A Critical Analysis of Buyer Authenticated Credit Card Payment Programs: The Online Merchant's Perspective

by
Mustafa A. Ally
and
Mark Toleman

Department of Information Systems
Faculty of Business
University of Southern Queensland
Toowoomba, Queensland 4350
Australia
Email: Mustafa.Ally@usq.edu.au and Mark.Toleman@usq.edu.au

Abstract

Recently introduced by the major credit card associations as replacements for the decommissioned SET and 3DSET protocols, the new payment models, 3DSecure and UCAF/SPA, have been designed to provide online merchants with a solution to an existing problem in online credit card transactions – the lack of an effective and efficient means of authenticating cardholders. The expected benefits arising from this added level of security from the merchant's perspective are increased consumer confidence, significant reduction in the levels of fraud and chargebacks and "liability shift". Using data gleaned from preliminary interviews, discussion forums and promotional material, we present a critical analysis of the potential barriers and facilitators that will impact on the widespread traction of these programs in the marketplace in the coming years.

Keywords

Payment systems, credit card fraud, buyer authentication models

Introduction

A secure, efficient payment system is considered to be one of the key drivers of e-Commerce. Credit cards are the primary means of payment of goods and services over the Internet but many characteristics of credit cards leave merchants vulnerable to fraud, inconvenience and loss of potential customers. Over the past decades card organizations have largely addressed the security issues of confidentiality and integrity in real-time credit card payment processing systems, but, from the merchant's perspective, the lack of customer authentication has been the one elusive link in the chain. 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. The need for a more secure solution is increasing in the light of the rise in online fraud. "Over half of online sellers avoid multinational sales, mainly due to fear of fraud in cross-border eCommerce, according to Gartner research," said Avivah Litan, Vice President and research director at Gartner Inc. "Further, over 10% of retailers who once engaged in cross -border online sales stopped last year, mainly because of high fraud losses." (CyberSource Corporation, 2003). To further exacerbate the situation, fraud screening tools and strategies used to combat online fraud have shown to be less than completely effective with studies showing that merchants are also rejecting a significant number of valid orders due to suspicion of fraud (CyberSource Corporation, 2004).

This study attempts to discuss various attributes and potential influences within the context of the recent initiatives by the credit card organizations (Visa and MasterCard) to introduce the 3DSecure ("Verified by Visa") and UCAF/SPA ("SecureCode") buyer authentication programs respectively. With the failure of earlier versions of buyer authenticated credit card payment programs (BACCPPs), a study of these new initiatives provides fertile ground for understanding the issues likely to influence their successful adoption by merchants, customers and financial institutions.

Critical Analysis of BACCPPs

Using factors of influence identified in established theories of adoption and diffusion we discuss the attempts by the major credit card organizations to address the requirements of merchants for a secure, economically efficient online credit card payment system through their BACCPPs.

Relative advantage

Research has shown that the relative advantage of an innovation is one of the best predictors of the extent of adoption. It refers to the extent to which the potential adopter perceives an innovation is superior to alternative products, services or concepts (Rogers, 1995). Especially for organizations, the differential advantage of using an innovation over alternatives is important as the productivity of its business is at stake.

Authentication: the missing link to secure payments?

A fundamental problem associated with the processing of online credit card transactions has been that of authentication, that is, the ability to verify that the purchaser is actually the cardholder. The card-not-present nature of these transactions leaves the merchant vulnerable to fraud, higher transaction costs and loss of revenue, cardholder repudiation and costly chargebacks (GPayments, 2001). Also, without effective authentication there is erosion of consumer confidence and trust in the merchant and higher cost of services and chargebacks for banks, ultimately stifling the growth of e-commerce and causing damage to the image of the credit card as an online payment instrument.

Authentication is also a significant industry challenge because it must satisfy the diverse and often contradictory needs of all the stakeholders, including consumers, merchants, and the financial institutions (issuers, acquirers). There are two primary needs of online merchants who accept payments, namely, protection from chargebacks resulting from fraudulent transactions and authentication solutions that identify the customer but at the same time minimize the interruption of the customer's "shopping experience" (Sienkiewicz & Bochicchio, 2002). 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 electronic payments (Jewson, 2001).

Balancing the online consumer experience with stronger authentication methods has traditionally been difficult (VeriSign, 2003a). Methods developed by card organizations in the past have met with both consumer and merchant resistance (SET, 3D-SET). Historical authentication requirements have been cumbersome, time consuming and ineffective. Shopping and paying online is all about customer convenience and making it easier for people to do business with merchants. When additional steps are involved to complete the purchase, customers usually abandon the transaction.

Most merchants 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's server. However, while SSL digital certificates could potentially provide consumer authentication as well, this feature is not widely used by merchant servers.

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 gain critical mass. The SET model failed to secure market acceptance because of perceived resistance by the public to buying digital certificates, "disproportionate" costs and the fact that the system could only be operated from a dedicated computer (where the digital certificate is installed) rather than from another computer.

The BACCPPs provide for cardholder authentication at the point of sale, and a key benefit suggested of the BACCPP is that the authentication process itself has been made more streamlined and customer friendly than its predecessors. These solutions expect no software to be loaded onto the cardholder's PC but, instead, require the cardholder to register a "password" or some other authentication mechanism (such as a smart card) with their issuing bank to enrol in the scheme (see figure 2). At the point when the cardholder hits the "buy" button on a merchant site, a plug-in is activated (on the merchant site), which queries a directory server to determine whether the cardholder is enrolled in the scheme. If he/she is enrolled, the merchant plug-in sends an authentication request to the issuer via the cardholder's browser. The cardholder sends authentication information to the issuer who then confirms the transaction to the merchant who, in turn, submits an authorisation request to the acquirer. Eight-four per cent of the respondents to a recent survey reported in ePaynews.com (2003) felt the use of secure passwords was an adequate safeguard against online credit card fraud.

On the other hand, from a cardholder perspective it could well appear that the incentive to enroll in such schemes could be minimal. With the limited implementation of these solutions by merchants, customers will find that fraudsters can still use their card numbers with merchants who have not implemented the schemes. So it will not stop a fraudster from generating card numbers and using them on sites where BACCPPs are not being used. In many regions in which credit cards prevail, cardholders are provided ample protection by local regulations that limit their financial liability in the case of fraudulent transactions. Visa also advertises zero-liability to cardholders. With these consumer protections, coupled with the perception that this is a less than comprehensive solution to the problems of identity theft and card number generators, purchasers might not be encouraged to make the additional effort required to use the programs.

A cardholder can purchase at any site without using the BACCPP, even when the site offers these options. What would be the motivation, in this case, therefore for a cardholder to sign up? Would merchants have to offer incentives to entice customers?

How strong are the authentication requirements? A cardholder could encounter difficulties in repudiating an online transaction in case his/her password gets stolen and used by a fraudster. SPYwares are relatively common and passwords/pass-codes can easily be obtained using them.

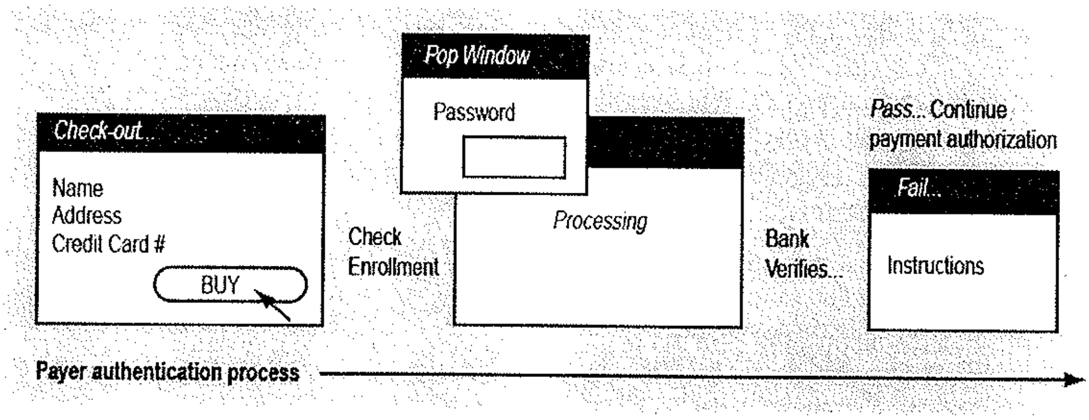
Does involvement in the process by the customer remove the right of the cardholder to repudiate a transaction when his/her credentials have been compromised and used fraudulently? Enforcing non-repudiation in some countries might eliminate much of the consumer protection that they currently enjoy. Will cardholder non-repudiation encourage consumers to use a solution that aims to do just that? The very process of repudiating a transaction can itself be a difficult one for a cardholder.

Then there is also the possibility that a fraudster, posing as a BACCPP enabled merchant, for example, could also pop-up the payer authentication stub, and obtain the card account number, expiration date and BACCPP password or pass-code. To mitigate this risk there is a "Personal Message" that is shown on the pop-up window. This message is one that the cardholder sets when he/she initially activates his/her password. If it is not correct or not shown at all then there is a strong possibility that the pop-up stub is not genuine. However, the onus is on the cardholder to take note of this message each time.

From the merchant perspective online merchants might nct accept these solutions for fear that the extra authentication procedure could discourage potential customers. Limited cardholder acceptance could be further disincentive to merchant adoption.

The introduction of new payment rules and cardholder authentication services from the BACCPPs guarantees payment to the merchant. Both schemes now offer merchants protection from chargebacks where the cardholder denies making the recorded purchase.

Figure 1 Buyer Authentication Process (Source: (CyberSource Corporation, 2002))



Merchants implementing these authentication programs will benefit from a liability shift to the issuing banks in the event of fraudulent and disputed transactions. According to the banks merchants who implement the BACCPP can also expect a significant reduction in 'No Cardholder Authorization' chargebacks. Possible economic benefits arising out of buyer authentication and limited liability are likely to include:

- Reduced fraud loss
- Reduced chargeback liabilities
- Reduced cost of investment in risk management tools
- Reduced overall operational costs
    - Transaction costs
    - Staff costs
    - Fraud and dispute handling

However, some merchants may be skeptical that the card associations' promise of a liability shift will eventuate even if they implement the program, with the suggestion that card issuers will re-classify the chargebacks to codes that still make the merchant responsible.

Compatibility

The compatibility of an innovation refers to the extent to which an innovation conforms to the potential adopter's existing values, previous experience and needs (Rogers, 1995). In general, compatibility has a positive influence on the acceptance of the innovation.

The use of credit cards as a payment instrument is a familiar and universal mechanism for finalizing transactions, particularly in the physical world. The BACCPPs make use of the existing credit card processing infrastructure. For those merchants who currently make use of credit card payment gateways, the BACCPP itself is an extension of the existing process of online card authorization. There is also support for multiple channel media (ITV, PDA, PC, Mobile, etc.) at low cost adaptation. From the cardholder's perspective the authentication process, namely the use of a username and password or PIN, is one that is generally familiar to them and is similar to the steps used quiet extensively for Internet banking and access to other computing systems.

However, at present very few large merchants offer BACCPPs. One possible reason could be that the schemes do not offer the option of referring to a prior transaction/authentication. Therefore a merchant cannot use the BACCPP during a "Sign Up" process once and process further transactions using the same Verification Code or Authentication Value. This is necessary in many environments such as ones where recurrent payments are required (e.g. monthly renewal of subscriptions) and where "one-click" payment options are supported, for example, "Amazon One Click". The work around the latter is by not reusing the CAVV/AAV of the previous transaction, but by making a new 3D transaction using the pre-registered card number. However, this will bring up the bank's pop-up window each time the cardholder does a checkout (completion of a purchase) at the merchant. The question is whether the extra work of an additional password entry is worth the payment guarantee.

Another issue that could be of concern to the potential merchant adopter is the level of interoperability of the two competing programs from the two major card organizations. Having to manage and maintain the two different schemes could be seen as an additional burden on the part of the merchant.

Complexity

Complexity, according to Rogers, refers to the extent to which an innovation is perceived as difficult to understand and use. The perceived complexity of innovations negatively affects its speed and probability of adoption.

For existing online card processing merchants the implementation process requires the installation of a Merchant plug-in and the addition of a few processing steps based on the new response codes. There is no need for the merchant to go through the integration process over again. Once this integration is done and tested, it is up to the cardholders' issuer to authenticate its cardholders for online transactions. In this way, merchants are relieved from the complexities of the transaction authentication concerns.

While the authentication process for the cardholder is far less onerous than previous efforts, some might still see that the solution is less than ideal. According to Bank Systems Online (2003), less than one per cent of online retailers were using the authentication programs in the first full year of its operations, with large online retailers such as Amazon.com seeing authenticated payments as "intrusive". This is supported by (Rasch & Linter, July 2001) who have found that each additional click in the purchasing process increases the number of customers who quit before completing their transactions.

Trialability

Trialability is the extent to which an innovation can be tried out on a limited scale (Rogers, 1995). Research has shown that trialability is more important for innovators and early adopters than for those who purchase the innovation later. The latter have less uncertainty with regard to the innovation because they know from the early innovators how effective the innovation is.

While it is not possible for a merchant to implement these programs on a trial basis, there are opportunities to test and view demonstrations of the programs.

Although the ultimate success of BACCPPs will be their mass adoption, there is one other measure of success that will provide an important milestone along the path to mass adoption. This will be the use of the BACCPPs as an "as-needed" solution. Security conscious consumers and fraud-prone merchants will have a viable solution to protect themselves. These early adopters will test the waters and measure the potential for a mass-market solution.

Observability

Observability is the extent to which the results of an innovation are visible to others (Rogers, 1995). Innovations with a clearly visible (positive) result are more likely to be purchased than innovations with poor visible results. It is suggested that any drop in fraud rates and increased consumer enrolment could provide clear evidence of the efficacy of the programs.

Marketing Initiatives

Rogers (1995) states that the awareness or knowledge of an innovation precedes and facilitates its eventual adoption. In this respect, a well executed promotional campaign by the vendor of a newly launched product or service can have a strong effect in fostering diffusion of the innovation (Chau, 2001). How influential is the role of marketer/supplier dominated activity on the adoption of the BACCPP?

A marketing campaign promoting BACCPPs has been started through television advertisements in Australia, and through the web sites of issuing and acquiring banks and the major card organizations. An updated list of merchant adopters together with testimonials is being maintained on these sites. Such effort is likely to create awareness both among merchants and potential online purchasers.

The liability shift as a marketing incentive

When a purchaser claims that he or she did not authorize a particular transaction and disputes the charge then this results in a chargeback. Most chargebacks in electronic commerce are 'No Cardholder Authorization' chargebacks – the cardholder either denies responsibility for the transaction or the merchant lacks evidence of the cardholder's authentication. The cardholder's issuing bank takes the money back from the merchant's acquiring bank, leaving the merchant bearing the brunt of the lost sale. The financial implications for a merchant who processes a fraudulent online transaction include inventory loss and shipping costs, and chargeback penalties.

In March of 1999, Visa International reported in Computerworld that less than 2 per cent of their credit card transactions occurred over the Internet, but that online transactions accounted for up to 50 per cent of their disputed charges (Legard, 1999). First Data Corp reported that 1.25 per cent of all Internet transactions are charged back, whereas only 0.33 per cent of catalogue orders and 0.14 per cent of brick and mortar transactions are charged back (Angwin, 2000). It has been estimated that a chargeback investigation costs US$100-US$125.

The impact of rising online credit card fraud and the concomitant costs due to chargebacks is therefore one of real concern to online merchants. VeriSign (2003b) identified the following costs to the merchant due to chargebacks:

- Loss of revenue
- Per-chargeback fees for reversing the transaction, typically between US$40 and US$100
- Higher discount rates assessed as a result of processing fraudulent payments
- Card association fines for consistently high chargebacks, in the region of five to six-figure amounts
- Labour costs for the merchant to investigate and resolve the chargeback
- Risk of losing merchant account due to high chargeback rates, and associated loss of ability to accept credit cards online

To stimulate adoption by merchants who might be wary of the impact of repudiated payments to their bottom line, the card organizations have introduced a marketing incentive to reduce the risks of early adoption by shifting the liability of chargebacks from the merchant to the cardholder's issuer if the merchant implements the programs, notwithstanding whether its customers enrol in it or not. However, two factors might make this incentive less attractive than it would first appear. The first one is that merchants and the financial institutions have to some extent already factored the cost of fraud into the cost of their products or services. Secondly, merchant investment in fraud screening tools has been large in recent years because card acquirers did not offer appropriate solutions to combat fraud. The question arises as to what the likelihood is of these investments being written off just because of a liability shift.

Risk Mitigation Measures

The objective of risk mitigation is to take actions and implement policies and procedures that reduce the likelihood of a loss. 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.

The first step in efficiently and effectively reducing the risk associated with card-not-present type transactions is through the use of a payment gateway which will support the validation of the card number and the identification of a lost or stolen card. Most acquiring banks are now recommending, and in some instances mandating that merchant usage of a secure payment gateway solutions for processing of payments sourced online. However, this process alone does not tell a merchant if the person is authorized to use the card. The next step, namely, cardholder authentication, should make it harder for fraudsters to initiate fraudulent transactions. An important milestone on the road to mass adoption will be the reduction in fraud arising directly out of BACCPP adoption. Early adopters will test the waters and measure the potential for a mass-market solution. If it is widely adopted it has the potential to dramatically reduce the impact of fraud on Internet merchants and consumers (VeriSign, 2003b).

Conclusion

BACCPPs promise to deliver a solution to the problem of cardholder authentication, consequently reducing fraud levels and chargebacks, increasing consumer confidence in e-Commerce, and eventually providing a better return on investments for merchants. This study addresses those factors that are likely to influence their adoption, using past and existing solutions as a basis of comparison. This should serve as a starting point for the various stakeholders to address the practical issues arising from developing, marketing, implementing and using these new models.

References

Angwin, J. (2000). Credit-Card Scams Bedevil E-Stores. *Wall Street Journal.*

Bank Systems Online. (2003, 28 November 2003). Jury Remains Out On Success of 3D-Secure. *ePaynews.com.*

Chau, P. Y. K. (2001). Inhibitors to EDI Adoption in Small Businesses: An Empirical Investigation. *Journal of Electronic Commerce Research, 2*(3).

CyberSource Corporation. (2002). *New Payment Rules Change Online Retail 2003.* Retrieved 14 April 2003, from the World Wide Web: http://www.cybersource.com

CyberSource Corporation. (2003). *CyberSource Launches Global eCommerce Initiative.* CyberSource. Retrieved 12/12/2003, from the World Wide Web: http://www.cybersource.com/news_and_events/view.xml?page_id=1090

CyberSource Corporation. (2004). *5th Annual Online Fraud Report.* Mindwave Research. Retrieved 12/12/2004, from the World Wide Web: http://www.security.iia.net.au/downloads/2004_fraud_report.pdf

ePaynews.com. (2003, 05 December 2003). Consumers Buying Online Despite ID Theft Fears. *ePaynews.com.*

Gowrisankaran, G., & Stavins, J. (1999). *Are there Network Externalities in Electronic Payments?*Unpublished manuscript, University of Minnesota.

GPayments. (2001, 2001). *Authentication: the missing element in online payment security.* Retrieved 12/04/2002, from the World Wide Web: http://www.gpayments.com

Jewson, R. (2001). *e-Payments: Credit cards on the Internet.* Retrieved 20/04/2003, from the World Wide Web: www.aconite.net

Legard, D. (1999). *Visa: e-commerce is major fraud source.* Computerworld. Retrieved 20/01/2000, from the World Wide Web: http://www.computerworld.com/home/news.nsf/CWFlash/9903243visa

Rasch, S., & Linter, A. (July 2001). *The Multichannel Consumer: The need to integrate online and offline channels in Europe*: The Boston Consulting Group.

Rogers, E. M. (1995). *Diffusion of Innovations.* New York: Free Press.

Sienkiewicz, S. J., & Bochicchio, M. (2002, 19 June 2002). *The Future of e-Commerce Payments.* Paper presented at the The Future of e-Commerce Payments.

VeriSign. (2003a). *Fraud Prevention: What every merchant should know about Internet fraud.* Retrieved 07/08/2003, from the World Wide Web: www.verisign.com

VeriSign. (2003b). *VeriSign PayFlow Fraud Screen* [White paper]. Retrieved 07/08/2003, from the World Wide Web: http://www.verisign.com