THE IMPORTANCE OF RISK REDUCTION ON MERCHANT UPTAKE OF REAL-TIME CREDIT CARD PAYMENT PROCESSING SYSTEMS

Mustafa A. Ally
Department of Information Systems
Faculty of Business
University of Southern Queensland
West Street
Toowoomba 4350
Queensland
Australia

Tel: +61 7 4631 1232
Mobile: 04 02 026 786
Fax: +61 7 4631 5594

e-mail: Mustafa.Ally@usq.edu.au

ABSTRACT

Credit cards are the primary means of payment of goods and services over the Internet. Many characteristics of credit cards leave merchants vulnerable to fraud, inconvenience and loss of potential customers. Despite the fact that the security issues of confidentiality and integrity are largely addressed in real-time credit card payment processing systems (RTCCPS), the one missing link from a merchant's perspective has been customer authentication. The lack of effective payer authentication mechanisms has seen a high level of reported fraud resulting in revenue loss and costs to the merchant that are associated with chargebacks, merchant liability, fraud screening and dispute resolution. This research-in-progress paper proposes a model that has the potential to predict the likelihood of the adoption of a RTCCPS when these risks are mitigated by a reduction of fraud levels and monetary losses through customer authentication and merchant liability shift.

1. INTRODUCTION

The Internet has opened the possibility of purchasing goods and services online. There has been an exponential growth in e-Commerce that is expected to continue for the foreseeable future. In e-Commerce the exchange of value for goods purchased over the Internet involves the exchange of data. This virtual exchange poses a set of risks for both merchants and consumers that could hinder the further development of e-Commerce. These risks originate from the insecure nature of open networks with evidence that the number of security breaches is on the increase (Computer Security Institute 2001). Examples of the kinds of security breaches included communications' interception in order to copy or modify data; unauthorized computer access with malicious intent; execution of malicious code and malicious misrepresentation. As a consequence, consumers and merchants both face a number of risks when transacting through these unsecured open networks.

1.1 Internet Payment Risks

In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with no authentication (GPayments 2001). "This account information provides key elements needed to create counterfeit cards and/or fraudulent transactions. While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high-volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers from a data stream), and the potential for "mischievous fraud" that appears to be characteristic of some hackers" (SETCo 1997).

From a payment perspective the risks to consumers continue to receive wide coverage in the media. Consumers face the risk of transacting with fake or fraudulent merchants who bill transactions but never deliver or have their credit card or account data used fraudulently. Merchants, on the other hand, face the risk of transacting with consumers who may be using stolen or fake payment data. This ultimately leads to repudiation by the rightful owner and the merchant is usually held liable for the value of the transaction (legitimate repudiation risk). Merchants also confront the risk of their transactions being repudiated by customers making purchases and later denying responsibility (fraudulent repudiation risk).

1.2 Risk Reduction Measures

In the physical marketplace, the transacting partners have relied on a number of mechanisms to mitigate these risks: the physical presence of the store, the payer's presentation of a payment card, the use of a secret PIN code, the visual aspect of the payment card (brand mark, signature panel), and the use of a hand-written signature to conclude a payment.

To manage these risks more effectively in an open network environment where e-Commerce is conducted requires the consideration of new sets of rules and security measures. This has led to the development of technologies that support data confidentiality and integrity, consumer and merchant authentication and non-repudiation for each individual transaction, and payment guarantees in the case of fraud (Centeno 2001). The "hard" or technology-based payment solutions range from the cheap and easy SSL, address and CVV/CVC2 validation, the use of passwords and user identifications, virtual and pseudo card numbers, SET, 3D-models and EMV smart cards. However, except for the broad adoption of SSL for data confidentiality and integrity, the diversity and lack of interoperability among solutions, the lack of incentives for merchants and consumers, and the potential impact on the cardholders have served to stifle widespread diffusion of these solutions (Centeno 2002).

1.3 Fraud on the Internet

Whilst the complete automation of the payment process on the merchant's side has opened up new commerce opportunities, it has also opened up new scope for payment fraud (Jewson 2001). Global statistics point to credit cards as the most important Internet payment instrument (Bohle & Krueger 2001), being used in 95 per cent of on-line transactions (Visa 2001). But managing online credit card fraud continues to be a major challenge for merchants of all sizes. According to (Verisign 2003) more than $700 million in online sales were lost to fraud in 2001, representing 1.14% of total annual online sales of $61.8 billion, according to GarnerG2. Online fraud losses for 2001 were 19 times as high, dollar for dollar, as fraud losses resulting from offline sales. According to the Garner Group, fraud on the Internet is taking its toll on merchants with 160 surveyed companies reporting 12 times more fraud in Internet transactions than in traditional retail.

1.4 Impact of Fraud on Merchants

A survey carried out in the United Kingdom by the Consortium of British Industry (CBI) in 2001 reported that merchants were fearful of selling on-line, with two thirds of the firms reporting having suffered a serious cyber crime attack (Industry 2001). One of the main issues facing many online merchants appears to be finality or non-repudiation of payments (Pichler 2001). Currently, most merchants bear 100% of the fraud risk for online purchases – even if the transaction has been authorized by the bank. Fraud-related chargebacks result from identity theft, stolen card use or consumers fraudulently denying transactions. The card schemes have required the merchant to bear the full liability of a repudiated transaction. Other costs and fees are also incurred when charges are contested. In addition to the cost of processing chargebacks, (CyberSource 2002b) identified the following additional negative impacts of online fraud: loss of staff time, loss of revenue, loss of customer goodwill, loss of goods, increase in staff resources, chargeback fines, revenue reconciliation inefficiency, bank fees, discount fees and shipping and handling costs. To reduce fraud levels merchants have had to bear the additional burden of having to invest in manual and automated fraud detection systems. In many cases these costs alone have made the adoption of online payment systems by smaller companies untenable.

1.5 Authentication

The problem of repudiation generally arises from the card-not-present nature of the transaction where the merchant cannot physically see the credit card of the cardholder. The vast majority of these transactions are not authenticated thereby increasing the incidence of fraud (GPayments 2001). The merchant need for authentication derives from the need for a payment guarantee. Being able to prove the authenticity of the payment, the payer and the payee are 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 is defined by the business risks associated with this instrument (Centeno 2001).

1.6 The New Payment Models

A key benefit of authentication programs is protection from fraud-related chargebacks that often result from identity theft or stolen card use. The introduction of new payment rules and cardholder authentication services from Visa's Verified by Visa (VbV) and MasterCard's SecureCode guarantee payment to the merchant. Both schemes offer merchants protection from chargebacks where the cardholder denies making the recorded purchase.

This research-in-progress paper proposes a theoretical model to investigate the impact this liability shift (from merchant to issuing bank) and the new authentication measures are likely to have on the more ready adoption of online credit card payment processing systems by merchants who predominantly use traditional "offline" payment systems to finalize their transactions (Ally & Toleman 2002).

The research report is divided into several stages. The first stage examines the various Internet credit card payment initiatives to date and how they address the critical requirements of payment systems in general. The second step identifies and justifies a preliminary model to explain and predict the likelihood of adopting the new payment initiatives. The third stage describes the data gathering process. The report concludes with a discussion on the expected outcomes of this research.

2. ANALYSIS OF CREDIT CARD PAYMENT MODELS

This section outlines the protocols used by credit card schemes in which a payer and payee establish trust in each other and exchange value electronically across an open, insecure channel that is the Internet.

Most web sites accepting credit cards as a means of payment use SSL to provide confidentiality and integrity of the exchanged data between the consumer browser and the merchant server. However, while SSL digital certificates could potentially provide consumer authentication as well, this feature is not widely used by merchant servers,

Instead, merchants, who are liable for fraud in such types of transactions, have to build fraud risk management tools such as e-mail confirmation, consumer history database, phone calls to first-time customers, advanced payments, address validation, etc.(Centeno 2001)

As a means of providing a more secure environment for all parties concerned in a credit card transaction, Visa and MasterCard developed the SET (Secure Electronic Transaction) payment protocol in 1996. With the use of public key infrastructure (PKI), digital certificates and signatures, a trust chain was created at each step of the transaction processing, providing consumer and merchant authentication, data confidentiality and integrity and non-repudiation capability. Although SET provided all the tools for secure electronic transactions, the standard, per se, did not win favour in the market place and failed to win critical mass. The major implementation barriers identified in (Ally 2001) included:

- Lack of incentives for consumer adoption
- Additional complexity of use and understanding on the part of the consumer
- Complexity and costs of the overall implementation for the different parties
- Technical interoperability among different vendor solutions and lack of software tools

In order to reduce the barriers to implementing the SET protocol and to resolve the security weaknesses of SSL, Visa and MasterCard proposed a number of different solutions, chief of which was Visa's launch of the 3D-model in June 2000 in its variants: 3D-SET for Europe and Latin America and 3D-SSL for USA.

The principle of the 3D-Model is that the issuer bank authenticates the cardholder, the acquiring bank authenticates the merchant, and the banks authenticate each other, leaving the issuers and the acquirers with the freedom to choose the cardholder and the merchant authentication methods.

In the 3D-SET model, cardholder and merchant certificates continued to be used but were held at server wallets and accessed through bank defined authentication mechanisms such as PIN or password. This server-based SET model reduced the technology needed at the merchant and customer ends by only requiring "thin" modules for merchants and "slim" digital wallets for consumers. This model eliminated the need for cardholder/merchant mutual authentication and offered alternative – and simpler – authentication mechanisms as business relationships exist between the banks and cardholders and merchants, respectively.

However, neither SET nor 3D-SET gained widespread adoption and the credit card companies superceded it with authentication processes (GPayments 2001).

Current Developments

The challenge for credit card companies and card issuing banks is to reduce fraud and disputed online payments and its related costs while increasing consumer confidence in online shopping. To this end, both Visa and MasterCard announced two new competing cardholder authentication services, namely, "Verified by Visa" (September 2001) and "SecureCode" (May 2001), respectively. Merchants implementing these authentication programs will benefit from a liability shift to the issuing banks in the event of fraudulent and disputed transactions.

Both use SSL and provide additional mechanisms to authenticate the cardholder and the merchant. Verified by Visa (VbV) employs 3D-Secure, an Internet commerce payment authentication mechanism developed by Visa. First, a cardholder enrolls in the scheme at the issuing bank's site and registers a password. During a checkout process this password is requested off the cardholder to verify his/her identity. The 3D-Secure system requires that the card issuing bank verifies the online user as the legitimate cardholder. Once completed, the merchant can continue to process the transaction with standard payment processing methods.
The MasterCard SPA (Secure Payment Application) model is also focused around cardholder authentication, but requires the use of plug-in software or an electronic wallet by cardholders. Customers have to initially register for the service with their issuing bank. They then set a password and download a Java applet. At the checkout, they enter the password prior to finalizing their payment. The issuer authenticates the cardholder and generates an authentication value which is returned to the applet. The applet incorporates this value into a hidden part of the payment details form which is sent to the merchant. Finally, this value is then used when the merchant processes the purchase transaction (Jewson 2001). In this way consumer authentication, payment data and purchase order details are uniquely bound for each transaction, equivalent to a cardholder's signature, reducing repudiation risk.

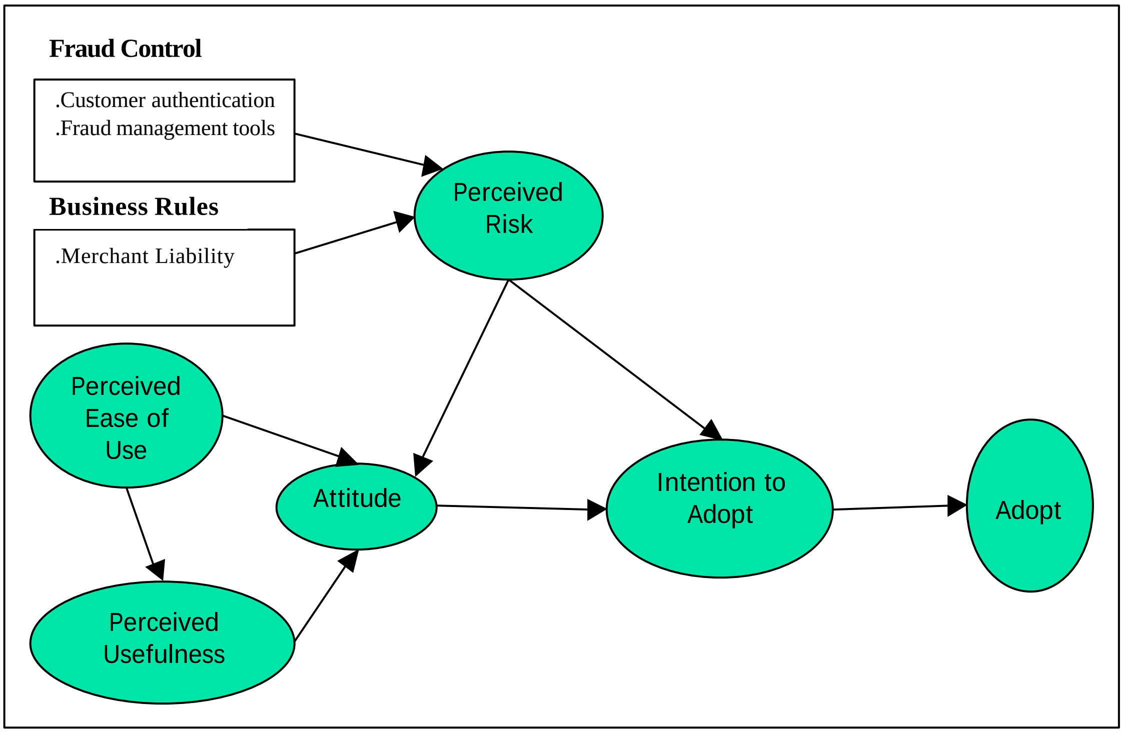
Both these models deliver a solution to the existing problem in online credit card transactions – a lack of authentication. The question arises as to whether this missing element in online payment security is sufficient to gain the expected traction in the marketplace.

3. A PROPOSED RESEARCH MODEL AND HYPOTHESES

In this research, a review of IS adoption/diffusion and payment systems literature was conducted with the purpose of identifying the appropriate constructs to explain the adoption of RTCCPS by online merchants.
As with most information systems, Internet technology adoption and use could be predicted by the Technology Acceptance Model (TAM) (Davis 1989). While TAM has initially focused on system usage in the workplace, recent research has successfully employed TAM to understand web technology usage as well (Teo, Lim & Lai 1999).

This research incorporates the construct of Perceived Risk with TAM's major constructs (ease of use and usefulness) to predict RTCCPS adoption. The relationships of these factors with the process of RTCCPS adoption intention and actual adoption are shown in Figure 1. As depicted in the model, the intention to adopt a RTCCPS is affected by the perceived risk inherent in the RTCCPS and the merchant's attitude towards the RTCCPS itself. In the context of this study two additional factors impacting on the merchant's perception of the risks involved are identified as Fraud Control and Business Rules.

Figure 1 A Conceptual Model of RTCCPS Adoption



3.1 Fraud Control

The lack of consumer authentication combined with merchants' liability for fraudulent credit card transactions motivated the development of merchant-based authentication solutions (Centeno 2002). However, there has been no single, complete solution to the problem of managing and reducing the costs of online fraud. To reduce the incidence of fraud and chargebacks merchants have had to use a variety of methods to manage the problem in a cost effective way (CyberSource 2002b). Example of such measures include commercial fraud screens and risk scoring services, address verification service (AVS), card verification number (CVN) etc. Merchants face several challenges in managing online fraud, including keeping fraud tools and strategies tuned and up-to-date on a regular basis, as well as intelligently applying the variety of tools required to reduce fraud. From a merchant‘s perspective, an important strategy is through the provision of payer authentication mechanisms. Without effective authentication merchants are exposed to loss of revenue, higher transaction and service costs, and loss of consumer confidence and reputation (GPayments 2002). Statistics from the credit card organizations indicate that at least 75% of all Internet chargebacks could be prevented by cardholder authentication (Riehm & Weber 2001). On the surface, authentication programs appear to solve all fraud problems, requiring only that merchants check cardholder enrollment to gain chargeback protection. However, the use of complementary fraud protection measures are still beneficial to help maximize overall revenue and profits (CyberSource 2002a).

Proposition 1
The use of fraud control mechanisms, namely payer authentication and fraud management tools, with RTCCPSs will reduce the level of risk as perceived by merchants.

3.2 Business Rules

In order to protect consumers, as well as their own interests and reputations, acquiring banks place strict rules and conditions for merchants to conform to before granting merchant accounts. Of particular importance to merchants is the extent of their liability in the event of repudiated transactions. Concerns over the reported degree of online fraud coupled with the card organizations' ruling that merchants were required to bear the full costs of chargebacks have, to date, not made the implementation of RTCCPS a viable proposition in the eyes of many merchants, particularly ones who are unable to afford the additional infrastructural costs to manage the fraud and whose profit margins cannot support the potential losses (real or perceived) resulting therein. Easing this requirement of liability could have a significant influence on reducing the level of risk a merchant is likely to contend with.

Proposition 2
Limitation of merchant liability from use of RTCCPSs will reduce the level of perceived risk.

3.3 Perceived Risk

The use of Perceived Risk as a construct reflects the notion of uncertainty inherent in online transaction processing, a factor not considered critical in traditional technology adoption. For example, the risk of fraud and consequent monetary loss to the merchant in an open technological infrastructure add a new dimension to the process of RTCCPS adoption.

The distant and impersonal nature of the online environment and the implicit uncertainty of using a global open infrastructure for transactions have rendered risk as an inevitable element of e-Commerce (Pavlou 2001). Risk is defined as a perception of the uncertainty and adverse consequences of engaging in an activity. One form of uncertainty naturally present in online transactions is that of behavioural uncertainty (Bensaou & Venkataman 1996). Behavioural uncertainty arises because customers have the chance to behave in an opportunistic manner by taking advantage of the distant and impersonal nature of e-Commerce. Behavioural uncertainty primarily creates economic risk because of the possibility of monetary losses.

An investigation into online payment fraud data has found a lack of coherent, accurate and publicly available sources (Centeno 2002). The lack of reliable fraud statistics and chargeback numbers is due in part to the reluctance or inability of merchants to readily divulge such information making the capturing of the risk construct as an objective reality difficult. It is impossible to know the real fraud rates as detection is less than perfect and there is no central and unbiased authority (Shankar & Walker 2001). Much of the perceptions about the extent and level of the potential loss to merchants arises from anecdotal evidence and sensational newspaper reporting. Research from Jupiter Media Metrix showed that fears of online fraud are more common than fraud itself (Verisign 2003). The related literature has also predominantly addressed the notion of perceived risk which is defined here as the merchant's subjective expectation of suffering a loss through fraud and chargeback liability arising as a consequence.

The focus in the ongoing evolution of payment models by card organizations (detailed in Section 2 above) highlights the importance placed in alleviating the risk to merchants arising out of customer fraud and merchant liability, pointing to risk reduction as a critical factor in determining the likelihood of merchants readily adopting RTCCPS

Proposition 3
Reduced perceived risks associated with RTCCPS will increase a merchant's willingness to adopt a RTCCPS.

3.4 Usefulness and Perceived Ease of Use

The Technology Acceptance Model was developed to predict and explain the voluntary use of any type of end user computing system (Davis 1986). TAM purports perceived ease of use and perceived usefulness as the two major factors influencing attitudes toward system use.

Perceived usefulness is defined here as the degree to which merchants believe that a RTCCPS would facilitate the payment process in their online business. Instant authorization, fast payments and minimal manual intervention are just some of the benefits that could make a RTCCPS a viable proposition for an e-Commerce business.

Perceived ease of use is defined here as the degree to which a merchant believes that installing and managing a RTCCPS would be free of effort. Payment standards that have minimal hardware and software installation requirements and costs have a greater chance of being adopted by merchants (as borne out by the SET experience) (Egger 2001). For example, 3D-Secure has minimized the requirements for cardholders mandating that they only need a browser to participate. Also, 3D-Secure only authenticates the customer to the merchant and does not mandate merchant authentication to the customer, making it simpler than SET. The major problem of requiring certificates for cardholders, which was, to a large extent, the demise of SET, has been removed. The use of username and password is a relatively simple mechanism to implement and is expected to become the most common form of payer authentication for credit card transactions (GPayments 2001)

Drawing from TAM, perceived usefulness and perceived ease of performing the behaviour would directly influence behavioural intention and actual behaviour. Applying this to the study, an RTCCPS that is perceived to facilitate the payment process and be of benefit while being easy to operate is likely to be accepted by merchants

Proposition 4
Merchant intention to adopt a RTCCPS is positively related to perceived ease of use.

Proposition 5
Merchant intention to adopt a RTCCPS is positively related to perceived usefulness.

Consequently, a set of testable hypotheses that inter-relate intention to adopt RTCCPS with Perceived Usefulness, Perceived Ease of Use and Perceived Risk and its antecedents, Fraud Control and Business Rules, is proposed.

4. RESEARCH METHOD

4.1 Qualitative Data

Using current literature and interviews with managers of three card payment providers and three merchants, a preliminary set of constructs was developed. The interviews were conducted over telephone and e-mail. A series of single e-mail questions was posed to the interviewees using a pre-determined interview guideline. The follow-up questions were changed when other interesting issues surfaced. The types of questions posed included ones that related to the factors that were considered preventing greater merchant uptake and the future of the new models. Other sources of evidence were also considered and included published sources, e-mails, Internet-based discussion groups, Special Interest Groups, and informal discussions with other experts in the field.

4.2 Proposed Survey Study

Using the insights gained from the qualitative data collection phase and literature on innovation diffusion and intention-based behavioral models, a preliminary survey instrument has been developed. The preliminary research instrument to measure the constructs of interest was developed by converting the definitions of the constructs into a questionnaire format. All the variables are measured on a seven-point Likert scale. The survey will be pilot tested on the three merchants who are currently not offering online payment to their customers as well as the three managers interviewed previously. Based on their feedback and responses, some of the questions may have to be reworded and others possibly eliminated. The research instrument will be evaluated for reliability (using Cronbach's alpha), convergent validity and discriminant validity (using factor analysis).

Survey data will be collected from Australian e-Commerce companies identified in a previous study as ones currently not offering any online payment authorization systems. This data will be used to test the proposed model and the hypotheses developed from it using regression analysis.

5. LIMITATIONS

At this stage of the research the main limitation identified is in respect of the conceptual model. The main dependent variable – intention to adopt, is likely to be influenced by several variables other than those explicitly hypothesized for the purposes of this research.

The proposed model is justified in the context of the direct influence of risk reduction strategies on merchant uptake from the perspective of the merchant per se. It assumes that the existing credit card user base will prevail. However, the new standards could also have a bearing on customer acceptance and usage, and on merchant adoption rates as a consequence. Customers may be positively influenced by the provision of an additional layer of protection (fraud control) while, on the other hand, the enrolment and authentication processes might be conceived as an extra burden impacting on ease of use (thereby reducing the customer base). The resultant customer acceptance levels could be mediated by the risk construct and therefore have an indirect influence on merchant adoption rates. Other factors that could also have a bearing include merchant readiness, the business model, marketing strategies of credit card organizations, and transactional and related costs.

6. EXPECTED CONTRIBUTIONS

The efforts being put into developing online payment standards by the credit card organizations is an indicator of the need for new and improved payment methods to combat credit card fraud. Which methods will succeed is uncertain. Backward compatibility, guaranteed payment and ease of use for consumers are important to merchants, and any new authentication methods must not be inconvenient to merchants and customers. This study hopes to determine the efficacy of the new customer authenticated models proposed by the leading credit card companies with a view to gaining wider merchant acceptance through offering further reduction in risk. It is expected to show that risk reduction mechanisms have significant impact on the adoption of RTCCPS.

The eventual research results could have important implications for the various stakeholders in the online payment business. A negative outcome showing that merchant uptake will not be significantly improved by the introduction of the new scheme could result in banks having to re-assess their long term investment in the technology. For the credit card organizations it could mean a re-evaluation of their payment schemes and marketing strategies. Merchants, on the other hand, will continue to resist and delay the move to online payment processing even longer. However, a positive outcome indicating the potential for widespread diffusion of the scheme, could encourage investment in the technology both by merchants as well as the banks, the eventual consequence of this being a better return on investment for the key stakeholders. In the case of researchers, the results have the potential to contribute to understanding and explaining the problems surrounding the adoption of payment systems in general and possibly extend the current theories and models of adoption in the context of payment systems.

7. REFERENCES

Ally, M. (2001). *The Integration of SET in Australian based Internet Payment System Products: A Systems Developers Perspective*, paper presented to 14th Bled Electronic Commerce Conference, Bled, Slovenia.

Ally, M. and Toleman, M. (2002). *Meeting Consumer Trust Concerns at the Checkouts of Australian Online Retailers*, paper presented to ACIS 2002, Melbourne.

Bensaou, M. and Venkataman, N. (1996). *Inter-organizational relationships and information technology: A conceptual synthesis and a research framework*., European Journal of Infromation Systems, vol. 5, pp. 84-91.

Bohle, K. and Krueger, M. (2001). *Payment Culture Matters - A Comparative EU-US Perspective on Internet Payments, ePSO project-Background Paper No. 8*, ePSO Newsletter, vol. 6.

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

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

Computer Security Institute, US. (2001). *CSI/FBI Computer Crime and Security Survey*, Computer Security Issues and Trends, vol. 7, no. 1.

CyberSource (2002a). *New Payment Rules Change Online Retail 2003*, viewed 14/04/2003 2003, <www.cybersource.com>.

------- (2002b). *Online Fraud Report: 2002 Results*, Cybersource, <www.cybersource.com>.

Davis, F.D. (1986). *A Technology Acceptance Model for testing new end-user information systems: Theory and Results*, MIT Sloan School of Management, Cambridge, MA.

------- (1989). *Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology*, MIS Quarterly, vol. 13, no. 3, pp. 319-40.

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

GPayments (2001). *Authentication: the missing element in online payment security*, viewed 12/04/2002 <www.gpayments.com>.

------- (2002). *Verified by Visa Overview*, <www.gpayments.com.au>.

Industry, C.o.B. (2001). *The Cybercrime Survey 2001*, viewed April 2002, <www.cbi.org.uk>.

Jewson, R. (2001). *e-Payments: Credit cards on the Internet*, viewed 20/04/2003 2003, <www.aconite.net>.

Pavlou, P.A. (2001). *Consumer Intentions to Adopt Electronic Commerce - Incorporating Trust and Risk in the Technology Acceptance Model*, Marshall School of Business, University of Southern California, LA.

Pichler, R. (2001). Finality of Credit Card Payments and Consumer Confidence - Different Approaches in the United States and in Europe, *Electronic Payment Systems Observatory - Newsletter*, February 2001, pp. 4-6.

Riehm, U. and Weber, A. (2001). *Massive reduction of Chargebacks*, ePSO Newsletter, no. 10, pp. 8-11.

SETCo (1997). *SET Secure Electronic Transaction Specification Book 1: Business Description Version 1.0*, <www.setco.org>.

Shankar, U. and Walker, M. (2001). *A Survey of Security in Online Credit Card Payments*, viewed 24/04/2003 2003, <http://www.cs.berkeley.edu/~ushankar/research/ecommerce/credit.htm>.

Teo, S.H.T., Lim, V.K.G. and Lai, R.Y.C. (1999). *Intrinsic and extrinsic motivation in Internet usage*, Omega International Journal of Mangement Studies, vol. 27, pp. 25-37.

Verisign (2003). *Guide to Securing Your Web Site For Business*, <www.verisign.com>.

Visa (2001). *Verified by Visa Fact Sheet*, viewed April 2003 <http://www.visa-asia.com/newsroom/verified/au/dloads/Verified_by_Visa_FactSheet.pdf>.