring potential consumers from finalising purchases: 64% of online shoppers have abandoned a shopping card/basket or failed to complete an online purchase because they did not get a sense of security and trust when it came time to providing payment information; 56% of users reported that they were protecting themselves from identity theft specifically by limiting their online purchases to reputable web sites. These translate to an urgent need for merchants to allay these fears and to engender in their consumers the requisite trust in the payment instrument as well as in the payment process as a whole.

Trust has been recognized as a critical factor in the development and growth of e-commerce. In fact, according to Van Slyke and Belanger (2003) the level of trust that individuals and organizations are willing to place in businesses selling goods and services online is one of the most important barriers to the use of the Internet for conducting business today. The lack of consumer trust with respect to online privacy and security, for example, has prevented many consumers from engaging in online shopping. Many consumers are not comfortable divulging personal and financial information to a virtual storefront. Equally importantly the financial risks involved in online transacting, namely through fraud and loss of purchase, have made consumers wary of purchasing and paying for goods over the Internet.

This resistance on the part of customers to pay for goods and services online is prevalent despite the rapid developments in technologies that have made significant contributions to securing the Internet for electronic commerce. The question arises as to what is it that is preventing them from doing so. Yousafzai, Pallister & Foxall (2003) suggest that creating greater awareness and educating customers is an important key to increasing consumer confidence. One obvious approach in this regard is for merchants to inform and reassure their customers about the security features and mechanisms that they have put in place to support the available electronic payment options.

Given that disclosure (Shneiderman 2000) and transparency (Grabner-Kraeuter 2002) are presumed to be trust building approaches in website transactions, the objective of this study was to undertake an assessment of a selected number of Australian web sites in order to identify the Payment Security Mechanisms they had in place and to evaluate the quality of their Security Information, within the background of a framework developed for this study (see Figure 1). This web assessment is the first step toward determining the factors that influence the decision to use a payment instrument at the checkout stage during a transaction. It is therefore assumed, for the purposes of this study, that all the factors necessary for engendering trust in the merchant are already in place and the dilemma facing the online customer is concerned with the risks associated with which EPI to initiate in order to conclude the final part of the transaction process, the payment step.

The framework also helps contextualize the two aspects (payment security information and payment security mechanisms) that were assessed on the websites and draws their likely relationship to the concept of trust based on theoretical constructs and factors identified in past studies.

The next section describes the selection of the web sites for assessment and the process used for ascertaining the elements associated with security mechanisms and information quality. This is followed by a description of the results obtained within the backdrop of the theoretical foundations of the proposed framework and the justification of the constructs used in this context.

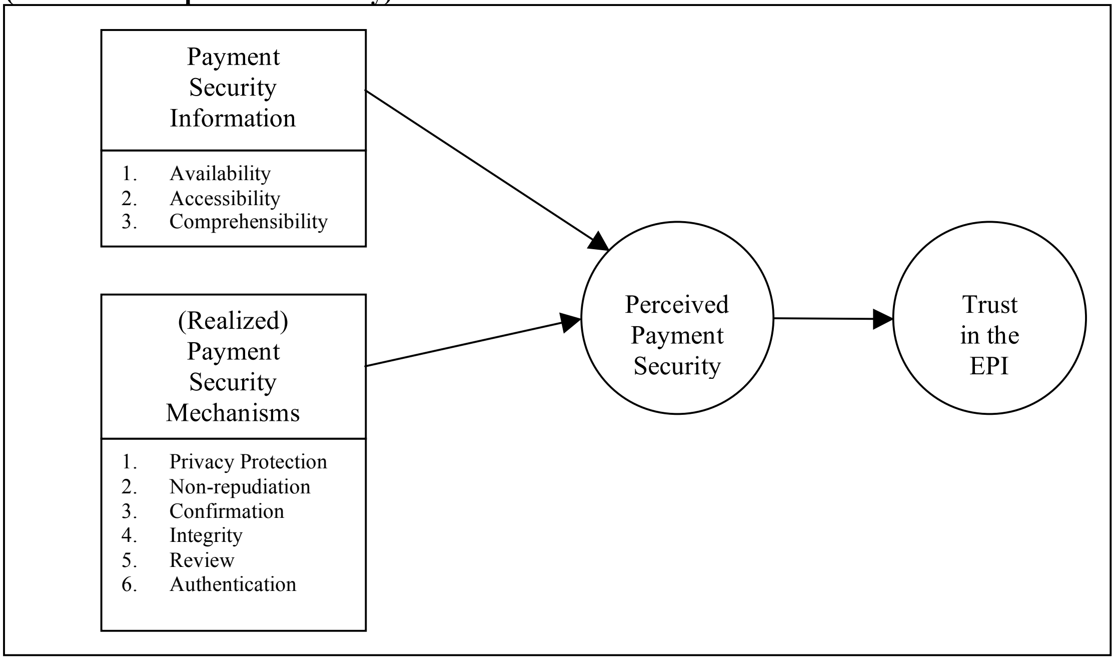
2. Research Method

In an attempt to provide an experience-based snapshot of what is essentially a very fast-changing situation, a sample of eighty-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 such as Amazon.com have often served 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. They reflect a diverse range of small, medium and large-sized stores with offices in Australia and whose main source of income revenue is derived from the Australian market. 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 then searching, identifying and recording the security and privacy elements (see

Table 1) that a consumer would typically look for and encounter in the course of making a purchase. The steps taken during the assessment process commenced with scanning the home page of the site for any explanations given regarding its security features and its privacy policies along with any explicit assurances given to its customers. This was then followed by stepping through a typical purchasing cycle (selecting an item, adding it to the shopping cart, going to the checkout, entering the payment details) and recording the required information along the way but stopping short at the final confirmation of the payment details.

Figure 1: Framework for Assessing Payment Security Mechanisms and Security Information (Source: Developed for this study)



3. Theoretical Foundations

3. 1 Trust (in the EPI)

Following Mayer et al. (1995) and Rousseau et al. (1998), for the purposes of this study a customer's trust in an electronic payment instrument is defined as a psychological state which leads to the willingness of the customer to use an EPI for the purposes of finalizing an online purchase, with the expectation that all the parties concerned with the transaction (merchant, financial institutions, payment service providers, etc.) will fulfil their contractual obligations and that all the necessary payment infrastructure and control and security mechanisms are in place, irrespective of the customer's ability to completely monitor or control the payment process.

According to Yousafzai et al. (2003), this definition captures two discrete but non-separable aspects of trust in the context of online purchasing. Firstly, it involves the traditional view of trust in a specific party or parties i.e. the organisations involved in the transaction process, and secondly, it implicitly encompasses trust in the integrity of the payment instrument.

Two of the dimensions of trust proposed by McKnight and Chervany (2002) have particular import in this study. One of the dimensions '*institution based trust*' represents the beliefs held by an individual that the necessary conditions (structures and situations) are in place to be able to confidently anticipate a trusting outcome from an endeavour. It represents an environment in which "one feels safe, assured, and comfortable (not distressed or fearful) about the prospect of depending on another". This trust in control mechanisms (control trust), refers to embedded protocols, policies and procedures in e-commerce that help to reduce the risk of opportunistic behaviours among consumers and Web retailers.

The other dimension of trust that can lead to a person's trusting intention is that of '*trusting beliefs*' which embodies the perception of the competence, integrity and benevolence of (in this case) the payment instrument. Their third trust dimension, namely, a person's '*disposition to trust*' is not considered in our model. While the institutions have the ability to influence their customer's trusting beliefs (trust in the payment security mechanisms) as well as their institution based trust (perception of trustworthiness in the EPI), this aspect of trust cannot be influenced by the merchant or the EPI itself in any direct way to help encourage customers develop confidence in the instrument and to believe that it is safe to use it.

Various attributes that impact on the level of trust in an online environment have been identified over recent years. In particular, Hoffman et al (1999) focus on security and privacy as the key drivers of online trust with others also asserting that only after security and privacy have been addressed will a consumer consider other web features to determine the extent to which they can trust and feel safe transacting with the web merchant (Dayal et al. 1999).

3.2 Perceived (Payment) Security

Following the extant definitions of perceived information security (Chellappa et al. 2002; Ratnasingam et al. 2003; Yousafzai et al. 2003) applied in a general e-commerce context, we describe perceived payment security, for the purposes of this research, as the subjective probability with which consumers believe that their payment information will not be viewed, stored, manipulated or fraudulently abused by unauthorised users during transit, storage or processing, in a manner consistent with their expectations that the obligations of all parties concerned in the transaction (including the payment instrument itself) will be fulfilled. This suggests that any assessment of the risks involved is intuitive rather than one involving any objective measurement.

However, while perceived security is a subjective belief, the mechanisms that serve as the antecedents are built upon the self-assessment of various objective technological solutions (Chellappa et al. 2002). Therefore, the perceptions of security are influenced by implementation of such security measures as privacy, transaction integrity, authentication, confidentiality, non-repudiation etc.

In addition, the way, and the extent to which, this security information is presented to the potential customer is likely to impact on the customer's understanding and confidence in the payment security being provided by the merchant. According to Furnell and Karweni (1999) consumers who have a greater awareness of security are more likely to use Internet-based services, implying that awareness is fundamental to increasing consumer confidence.

The importance of these factors is re-iterated in the principles of the *Australian e-commerce Best Practice Model* (BPM) (http://www.ecommerce.treasury.gov.au) which set out to improve online security and promote consumer confidence. The BPM recommends that online businesses:

- Provide security appropriate for protecting consumers' *personal and payment information*;
- Provide security appropriate for *identification and authentication mechanisms* to be used by consumers.
- Update their *security and authentication mechanisms* over time to make sure the security offered is maintained, at an appropriate level.
- Provide consumers with *access to information* on ways of making payments and how to best use those mechanisms. It is an established principle of the consumer protection

law that information communicated to consumers should in general be widely available, easily accessible and comprehensible.

The following two sections identify and elaborate on how, and to what extent and level, these requirements have been realized in our sample website assessment.

4. Payment Security Mechanisms

(Perceived) security plays a crucial role in gaining customer confidence in the payment instrument. It is derived from, among other things, the level of security provided by the technology, together with how it is marketed. If the system can offer convincing answers on issues of authorisation, authentication, privacy, integrity, redress mechanisms, and procedures for reviewing and amending erroneous transactions, then a high level of trust in the system should ensue.

This section discusses the security mechanisms likely to have an impact on consumer perceptions of both security and trust alongside an overview on the realization of security solutions and other trust mechanisms in practice, arising from our preliminary assessment of our selected web sites in Australia. The purpose of the investigation was to assess what security solutions were in practice and how in fact these security measures were being implemented.

We focus on what could be observed with regard to payment possibilities and visible security measures, i.e. the ‘external’- focus rather than the inherent ‘internal’ features of each payment product.

According to Hegarty et al. (2003) secure payment solutions depend on the following factors:

- Inherent security features of the payment products used
- Site security, i.e. how well secured is the site infrastructure
- The way security features of payment products are implemented
- Non-technical security measures (procedures, policies, etc)

Research has shown that online merchants can have a substantial effect on influencing institution based trust by implementing security measures that ensure transactional security (Benassi 1999; Bhimani 1996). The perception of risks associated with system dependent uncertainty, that is, concerns about the functional and security aspects that could arise from use of an EPI for payment purposes, can be strongly influenced by a merchant’s behavioural actions that aim to reduce infrastructure-related concerns and increase trust in the instrument.

Chellappa (2002) argued that trust would be favourably influenced by an increase in perceptions of security and privacy in electronic transactions. In a Web survey of 502 cases of Internet banking users Suh and Han (2003) found that customer perceived strength of non-repudiation, privacy protection, and data integrity were important determinants of e-commerce acceptance. It is therefore proposed that consumer perceptions of security are likely to be engendered through visible mechanisms such as privacy statements, authentication, integrity, non-repudiation, payment review and confirmation.

The antecedents of perceived payment security

Technology trust, that is, trust in the transaction infrastructure and underlying control mechanisms is based on technical safeguards, protective measures, and control mechanisms that aim to provide reliable transactions from timely, accurate, and complete data transmission (Cassel et al. 2000). Technology trust encompasses security services such as

digital signatures, encryption mechanisms (public key infrastructure) and authorization mechanisms (User IDs and passwords).
In relation to the actual use of a payment instrument during and after making an online payment, there are several key areas that are considered to be sensitive enough to be a potential source of concern for consumers.

Authentication is the mechanism by which the one party to a transaction presents an identifier and the other party verifies the claimed identity, preventing both forgery and impersonation. The problem of repudiation generally arises from the anonymous nature of the transaction where the merchant cannot physically see the customer. The vast majority of these transactions are not authenticated thereby increasing the incidence of fraud (GPayments 2001). Being able to prove the authenticity of the payment, the payer and the payee is fundamental to the widespread adoption of e-payments (Jewson 2001). The exact authentication methods and authorization processes used to obtain this guarantee depend on the payment instrument or payment model being used, which in turn are defined by the business risks associated with this instrument (Centeno 2001).

When a customer provides payment information he needs assurance that his payment transaction is being made to the merchant with whom he is dealing. SSL/TLS, with a server certificate only, is a commonly used cryptographic technique to encrypt the information transferred across the Internet. However, it also allows the end user to easily verify whether the webserver actually belongs to the merchant (if he has trust in the issuer of the server certificate). Typically merchant authentication is effected through independent third parties such as Thawte (www.thawte.com/) and VeriSign (www.verisign.com/) who provide such guarantees.
While electronic payment instruments offer increased economic efficiencies and convenience over traditional payment systems they are subject to a number of risks arising from the open nature of the Internet, not least of which is the risk of fraud. Closely allied to the need for authentication is the consumer's fear of falling victim to fraud. The reported volume and growth of Internet fraud and crime add to a widespread perception that the Internet is riskier for transactions than the face-to-face environment.

A variety of techniques and tools to combat online fraud, particularly with card usage, have been developed and refined over the years. These include Address Verification Services (AVS) where the numeric data in a customer's street address and postal code are checked against an existing database; Card Security Code (CSC) check requiring the customer to enter the three digit code on the back of the card and used as an authentication scheme to reduce fraud for Internet or card-not-present transactions; commercially and internally developed fraud screening tools; recording of IP addresses; and manual reviews of orders. It is important to note that while these measures do not guarantee the customer non-fraudulent transactions it does assist with mitigating some of the risks associated with it.

Recently the credit card organizations (Visa and MasterCard) introduced the 3DSecure ("Verified by Visa" or VbV) and UCAF/SPA ("SecureCode") buyer authentication programs respectively, designed to provide an added level of security for merchants and consumers. Developed to address the problem of the lack of an effective and efficient means of authenticating cardholders, the schemes require the customers to register with his issuer once and then enter a password at the point of payment each time the buyer makes a purchase, thereby authenticating his identity and reducing his (and the merchant's) exposure to card-not-present fraud loss.

Without strong and effective authentication there is erosion of consumer confidence and trust in the process. Given that authentication is an implicitly perceptible mechanism and directly related to payment security it should also influence consumer security perceptions (Chellappa et al. 2002).

This study proved SSL/TLS, with a server certificate only, to be by far the most popular security mechanism and used by all of the web sites in our sample that requested credit card details (whether the credit card payment was being processed instantly or manually).

None of the websites used SSL with both server and client certificates that would have allowed for the identification of both the vendor and the customer during the transaction process.

Despite also offering merchants protection from chargebacks due to fraud ***none*** *of the sites assessed are currently using the card association payer authentication schemes (VbV and SecureCode).*

While very popular in the US and the UK, Address Verification Systems (AVS) which check to see if the address of the order is the same as the authorized user is not in use Australia largely because of the country's privacy policy. Less than 1% of the sites requested for the customer's three or four-digit card security code (CSC) when paying by credit card but more than half warned that they were capturing and saving the customer's IP address in order to protect against fraudulent activities and to identify the geographical location of the cardholder.
During the assessment process it was impractical to establish the extent of any backend manual review of the order that might have been taking place.

Non-repudiation mechanisms should make it very difficult for a customer, once having made a payment, to (a) deny responsibility for the transaction and (b) demand reimbursement of funds from the merchant. On the other hand the customer also wants the assurance that the merchant can link the payment instruction to him, and that this link cannot be denied. To that purpose, the websites could use customer accounts that are set up when first becoming a customer (and then re-used) with the establishment of credentials or simply a personal e-mail address.
More elaborate schemes for non-repudiation are through the use of digital certificates and signatures), and PIN and password-based (payer) authentication schemes (for example, Verified by Visa (VbV) and SecureCode).
The problem of repudiation of a transaction is exacerbated by the separation of the merchant and the customer and the absence of physical identification, signature or similar means of proof of purchase or payment.
The extent to which mechanisms are put in place to facilitate dispute resolution should engender confidence in the payment process and influence consumer (and merchant) security perceptions.

We noted that a majority of the visited websites (65%) requested the set-up of a customer account before processing any transaction.
The one step online process was by far the most popular way of creating a customer account or customer profile. Less than 2% of the sites required a two-step registration process.

The websites analysed either did not have or did not explain the mechanisms they used to prevent repudiation of the transactions. Digital signatures were not used at any of the websites.

Privacy protection mechanisms can mitigate consumers' fear that their personal information is adequately safeguarded by the entity collecting the information. The customer would like assurance that the information given to the merchant in a payment instruction cannot be (re-) used by another party to generate another, fraudulent, transaction. This protection can take the form of physical control measures against intruders such as firewalls, and through disclosure policies that include assurances about who is collecting the data, how it will be used, how it is stored and how securely it is protected.

Merchants are always interested in customer profiling for purposes of directing their marketing efforts more accurately. Despite security mechanisms, customers typically are very reluctant to divulge personal details over the Internet. Many have never made an electronic purchase because of fear of data misuse in the anonymity of the Internet.

By disclosing a website's privacy practices and the measures in place to protect the consumer, merchants will significantly ease consumers' privacy concerns when submitting payment details, building a more trusting environment for online transactions in the process. Given that protection is a commonly encountered mechanism for information security, its extent should influence consumer security perceptions.

96% of the visited websites collected the payment information themselves while the others re-directed the customer to a third party.

65% of websites were specific about which elements of the customer's personal details they would be storing as well as other types of data such as customer domain and host names, IP addresses, browser software and operating system being used, date and time of access, the Internet address of the web site from which the customer linked to the merchant site, etc, explaining that these were being used to monitor usage of their sites.

About 29% of the websites provided any information about the place where and how customer information was going to be stored. This included such protection mechanisms as secure databases and firewall safeguarded server systems.

Amongst the websites storing customer information, 40% indicated that they stored the credit card numbers but none gave their customers the opportunity to opt out of having such payment details of theirs stored by the merchant.

Table 1: Payment Security and Privacy Elements Assessed

REALIZATION OF PAYMENT SECURITY MECHANISMS
Authentication
SSL with server certificate
SSL with server/client certificate
identification of certification authority
payer authentication (Verified by Visa, SecureCode)
other fraud detection mechanisms
Non-repudiation
customer account required
explanations of non-repudiation given
explanation of non-repudiation mechanism used
digital signatures
Privacy protection
information collected by merchant
information collected by 3rd party
disclosure of type of information stored
disclosure of place where customer info is stored
storing credit card numbers
disclosure of protection mechanisms used (detailed or simple disclosure)
compliance with Privacy Act 1988
compliance with Privacy Amendment (Private Sector) 2001
Confirmation
reference to any confirmation method
originator of confirmation (merchant, third party)
Integrity
secured personal info
secured payment info
SSL
credit card info via e-mail
Review
confirmation of order details before finalization
information about final check
PAYMENT SECURITY INFORMATION
Availability
technical features of an EPI, usability, purpose and added-value of their implementation
instructions about how to use an EPI
procedures in the event of a transaction failure
instructions about how to prevent physical, functional or other defaults of an EPI and/or flaws of the e-payment system in question
Accessibility
easy to find
made available either in the general frame or as a link on each web page
location on web site
Comprehensibility
easily understandable
brevity and generality

40% of all the websites did not provide disclosure about any protection mechanisms they were using. However, this did not necessarily mean that they did not have any in place. Of the ones that did, 53% of them provided detailed descriptions while the rest supplied only brief explanations.

17% of the sites indicated that they complied with the Privacy Act 1988, while only 9% referred to the more recent Privacy Amendment 2001.

Less than 5% of the sites offered any explanations about cookies or whether in fact that they were using them during the ordering and payment process and for what purpose.

Confirmation acknowledging receipt of payment by the merchant can reassure a customer that the merchant has received his payment transaction. To assure the customer that the payment has in fact been received, a confirmation should be sent to him using one of several available methods (online, email, etc.). The originator of the confirmation can also be different, depending on the collector of the payment.
Providing confirmation information about a payment should influence a consumer's security perception.

As the assessment process stopped short of taking the final payment step it was not possible to determine the actual method the merchant or a third party was using (if any at all) to confirm receipt of the order and payment. However, a small percentage (less than 10%) of the merchants provided some explanations of how the order would be confirmed indicating the method (e.g. e-mail, online receipt) and the originator (merchant or payment processor) of the confirmation

Measures to ensure the **integrity** of the payment details during and after the initiation of a payment should be in place. Transaction integrity ensures that an unauthorized party cannot intercept a message and alter it en route to a recipient.
This can be achieved through readily available encryption mechanisms using, for example, Secure Sockets Layer (SSL) technologies and supporting web browsers. When such technology is implemented there are several ways in which the consumer is made aware of its presence: the use of the *https* protocol in the URL; the image of an unbroken key or a lock at the bottom of the browser; and web site or browser initiated messages on the presence of secure pages.

Electronic payment systems must be prepared for the possibility of accidental data corruption. It must be guaranteed that if a technical defect occurs, the transaction will not be completed from either side (totality). The customers need to know for sure that the agreed payment will reach the intended recipients and that only successful transactions will be charged to their account. In other words, customers typically require assurances that the transaction integrity is maintained, i.e. that the transaction will be carried as intended, that the amount and other data remain unchanged, and that the transaction will be executed only once
The presence and visible nature of this mechanism should influence a consumer's security perceptions.

SSL was used as the sole means of ensuring that sensitive transaction information was encrypted before transmission. We did not find any instances where credit card details were passed through to the merchant or the payment service provider via insecure web forms or e-

mails. However, a small percentage (less than 5%) of sites did not secure the personal data of their customers such as their names, addresses, contact details, etc. during the processing of the order.

However, very few websites explained the SSL mechanism and the role of digital certificates or how to verify if the site was secure (for example, the https protocol, and the browser padlock and key) and to whom the digital certificates were issued.

Some 16% of the sites requested the submission of personal details and contact information via insecure e-mail or web based order forms in order to process an order.

Review pages at a web site typically display a summary of the order and the final cost and usually offer the customer an opportunity to change any of the shipping or payment information before completing the final stage of the ordering process. Providing such an option can also engender in the customer a sense of confidence and control over the entire payment process and a reassurance that they can still verify the integrity and completeness of the order and payment details right until the finalization stage

Although majority of the merchants provided the facility to verify an order before finalization of the actual payment, they only rarely supplied an explanation or reassurance of this step to the customer elsewhere on their site. Also only a handful of sites offered any detailed explanations as to how to go about cancelling or modifying an order after it had been placed and paid for, or whether such an option in fact existed. Less than 1% of the sites explicitly stated whether a payment could be cancelled or how to go about doing so. This can be attributed to the fact that while it may be in the interest of the customer to cancel a payment, it poses problems for the merchant who might be inclined to rule this out as far as possible, in view of high chargeback fees and the fear of bad debts arising from it.

Overall Assessment of Implemented Security Measures

The results are indicative of the external, visible security features of the payment systems as well as those identified and documented by the merchant and/or the third party payment provider. Putting such elements in place can serve to indicate a firm's technical competence and its ability to fulfil its fiduciary obligations to its customers, and in so doing convince them of the web site's security and the commitment on the part of the firm to fulfil its purchase agreement with the customer.

5. Payment Security Information

This section primarily concentrates on the level and quality of information provided to consumers in relation to the technical features of the electronic payment solutions in place. Consumers are reluctant to use Electronic Payment Instruments (EPIs) and Systems (EPSs) because, among other reasons, they are not sufficiently aware of how securely their transactions are carried out through these means of payment (Hegarty et al. 2003). We suggest that by informing and reassuring customers about the security of their payment options merchants will be able to influence their security perceptions, and hence their trust in them. This too is supported by Miyazaki & Fernandez (2000) who argued that security-related statements placed on web sites were likely to increase the chances of consumers purchasing and paying over the Internet. The rationale that supports this proposition has its basis in the concept of *information asymmetry* and the role it plays in decision making.

Information asymmetry is a situation where one of the parties to a transaction does not have access to all of the information they need in order to make a decision (Akerlof 1970). This has been recognized as one of the major problems in electronic markets. According to Mukherjee & Nath (2003) information asymmetry is an important factor affecting customers' trust in online activities. Among the many aspects of information asymmetry is that of the uncertain quality of the product.

Typically with electronic payment services less personal contact is involved in the payment transaction, and consumers have to increasingly depend on accessing and interpreting by themselves information provided at a distance about the use, functionality and security of EPIs. As with any service or good offered over the Internet, a customer' decision to make use of a payment option will be influenced by the quality of the information being made available to him.

The extent of the information asymmetry should therefore influence consumers' perceptions about the security and technical competence of the EPI.

In this fact-finding part of the study we conducted an assessment of the information supplied by our preliminary sample of websites to consumers in relation to the security of EPIs. This aspect of the investigation is based on the three criteria of security information (availability, accessibility and comprehensibility) as was used in a similar study conducted on European websites (Hegarty et al. 2003), and is supported by Urban et al. (2000) who suggested that quantity, quality and timeliness of information on the website can improve online trust.

Availability is related to the presence of any information at all that supports the use of a given EPI and the carrying-out of an online transaction in general. The consumer of any product or service needs to learn what the offered product or service is and how it actually works.

Therefore, the starting point of our website assessment was to examine whether or not the websites surveyed provided any general information on the meaning, technical description and functionality of EPIs, namely on

- The technical features of an EPI, usability, purpose and added-value of their implementation;
- Instructions about how to use an EPI;
- Instructions about how to prevent physical, functional or other defaults of an EPI and/or flaws of the e-payment system in question.

On average, only 9% of the websites visited contained detailed explanations about how the website secured payment transactions, the functionality of the EPIs being offered and what the customer could do to minimise the risks associated with using the payment instrument.

Accessibility relates to the ease with which customers are able to find information concerning the security aspects of electronic payment methods and products in use. The information provided to consumers should be made available in such a way that it is not difficult for an average consumer to find. Insufficient information about the security of EPIs can be a barrier to the wider use thereof. In the light of this finding, it seems that informative elements, which, in the view of the average consumer, can significantly influence the final decision to use or not to use an e-payment system, should be within easy reach to him/her. Accordingly, consumers should not need to make any special or extraordinary effort to find the information.

The findings of our survey regarding the level of accessibility of the security-related information on the websites scanned are as follows:

- *On average, explanations on the security features were easy to find on 60% of the websites visited.*
- *Where security-related information was easy to find, it was made available either in the general frame or as a link on each web page (42%)*
- *In many cases (25%), the security-related information was part of the Frequently Asked Questions (FAQ), Help, or Privacy sections of the website, often only as part of other general issues relating to the use of e-commerce functions.*

Comprehensibility concerns the appearance and form in which security-related information is brought to the knowledge of consumers in such a way as to raise their confidence in the quality and efficiency of the technical means implemented in or supporting electronic payments. Making security-related information comprehensible means that, it should appear in a clear and explicit manner, drafted in a wording that attracts consumers' attention and makes it understandable to an average consumer.

Accordingly, the explanations should be provided in plain language largely free of technical jargon. Technical information shall also be provided in a way that reflects layman thinking without supposing or requiring specific IT knowledge (e.g., in relation to encryption etc.). Complicated or too technical a language can also have the effect of making the information practically 'inaccessible' to the average consumer.

In this respect, our survey illustrated the following:

- *Where information is available on the website, it is drafted in an easily understandable way in 56% of the visited websites*
- *In 8% of cases the explanations were simplistic, or too general, or too brief to offer sufficient reassurances to potential purchasers.*

Overall Assessment of Security Information

As a result of the absence of personal contact involved in the performance of electronic transactions, customers find themselves in the position of having to seek out by themselves the information that companies make available on their website when clarifying the various aspects of the payment process. At every step of the transaction process, customers must be able to find answers to their questions regarding security, privacy, as well as terms and conditions. Merchants must demonstrate that they understand and care for their customer's trust related concerns. If the information is not sufficiently clear, consumers are likely to interpret it on the basis of their own knowledge, experiences and understanding of the process, which, in the case of choice of payment instruments is likely to be influenced by second-hand anecdotal evidence and sensational media reporting.

6. Future Work

There is a widely held perception that the general public lacks confidence in the security aspects of conducting transactions electronically, particularly those that involve a payment of some kind using Electronic Payment Instruments. This general perception, often perpetuated in media sensationalism, and sometimes merely anecdotal, needs to be clarified and measured:

- To what extent this perception actually exists in the minds of the citizens, or is merely media "hype"?
- What are the real concerns of citizens?

The next phase of the study will comprise a quantitative study of the perceptions of consumers as regards their security concerns particularly in the light of the our assessment of websites and the security information and measures we know to be (or not to be) in place.

7. Conclusion

Studies on trust in e-commerce largely focus on the issues related to overall trust in the merchant or the transmission medium (the Internet infrastructure) in a generic fashion. Several models on trust depict the causal relationships between the antecedents of trust and trust in the system, the business, the individual or the medium. Where the security factor comes under scrutiny, it is typically dealt with generally and in terms of the overall security of the website. In the light of the ever increasing online and offline payment options available to the consumer, this study extends the notion of technology trust to electronic payment instruments where security and trust mechanisms play an especially important role in their acceptance. Perceptions of trust depend on perceptions of technical competence. How potential customers perceive the technical competence of an EPI plays an important part on their likelihood of using it. This study has made the argument that this perception can be influenced by the level of security realized at the website and appropriate assurances given by the merchant.

8. References

Akerlof, G. "The market for lemons: quality uncertainty and the market mechanism," *Quarterly Journal of Economics* (84:3) 1970, p 488–500.

Benassi, P. "TRUSTe: An online privacy seal program," *Communications of the ACM* (42:2) 1999, pp 56-57.

Bhimani, A. "Securing the commercial Internet," *Communications of the ACM* (39:6) 1996, pp 29-35.

Cassel, J., and Bickmore, T. "External manifestations of trustworthiness of the interface," *Communications of the ACM* (43:12) 2000, p 50.

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

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

Dayal, S., Landesbeg, H., and Zeisser, M. "How to build trust online," *Marketing Management* (8:3) 1999, pp 64-69.

Furnell, S.M., and Karweni, T. "Security implications of electronic commerce: a survey of consumers and business," *Electronic Networking Applications and Policy* (9:5) 1999, pp 372-382.

GPayments "Authentication: the missing element in online payment security," *Date Accessed*: 12/04/2002, http://www.gpayments.com.

Grabner-Kraeuter, S. "The Role of Consumers' Trust in Online-Shopping," *Journal of Business Ethics* (39:1/2) 2002, pp 43-50.

Hegarty, T., Verheul, E., Steuperaert, D., and Skouma, G. "Study on the Security of Payment Products and Systems in the 15 Member States: Final Report," PricewaterhouseCoopers.

Hoffman, D.L., Novak, T.P., and Peralta, M.A. "Building consumer trust online," *Communications of the ACM* (42:4) 1999, pp 80-85.

Jewson, R. "e-Payments: Credit cards on the Internet," *Date Accessed*: 20/04/2003, www.aconite.net.

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

McKnight, D.H., and Chervany, N.L. "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology," *International Journal of Electronic Commerce* (6:2) 2002, pp 35-59.

Miyazaki, A.D., and Fernandez, A. "Internet privacy and security: An examination of online retailer disclosures," *Journal of Public Policy and Marketing* (19:1) 2000, pp 54-61.

Mukherjee, A., and Nath, P. "A model of trust in online relationship banking," *The International Journal of Bank Marketing* (21:1) 2003.

Ratnasingam, P., and Pavlou, P.A. "Technology Trust in Internet-Based Interorganizational Electronic Commerce," *Journal of Electronic Commerce in Organizations* (1:1) 2003, pp 17-41.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., and Camerer, C. "Not so different after all: A cross-discipline view of trust," *Academy of Management Review* (23:4) 1998, pp 393-404.

Shaw, M.J. "Electronic commerce: Review of critical research issues," *Information Systems Frontiers* (1:1) 1999, pp 95-106.

Shneiderman, B. "Designing trust into online experiences," *Communications of the ACM* (12:43) 2000, pp 57-59.

Suh, B., and Han, I. "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of Electronic Commerce* (7:3), Spring 2003 2003, pp 135-161.

Urban, G.L., Sultan, F., and William, Q. "Making trust the centre of your Internet strategy," *Sloan Management Review* (1), Fall 2000, pp 39-48.

Van Slyke, C., and Belanger, F. *e-Business Technologies* John Wiley & Sons, Inc, USA, 2003.

Yousafzai, S.Y., Pallister, J.G., and Foxall, G.R. "A proposed model of e-trust for electronic banking," *Technovation* (23) 2003, pp 847-860.