Prestige e-Journal of Management and Research
Volume 3, Issue 2 (October, 2016)
ISSN 2350-1316

E-Commerce Transactions: A Critical Analysis

Dr. Amitabh Joshi*

E-commerce signifies a web-based Internet market that has mount from zero, to over a trillion dollars globally, in just small span of time. The shift from physical to virtual payments has brought enormous benefits to consumers and merchants. For consumers it means ease of use. For mobile operators, mobile payment presents a unique opportunity to consolidate their central role in the m-commerce value chain. However, the security confront faced by the world's largest open (and effectively anonymous) network, have intended that the growth of the Internet – and e-commerce – has been met with an uniformly swift expansion in the activities of those purpose on using the Internet as a vehicle for wicked and criminal activities online. It is within the context of the growth of the Internet, and in particular e-commerce, that this report will examine current efforts to reduce the level of fraud in payment card-based ecommerce. Additional findings include the observation that despite well documented weaknesses and costs associated with the use of payment cards via a web browser and SSL, there has been a lack of progress by the payment-card industry in providing suitable alternatives. E-commerce as a whole is likely to see dramatic changes over the coming years as the potential for integrating smart cards and tokens with mobile devices is fully realized.

Keywords: E-Commerce, M-Commerce, Web Browser.

*Associate Professor, Prestige Institute of Management, Dewas, (M.P.), E-Mail: dramitabhjoshi@gmail.com.

INTRODUCTION

E-Business Transactions

Communities countrywide have been taking benefit of technology to modernize operations in the all the departments of organizations. Now, with the increase in no of websites or can be said that each firm have their websites may be used for information, or collection purposes, one area worth exploring is on-line bill payments. Transactions between unfamiliar persons are growing on full-fledge basis at a tremendous rate in recent years, largely as a consequence of the attractiveness of eBay and other Internet auction sites. Internet auctions are an international occurrence. In the United States alone, over 35 million people have participated in online auctions, and eBay alone boasts more than 22 million registered users globally. Correspondingly that people can purchase products via the Internet, there are services accessible for municipalities to offer on-line payment options to their taxpayers via a website. Most online transactions occur without a hitch, but the opportunities for mischief and error, in concert with the remarkable volume of dealings, inescapably upshot in a significant number of harms. Auction sites have embarked on pains to lessen the frequency of problems and, to a slighter degree, address troubles after they come up. Regrettably, fatalities of auction fraud and related issues frequently discover themselves without a sensible cure. Participants in online auctions use a mixture of payment methods, but cheques and money orders at a halt correspond to the most frequently used ways of payment. (Sorkin, 2002)

Credit cards afford superior protection to buyers, but until newly payment by credit card was not even an alternative for person-to-person transactions. However, quite a lot of online payment services have been recognized that enable individuals to make credit card payments to one another, usually with the payment service acting as a conciliator. These services are increasing speedily, chiefly because of the velocity and ease that they offer. Yet comparatively little consideration has been paid to the risks and probable liabilities they occupy for buyers and sellers. (Sorkin, 2002). Mobile commerce (m-commerce) is developing radically. The worldwide m-commerce market is predictable to be worth a staggering US$200 billion by 2004. M-commerce can be understand as any electronic transaction or information interface conducted using a mobile device and mobile networks, for example, wireless or switched public network,

which leads to transfer of real or perceived value in exchange for information, services or goods (MobileInfo.com). M-commerce involves m-payment, which is defined as the procedure of two individuals or firms exchanging financial value using a mobile device in return for goods or services. A mobile device is a wireless communication tool, including mobile phones, PDAs, wireless tablets, and mobile computers. (Mobile Payment Forum, 2002).

Due to the widespread use of mobile phones today, numerous payment schemes have come into view which permits the payment of services/goods from these mobile devices. In the subsequent sections an overall view of the E-payment systems and their characteristics are discussed. Also the operational issues are analyzed, which are critical to the adoption level of a payment system. The operational issues or characteristics will help in the unambiguous identification of the payment solutions.(Nambiar and Tien Lu, 2005).

The Birth of E-commerce

In 1989, Tim Berners-Lee wrote a note to the European Organization for Nuclear Research (CERN) management describing a worldwide hypertext arrangement– which would ultimately lead the development of the hyper text transfer protocol (HTTP), hyper text mark-up language (HTML), the 'browser', and what would eventually become the millions of web sites hosting web pages that we visit and view everyday via the Internet – collectively referred to as 'The World Wide Web' or 'The Web'. Public awareness of the Internet and the World Wide Web began to climb in the early 1990s and it wasn't long before retailers began to see the prospect to 'sell' on 'The Web'. Presenting a catalogue of commodities via a web page was one thing – permitting clientele to pay securely was another. In 1994, Netscape released the 'Navigator' browser and, later in the same year, released the first version of the Secure Sockets Layer protocol (SSL) – a protocol designed to establish an authenticated and confidential channel between a browser and a web server. A user using the Navigator browser was given a visual indication that they were now communicating securely with a web server via the padlock icon. The image of the padlock 'unlocked' would represent an insecure connection – while the image of the padlock 'locked' would represent a secure connection via SSL.

With an apparent solution to the problem of being able to securely transmit data from the user's browser to the receiving Web server, e-commerce sites quickly began to accept credit cards as a method of online payment for goods and service advertised on the Web. Giants such as eBay and Amazon, and a web-based Internet economy that has risen from zero to over a trillion dollars worldwide (See Appendix A – The History of E-commerce). In the UK alone, e-commerce is now estimated at a yearly value of 100 billion pounds, or 7.2% of GDP. The challenges of keeping payment systems secure have risen proportionately – particularly in the case of payments made via payment cards over SSL and despite advances in security mechanisms in general. These challenges include:

1. The expectation that the average Internet user is able to make informed security decisions about their personal and commercial actives online.
2. The overreliance of usernames and passwords as a primary method of authentication on the Internet.
3. The need for effective user-friendly payment methods that also represent good security practices.

OBJECTIVES

It is within the context of the requirement to generate enhanced and user-friendly mechanisms for secure payment systems, as well as to guarantee that all parties are quite sheltered. The objectives of this paper, therefore, are as follows:

1. To present a background to payment models
2. To draw conclusions as to whether given the current 'state of affairs' of e-commerce and online payments systems

PAYMENT SYSTEMS

Traditional Payment Methods

Most online auction transactions involve the use of checks, money orders, and other traditional means of payment. These mechanisms are generally less efficient than online payment methods, primarily because they require physical delivery of a payment instrument from the buyer to the

seller. The cost of using traditional payment mechanisms varies from trivial to substantial, and they also involve varying levels of risk. The continuing popularity of these mechanisms is probably the result of a combination of general satisfaction with current practices, switching costs and inertia, and lack of knowledge and possible distrust of new mechanisms.

Online payment systems

A great number of new Internet-based payment mechanisms have been created in recent years, although some of the pioneering efforts disappeared after failing to gain sufficient acceptance.41 Most of these mechanisms require the use of a third party to serve as an intermediary to the transaction. Depending on the mechanism, the intermediary may have a contractual relationship with the buyer, the seller, or both. In some instances, one party may not even be aware that an intermediary is being used. This broadly includes the following:

1. **Payment Cards -** Visa and MasterCard operate under what is called a four-party system. The four entities are:

a) **The Cardholder:** The individual in possession of a payment card.
b) **The Issuer**: The bank or organisation that issues the card to the cardholder.
c) **The Acquirer: T**he bank which receives payment from the issuer on behalf of the merchant.
d) **The Merchant**: The entity with goods or services to sell that receives payment instructions and details from the cardholder – to be settled by their acquirer (via the scheme network) with the issuer.

Merchants typically bear the cost of both a payment processing fee by the acquiring bank as well as an interchange fee. The interchange fee is designed to recover the costs of operating the scheme network, as well as correct the imbalance in costs incurred between the issuer and acquirer [25]. While the acquirer will typically have payment devices at point of sale – a terminal or card reader, capable of accepting payments from many cardholders – the issuer will bear the greater cost of issuing and managing payment cards and transactions for every cardholder.

2. **E-commerce via a Web Browser –** It illustrates the ‘straight-line’ communication between a user, using a web browser, and an e-commerce merchant, using an SSL certificate, to enable a secure channel between the browser and the merchant’s website.

These third-party service providers give taxpayers the ability to pay by electronic check transfers or credit card payments 24 hours a day. The community typically sets up a link on its website called "online payment," or something similar, which redirects the taxpayer to the third-party website. The service provider can create its page to look like the municipal website or not. If the community does not have a website, then taxpayers can be directed to the service provider's website via advertisements or bill inserts. At that point, the taxpayer has the ability to pay for their tax, excise or fee (depending upon which on-line payments the municipality has available) using either an electronic checking transfer or a credit card. The e-check option is usually free, while the credit card fee is passed on to the taxpayer. The "customer" will receive an email confirming payment. Ideally, once the system is in place, the collector sends the tax, excise, or utility commitment to its service provider, who would upload it into their system. Depending on the software in place in the collector's office, the outside vendor may or may not have compatibility issues.

This is something that the collector should discuss with the vendor before an agreement is reached. Once the commitment is on the service provider's system, payments, either through electronic check or credit card, became possible. The service provider can then wire the money to the municipality, or deposit it directly into a deposit-only bank account in the municipality's name. The third-party service provider should also provide the municipality with an electronic and hardcopy register of payments received. If the municipality and the vendor have compatible software, the collector can download a record of payments received and post them immediately. If not, then payments would have to be manually posted. A separate form of "on-line bill payment" is available to the taxpayer who chooses to utilize the electronic bill payment service through their own bank. In this situation, taxpayers direct their bank, through its website, to pay a certain amount to a vendor, in this case, the municipality. The bank then mails out a check. This method can be misleading. The average consumer is often under the impression that their bank wires the money to the vendor, thus decreasing the "float" time between payment and receipt.

CHECKLIST OF E-TRANSACTIONS

An ideal requirements wish-list for online payments in e-commerce might look something like the following:

1. **Confidentiality** – The payment scheme should offer optional levels of confidentiality – allowing details of the transaction to only be made known to those parties to whom the customer or merchant so wishes.
2. **Integrity** – The scheme should maintain the integrity of the transaction – making tampering or changes to the details of the transaction practically infeasible.
3. **Authentication** – The scheme should provide methods for the authentication of communicating parties and/or the authentication of messages that are relied upon for payment authorization – making fraudulent activity difficult.
4. **Non-Repudiation** – The scheme should provide non-repudiation services – protecting both the merchant and customer against false claims.
5. **Availability** – The scheme should be highly available – allowing customers and merchants to participate in payment transactions when required.
6. **Implementation** – The scheme should provide clear benefits to merchants and customers justifying any costs associated with the scheme's implementation. The implementation details should attempt to abstract complexity and provide interfaces with merchant systems that represent good practices in software development in general.
7. **Interoperability** – The scheme should be interoperable – providing the widest possible access to merchants and customers.
8. **Ease of Use** – The scheme should be easy to understand and use for the customer.
9. **Scheme Protection** – The scheme rules and policies should continue to provide consumer protection from unscrupulous or fraudulent merchants. The scheme rules, policies and regulations should also continue to protect the payer when a claim of fraudulent activity is made. The onus should be on the scheme owners to disprove the validity of the claim, and not rely solely on the mechanisms of the scheme to automatically dispute such claims.

ONLINE PAYMENTS BENEFITS

Efficiency and convenience appear to be the primary motivations for buyers and sellers to use online payment systems and, albeit to a lesser extent, the factors that differentiate the systems

from one another. Other relevant intrinsic characteristics include reliability, security and finality. Online payments enable transactions to be completed more quickly and often with less effort. A buyer who has bid on and won an item at an online auction site can submit payment via the web rather than by mail. The seller immediately receives payment or, in the case of BidPay and online escrow services, notification that payment has been made and authorization to proceed with the transaction. Thus the seller can ship the goods promptly rather than waiting a few days to receive payment or possibly much longer for a check to clear.

Online payment services are particularly well-suited to international transactions where mailing a payment instrument would take even longer and would likely involve additional transaction and conversion costs. However, while acceptance of traditional payment devices is nearly universal, many buyers and sellers do not use online payment services. Unless both parties agree to use an online payment service and agree upon which particular service to use, a transaction is likely to be completed using a traditional payment device. Cost is another concern, but, surprisingly, it does not seem to be as major a factor as convenience, for online auction participants, in deciding whether to switch from traditional payment devices to their online counterparts. For most online payment services, the seller typically contracts with the service and pays the transaction fee. While the buyer is normally aware that a third-party payment service is being used, the buyer generally need not be a registered user of the service and may not even be familiar with its transaction fees. The fees tend to be approximately the same as those payable by merchants for accepting traditional credit card payments; for example, under $1 for a $10 sale, or about $3 for a $100 sale. Sellers may view these costs as comparable to the costs of processing other forms of payment, or, perhaps more likely, may believe that accepting online payments increases the demand by potential bidders for their goods. Most sellers apparently understand the fees charged by online payment services and seem to be somewhat sensitive to differences in fees charged by competing services. With BidPay, the buyer, rather than the seller, contracts with the payment service and pays its fee. The seller may not even be familiar with the service. From both parties' perspective, a BidPay transaction is effectively equivalent to a buyer purchasing a money order and mailing it to a seller, except that BidPay makes this process more convenient for a buyer. Especially for small transactions, BidPay's minimum fee of $5 may seem high, but most buyers

who choose to use BidPay are presumably willing to pay for the convenience that it offers, at least where the seller does not accept payments through other online payment services. There are a number of advantages to offering on-line payments:

- It sends a progressive message to taxpayers about customer service and the use of technology.
- It reduces foot and mail traffic to the collector's office (reduces lock-box fees, if applicable)
- It can result in faster deposits and postings of payments.
- It can reduce delinquencies by offering greater payment convenience to the taxpayers.
- It reduces the number of over- and under-payments in a few ways. The collector does not receive a mailed check after the due date, and the on-line information is in real time, therefore the taxpayer can determine the exact amount due, plus interest if applicable.
- It can reduce telephone inquiries.
- Mortgage companies tend to take advantage of this feature, reducing collector hours spent managing those accounts.

THE INSECURE INTERNET

There are now an estimated two billion Internet users globally with over 30 million adult users accessing the Internet everyday in the UK alone. From its origins as an experiment in reliable 'packet based' networking in the late 1960s and 1970s – The Internet has grown into a pervasive interconnected network of computers and applications that spans the globe and is dramatically changing the world we live in. The early inventors of the Internet did not anticipate its current size or impact, and while its growth might serve as a testament to the eloquence of its original design – from a security perspective, things are a little more complicated. Early users of the Internet accessed the network from the relatively safe environment of academic institutions and protected data centres. Issues of identity and authentication were considered lightly at a time when the Internet existed within a culture of co-operation, trust and resource sharing. The result was that the foundation protocols of the Internet were vulnerable to those who saw the Internet as a convenient vehicle for malicious and criminal activities.

From a purely commercial perspective, The Internet Crime Complaints Centre (IC3) in the USA in its 2009 IC3 Annual Report stated a dollar loss in referred complaints of 559.7 million US

dollars – up from just 17.8 million in 2001. The UK Cards Association reported 266.4 million pounds sterling in card-not-present fraud in 2009 – from 95.7 million in 2001.
The growth of the Internet has provided us with many novel and convenient methods of communication. And yet it would appear that as more 'value' moves into electronic form and onto the Internet, so too does the risk that information of value will be lost or used in ways to commit malicious and criminal acts.

It is at the confluence of these dramatic changes that we find ourselves today – with increasing value in personal, private and commercial information online, as well as increasing activity from those intent on making money from criminal activities via the Internet. It is also at the confluence of these changes that most Internet users finds themselves confronted by a bewildering landscape of terminology and technology. Users are expected to choose (and remember) numerous account names and passwords. Users are also expected to defend themselves from solicitous and often fraudulent emails as well as somehow determine whether the website to which they are about to hand over their credentials or payment details, is trustworthy and legitimate, as opposed to a cleverly disguised ruse designed to part them from their hard-earned cash. Users as individuals are not alone in their efforts to defend themselves online, as security has become a major concern for the commercial and public sectors as well. However, it's at this point that the interests of larger organisations with deep technical knowledge and dedicated resources may not entirely align with the interests of the average Internet user. The average user is as potentially vulnerable to changes in the 'terms' within which they are expected to interact and exchange information online as they are to the overt actions of a malicious third party.

It also seems unrealistic to expect users of the Internet to be able to make informed decisions about the security of their activities online – when most don't actually know what the Internet ***is*****.** Take for example a light-hearted 2009 on-the-spot survey performed by Google employees (see http://www.youtube.com/watch?v=o4MwTvtyrUQ), where about fifty people were asked what a browser is. Of those asked, only about 8% were able to describe what a browser is and how it is used on the Internet. Some of the extrinsic harms of online transactions are:

A. Payment Service Failure

One of the risks faced by users of online payment services is the possibility that a payment service will commit an inadvertent error, intentionally misappropriate funds or go out of business altogether. The last of these possibilities seems most likely. In fact, several online payment services have already ceased operations. Nonetheless, all three possibilities warrant concern given the unregulated status of online payment services and the fact that the remote location of a payment service may reduce an injured party's prospects for a remedy.

B. Privacy Implications

A second set of extrinsic risks relates to the use and potential misuse of personal information by online payment services. Because they are largely unregulated, online payment services are generally free of legal constraints on collection and use of personal data, unlike banks and other financial services providers. Generally, online payment services provide at least some privacy protections voluntarily, either in their general terms of service or in a separate privacy policy.

C. Transaction Risk

Some consumers are familiar with the use of payment devices as a means of insuring against risk in an underlying transaction, either because they are familiar with legal protections119 or because they believe that the ability to stop or withhold payment may provide them with practical leverage in the event of a dispute. This awareness is probably rising as credit card providers and consumer advocates promote increased use of credit cards as a means of reducing the risks of engaging in online commerce.

CONCLUSION

The historical context presented earlier in this report makes clear that both the Internet and ecommerce have developed in ways that were unanticipated by their creators. And that this unanticipated growth was driven by novel methods of communication and trade. However inherent weaknesses in security, combined with the fundamental challenges of establishing trust and identity, meant that growth on the Internet, was followed closely by increasing levels of malicious and criminal activities online. Fraud and related problems are relatively rare but do arise in a significant number of transactions, and victims frequently find themselves without a satisfactory remedy. Payment systems can play a role in reducing transactional and other risks in

online auctions just as they do in traditional commerce, but relatively little attention has been paid to the effects of emerging online payment systems. As e-commerce developed – and despite attempts to develop alternative and arguably more suitable schemes for making payments online – payment cards became the predominate method for making payments in web based e-commerce.

REFERENCES

A Brief History of the Internet. http://www.isoc.org/internet/history/brief.shtml (accessed Aug 04, 2012).

A Little History of the World Wide Web. http://www.w3.org/History.html (accessed Aug 9, 2012).

Boston Consulting Group Report. http://www.connectedkingdom.co.uk/the-report/ (accessed Aug 02, 2012).

IC3 2009 Annual Report on Internet Crime Released, 2010. IC3. http://www.ic3.gov/media/2010/100312.aspx (accessed Aug 12, 2010).

Internet Usage Statistics, 2010. Internet World Stats. http://www.internetworldstats.com/stats.htm (accessed Aug 8, 2012).

Mobile Payment Forum. (2002). *Enabling secure, interoperable, and user-friendly mobile payments.* Retrieved September 9, 2003, from http://www.mobilepaymentforum.org/pdfs/mpf_whitepaper.pdf

MobileInfo.com: M-Commerce. Retrieved September 9, 2003, from http://www.mobileinfo.com/Mcommerce/index.htm

More Magic Software (2000, November 24). *Payment transaction platform.* Retrieved September 9, 2003, from http://www.moremagic.com/whitepapers/ technical_wp_twp021c.html

Nambiar, S., & -Tien Lu, C. (2005).*M-Payment Solutions and M-Commerce Fraud Management.* USA.

Sorkin, D. E. (2001). *Payment Methods For Consumer-To-Consumer Online Transactions.*

Transport Layer Security. http://en.wikipedia.org/wiki/Secure_Sockets_Layer (accessed Aug 9, 2012).