

Online Payment Process

Name Kathleen Kaye Acosta
Nr. 230431
Course E-Business Technologies – SS2008
Professor Dr. Eduard Heindl

Declaration

This is to certify that this term paper has been written by me. The articles and literatures read for the preparation of this paper has been acknowledge and are cited and can be found in the reference section of this paper.

Kathleen Kaye Acosta
16 June 2008

Table of Contents

1. Introduction	4
2. Online Payment Methods	4
3. Online Payment Process	6
3.1. Online Credit Card Payment Process	6
3.2. Some of the Online Credit Card Transaction Enablers	10
4. Security in Online Payment	11
4.1. Standard Security Protocol	11
4.2. Fraud Rate	12
4.3. Fraud Protection	13
5. References	14

1. Introduction

Why people came up for online business? There are many reasons why we go for this type of business. For the seller or merchants, they can operate their business profitably 24/7 and reach the market across the world - geographical boundary is not a barrier anymore. It is not necessary for them to establish their shops physically in many places around the world which means anyone even small businesses can have their business online. While at customers' end, it is more convenient where one can place his/her purchase orders in just a click of the mouse anytime of the day regardless of where one is standing. Another reason is transactions are even faster that transactions are done in just a few minutes. Payment transactions for these online businesses can be done either online or offline. However, nowadays the method of payment has become important and the possibility for online payment acceptance provides convenience to the customers. In this paper, I will be discussing about the online payment process.

What is Online Payment?

Online payment is when the customer or buyer makes his payment transactions for the goods or services purchased with the use of the Internet – to be online. “This type of payment lowers the costs for businesses as the more payments made electronically (online or offline) the less they spend for paper and postage. Also, it helps on improving customer retention as he is more likely to return to the same e-commerce site where his or her information has already been entered and stored.” [1]. With online payment, it is not necessary for the payer to be in a long queue as payment is made in just a click of a mouse. Additionally for example, almost all the banks have an online bill payment service where it is offered free of charge and is available all days of the week or 24/7 shall I say.

Nevertheless, the issue on security is a crucial element to the implementation as well as acceptance of payment both for sellers or merchants (fraud) and buyers or customers (privacy or identity theft). I will go into details about this topic in chapter 5 of this paper.

2. Online Payment Methods

For the purchases done online most likely he will also make his payments online. In this section, you will find the different methods on making online payments.

2.1. Credit Cards. This has been the dominant form of online payments when purchasing online. However, many people still resist the appeal and simplicity of credit-card transactions due to security concerns. Until now there are a high risk for stolen cards, identity theft thus customers fear credit-card fraud by merchants

and other parties [2]. Yet, there are some credit card issuers who have features that provide online fraud protection.

- 2.2. **Virtual Credit Cards.** This virtual credit card is an innovation in online credit cards. Credit card issuer provides a special number that can be used in place of the regular credit card number to make online purchases. This allows the user to use a credit card online without disclosing the actual number. Additionally, the user gives a transaction number instead of the credit card number – example is *Private Payment* by American Express. [3]
- 2.3. **Debit Cards.** With the debit card, the money for a purchased item comes directly out of the holder's checking account. The actual transfer of funds from the holder's account to the merchant's takes place within 1 or 2 days [3].
- 2.4. **Smart Cards.** This card looks like any plastic payment card but it has a microchip embedded on its face. This can hold more information than ordinary credit cards with magnetic strips. Rather than holding only card's information, it can also hold information for such as health care, transportation, identification and banking, and others. This enables information for different purposes to be stored in one location. The smart card can be used to make purchases over the Internet with the use of a card reader to read the card details necessary for payment and secure sending of data over the Internet [3].
- 2.5. **e-Checks.** An e-Check is an electronic version or representation of a paper check. It contains the same information as a paper check and based on the same legal framework. It works the same as the paper check however they are faster, cheaper and more secure [2]. To pay by e-check, an account number is keyed in and together with the bank's routing number. The vendor authorizes payment through the customer's bank, which then either initiates an electronic funds transfer (EFT) or prints a check and mails it to the vendor [1].
- 2.6. **Digital Cash.** Digital cash is an example of a digital currency, where it allows people who do not have credit card to shop online. It is similar to a traditional bank account: consumers deposit money into their digital cash accounts to be used in the purchase online. This is often used with other technology such as digital wallets [2].
- 2.7. **e-Wallets.** An e-wallet is a software component that a user downloads to their desktop and in which the user stores credit card numbers and other personal information. When a user shops at a merchant who accepts e-wallet, the user clicks the e-wallet and the forms are automatically filled in with all the necessary information in just one click. Credit card companies such as Visa and MasterCard also offer this e-wallet [3].
- 2.8. **Peer-to-Peer Payments.** P2P payments are one of the fastest-growing online payment schemes as they enable the transfer of funds between two individuals.

PayPal is one of the first companies to offer this service. A user will open an account with the username, password and also an e-mail address as well as the payment card or bank account number. Then the user adds funds to their account and once account has been funded, the money can be sent to the recipient who also has an account at PayPal, for instance. The e-mail that is sent to the recipient contains a link back to the service's (PayPal) website and can transfer the money from the PayPal account to their credit card or bank account. [3]

2.9. e-Billing. E-Billing is also called *electronic bill presentment and payment (EBPP)*. This enables the presentment, payment and posting of bills via the Internet. Presentment means taking the information that is typically printed on a bill and hosting it on a bill-presentment web server. Once the bill is available, the customer can view it with the browser, review and then pay online. When the payment is received, it is posted into the biller's account receivable system and the payment is transferred from the customer's account. It is said that online payments are expected to grow to more than 15% of 19 billion bills by 2011. [3]

3. Online Payment Process

In discussing the online payment process, I took the example of a credit card transaction as this is most commonly used when making payments for the purchases made online.

3.1 Online Credit Card Payment Process [4]

In the processing of a credit card payment, there are several entities that play important roles to make the online payment possible. For the payment to be successful, merchants must connect to a network of banks (both acquiring and issuing banks), processors, and other financial institutions so that the information provided by the customer can be routed securely.

1. Cardholder – the individual or the entity or simply the customer that uses his credit card to pay the purchases made online.

2. Issuing Bank – the financial institution that issues a credit card to the cardholder. The issuing bank establishes and verifies the cardholders' credit line to see if he has available credit to purchase a product/service and it provides the cardholder with the monthly billing statements, etc.

3. Credit Card Issuer/Association – a financial institution that provides credit cards and other products for banks who privately brand the products such as Visa International or MasterCard International. Also they often set up programs for merchants to accept the cards. Also they are involved in operating and managing the authorization and settlement systems worldwide.

4. Merchant – the entity or an individual that is selling products/goods or services. Goods can be either hard goods (tangibles) such as apparel, computer hardware any kinds of goods that is possible to sell over the Internet or soft goods (intangibles) such as service contracts or pay-per-view content.

5. Acquiring Bank – an entity that is often referred to as the merchant bank or acquirer. It is the financial institution that enables merchants to accept credit card payments. The acquiring bank often works with the third-party processor to accept or decline the cardholder's credit card purchase or request, deposits funds into the merchant's bank account, provides the merchant with the periodic deposit statements, etc.

6. Payment Application – the application that is used by the merchant to request credit card authorization and settlement of funds between the merchant and the acquiring bank. This application can either be self-managed application or can be an outsourced service.

7. Third-party Processor – also known as payment processing networks, frontend processors, or just processors, the organization that works with an acquiring bank (merchant bank) to process credit card transactions via the card issuers/associations. The third-party processor communicates to the card associations/issuers to obtain authorizations and execute fund transfers. In some cases, the acquiring bank and the third-party processor may be the same entity.

8. Independent sales organization (ISO) – an independent agent that solicits prospective merchants for merchant banks, ISOs are also referred to as merchant account providers. ISOs assist merchants in setting up merchant accounts and ensure that the accounts connect to the third-party processors. ISOs may either assume partial or shared financial liability for merchant activity.

When using the credit card for online payment, merchant's account must be in place with the acquiring bank or with the third party service. As soon as the customer makes a purchase online and pays using his credit card, he is required to submit his credit card information which is then sent securely over the Internet to the merchant's. Below is an illustration (see Figure.1) on how is the process going on when a transaction of purchasing and payment (thru credit card) is made online as well as the step-by-step process explanation of the figure. Nevertheless, please take note that this is a simple and generic online transaction processing, authorization and settlement where potential steps can be added into it [4]:

1. **Card issued:** The customer has a credit card with him issued by the issuing bank with the credit limit and an available balance.
2. **Buy button:** The customer visits a web site or the online shop using standard web browser and start shopping and add the product(s) into his shopping cart. Upon

checkout, he is required to submit his credit card information, expiration date, billing address. After which, he also selects the method of shipping for example and then click on the submit button to initiate the transaction. The information is then transmitted to the merchant's online shop where the outsourced payment service is setup. The outsourced payment service receives the encrypted information from the online shop, perform a fraud check, and then initiate the process of communicating the billing information and purchase amount to the third-party processor.

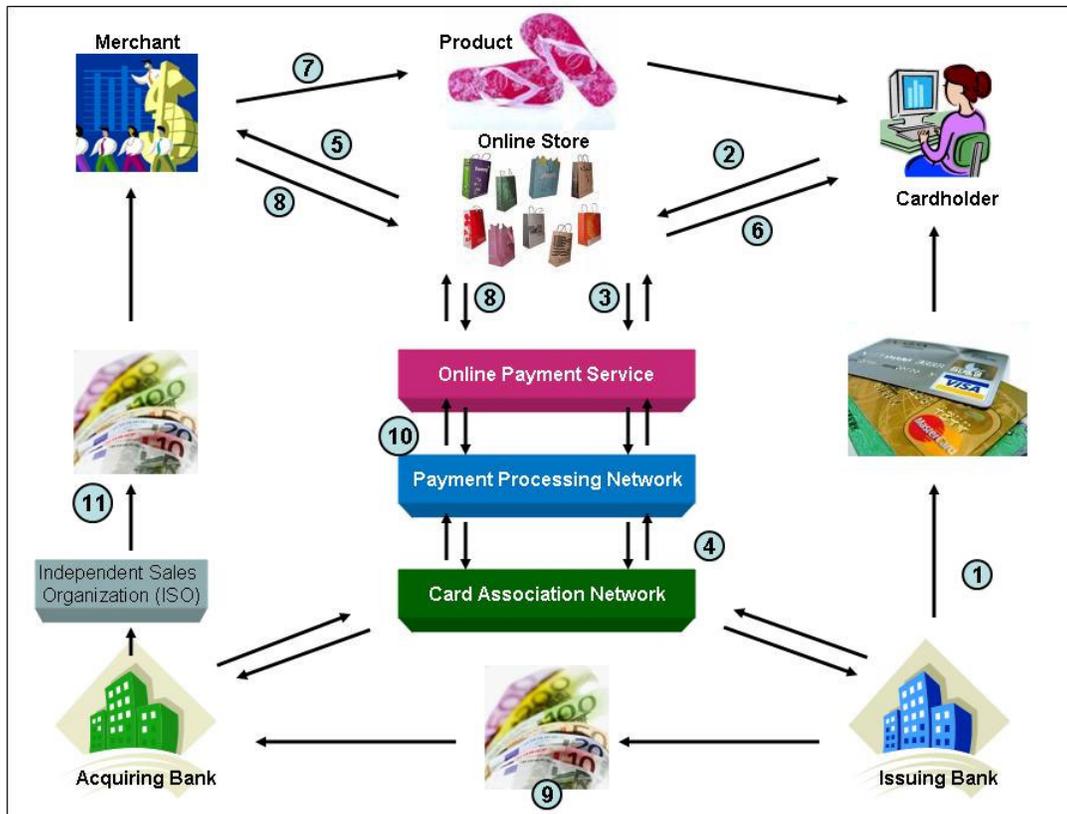


Figure 1 – Anatomy of an online credit card transaction [4]

3. Authorization request: The outsourced payment service encrypts the purchase information or data and transmits it to the third-party processor, who will forward the information or data further to the card association or card issuer for authorization and verification.

4. Authorization response: The issuing financial institution verifies the credit card information and determines whether the customer has sufficient credit available to pay for the purchase. An authorization number is generated and the available credit is reduced by the authorized amount. If it so happen that the credit card information is not correct or if there is not enough available credit, then a message declining the transaction is generated.

During this short span of time, the issuing bank also performs other operations such as address verification service (AVS), where the billing information entered online is compared to the entry in the issuing bank's database – this is the authentication part. After which, an authorization message is returned to the card association and forwarded to the third-party processor.

5. Merchant notification: The third-party processor receives the authorization message and other pertinent information from the card association or issuer and initiates the process of communicating the authorization message to the merchant. The third-party processor encrypts the authorization message and transmits the encrypted information to the merchant's secure commerce server.

6. Shopper notification: The merchant's server receives the information and is programmed to send immediately the purchase approval or decline message to the cardholder/customer. Normally when the credit card was declined, some pertinent information like a suggestion to check for the accuracy of the information provided or to use a different credit card is sent. As soon as the customer receives this information for example approved transaction he at the same time receives a confirmation number.

It takes only a few seconds end-to-end from the moment that the customer hit the buy button until he receives the authorization message back. The authorization process usually takes a few seconds, depending on the merchant's payment application and procedures as well as Internet traffic and other factors.

7. Fulfillment: The merchant begins the process of fulfilling the customer's order with the appropriate product/service.

8. Settlement request: The merchant compiles a batch of orders that have been fulfilled and begins the process of transmitting batch to the third-party processor for the settlement. The merchant first transmit the batch to his payment service that encrypts the purchase information and transmits the encrypted information to the third-party processor. The third-party processor receives this information and sends the settlement instructions to the appropriated financial institution to transfer the ticket amount from the cardholder's account to the merchant's account.

9. Settlement: For each credit card transaction in the batch, the appropriated financial institution is debited and the cardholder's credit card statement is updated. The acquiring bank receives the funds and makes a deposit into the merchant's bank account.

10. Settlement response: The merchant receives the notification that the funds have been deposited into his bank account. On a periodic basis, the merchant

receives reports that he can use to reconcile with his batch settlement requests with his deposit activity.

11. Funds available: The interval between the merchant's issuance of a settlement request, funds transfer and funds availability can take up to several days, depending on the issuing bank, the acquiring bank and the third-party processor. The settlement cycle time is actually affected by the acquiring bank's holding period on deposits, as well as other procedures and policies established by the acquiring banks and third-party processors.

3.2 Some of the Online Credit Card Transaction Enablers [2]

In this section, I will be presenting some of the online payment enablers that are commonly used by merchants to enable the acceptance of payments online particularly for the online credit card transactions. There are a lot more of them but I will only discuss a few of them. These companies established business relationships with the financial institutions to accept online credit card payment for their merchant clients.

1. **PayPal.** *“Arising from the popularity of eBay online auctions, PayPal (www.paypal.com) has quickly become dominant in online transaction processing”* according to Pan-Western E-Business Team [9]. Many people still think of PayPal primarily as the service to use to pay for items they buy on eBay. PayPal originally started as a peer-to-peer money transfer system for eBay auctions, but has also expanded as a third payment processor for any website. Two of their main gateway products that they offer are **Payflow Pro** and **Payflow Link** [10].
2. **Google Checkout™.** Google has an online payment processing service particularly for credit card transactions. The difference between PayPal is that the scope of Google Checkout™ is focused on enabling one-time payments to be made from a purchaser to a merchant [11].
3. **Authorize.Net.** Like any other payment gateways Authorize.Net handles online payment transactions for credit card and electronic payment processing between the merchants and financial processing networks [12].

These three vendors are almost the same in a way that they connect the merchants' website to the back end processing systems of the credit card issuer. Only they differ in the charging policy such as monthly fee and transactions fee that has been regulated differently.

4. Security in Online Payment

Security is vital when doing business be it online or offline. If I compare the traditional transaction using a credit card, what the merchant need is the signature of the cardholder and sometimes the photo on the credit card is also use to verify the identity of the customer. In the virtual world, information needed are the credit card number, the verification code and the billing address to verify the identity of the cardholder and fraudulent transactions are always around.

Common challenges that the merchants have to face are Internet fraud, product returns, non-delivery claims, disputes that leads to chargebacks and etc. As regard to the customers are stolen cards, theft identity and so on. Most people think that the customers are most in danger of being defrauded, however the truth is that merchants are more often the targets of fraud and they are at the same time held liable for these fraudulent transactions [4]. Therefore, a well devised security system can address these security issues that are very crucial to the online payment acceptance. VISA for example, has developed a list of “best practices” to be used by the merchants when conducting credit-card transactions. This list includes implementing a firewall, using encryption, anti-virus software and the incorporation of intercompany security practices and the protocols are also mandatory [3] which I will discuss in the next topic.

4.1 Standard Security Protocol.

SSL and SET technologies are used for data security where data are encrypted and digitally signed before transmission over the Internet. **Secure Socket Layer (SSL)** and **Secure Electronic Transaction™ (SET™)** are the standard security protocols that protect the integrity of these online transactions. **SSL** was developed by Netscape Communications, a nonproprietary protocol used to secure communication in the Internet and the Web. This SSL is built into many web browsers including Netscape Communicator, Microsoft Internet Explorer and numerous other software products. SSL uses public-key technology and digital certificates to authenticate the server in a transaction and to protect the private information and transmit the data over the Internet with integrity [2]. However, in the case of online credit card transactions for example, there are more to make than just encrypting the credit card information upon transmission to the merchant – such as checking the validity of the card, the authorization of the card, etc. **SET™** is a cryptographic protocol which was developed by Visa International and MasterCard International was designed specifically to protect and handle the complete online transactions both for the customers and the merchants. SET uses the digital certificates to authenticate each party in a transaction. Additionally, it requires special SET software to process transactions. With this protocol, the merchant never sees the customer’s information like the credit card information as it is not stored on his server which reduces the risk of fraud. [2].

Moreover, you will know that you are transacting safely or when the website is running on a secure server when you see the **lock** icon found in the status bar of your browser and also in the URL in the address bar has the prefix ‘**https**’ instead of ‘http’, see Figure 3 below.

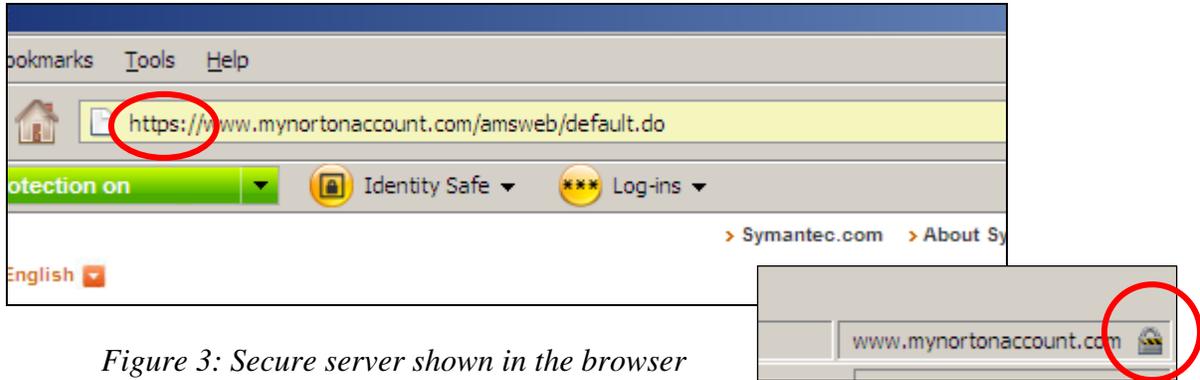
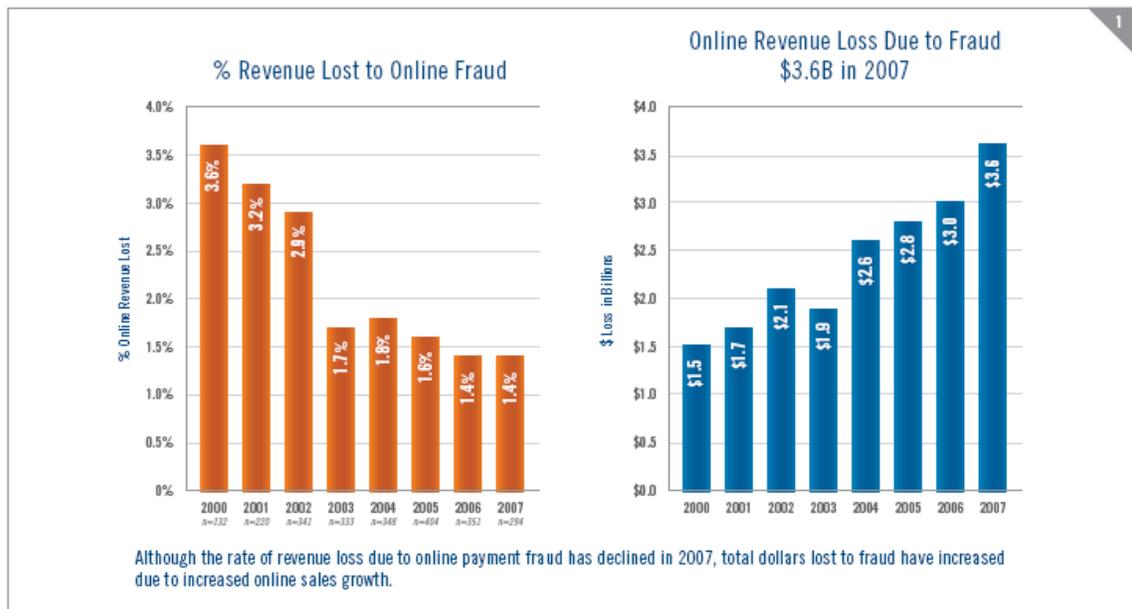


Figure 3: Secure server shown in the browser

4.2 Fraud Rate

In the graph below (Fig. 2) it shows how the online payment fraud is still a significant problem for many e-businesses. According to CyberSource® Annual Online Fraud Report – 2008 Edition, “Over the past few years the percent of online revenues lost to payment fraud has been slowly declining from 1.8% in 2004 to 1.4% this year. However, total losses from online payment fraud in the U.S. and Canada have steadily increased during this time as eCommerce has continued to grow 20% or more each year (U.S. Census Bureau Retail E-Commerce Sales reports, Shop.org & Forrester Research). In 2007, we estimate that \$3.6 billion in online revenues will be lost to online fraud — up from \$3.1 billion in 2006.” [5].



¹ U.S. Census Bureau Retail E-Commerce Sales reports, Shop.org & Forrester Research.

Figure 2: Fraud Rate [5]

4.3 Fraud Protection

As mentioned earlier, merchants are held liable for fraudulent transactions that lead to chargebacks. Some companies have a feature where transactions are monitored by how many times the credit card for example is being used within a day, where if the transaction is suspected, the merchant can reject the request. The credit card issuers had also established a solution to make the online payment transaction more secure. These are “Verified by Visa®” program of Visa Inc. and “SecureCode®” program by Mastercard which are used during the authentication process that protects both the cardholders as well as the merchants’ liability against fraudulent credit card transactions.

In MasterCard SecureCode® [6], every time the cardholder pays online through the merchant’s website, he will automatically be prompted to enter the unique and private code called the SecureCode that was issued and registered with his issuing bank as part of the authentication process of the transaction made before confirming that the purchase transaction is completed.

In Verified by Visa® [7], it uses the same system in authenticating the cardholder’s transaction. The cardholder activates his visa card online directly with Visa Inc. or with his issuing bank’s website. During activation process, the cardholder has to create a unique password which shall be used together with the credit card number when making a purchase online. Another way also is the use of the “3-Digit Security Code” by Visa Inc. as below:



Furthermore, there had been suggestions on how online merchants can prevent fraud in general (see points below) [9] or avoid chargeback problem such as subscribing to services like ChargebackPrevention.com and the like [8].

- Understand what existing technical measures are already in place to reduce fraud by your payment gateway.
- Retain and require documentation for every stage of the sale
- Respond to your customers in a timely fashion.
- Require human intervention for suspicious orders, such as international orders, mailing addresses with PO boxes, and orders over a certain amount of money
- Consider using a shipper that can provide you with a signature for proof of delivery
- Find out if your payment processor provides some sort of seller fraud protection, and follow their guidelines

5. References

- [1] URL: <http://communication.howstuffworks.com/electronic-payment2.htm>
<http://communication.howstuffworks.com/electronic-payment1.htm>
- [2] H.M. Deitel, P.J. Deitel, K. Steinbuhler. *e-Business and e-Commerce for Managers*. Prentice Hall Publishing, New Jersey.2001. pages 92, 94, 95, 97, 193
- [3] Efraim Turban, David King, Jae Lee, Dennis Viehland. *Electronic Commerce 2004 – A Managerial Perspective*. Pearson Prentice Hall, New Jersey. 2004. pages 498, 499, 507, 517
- [4] Bayles, Deborah. *E-commerce Logistics & Fulfillment: Delivering of Goods*. Prentice Hall PTR, New Jersey.2001. pages 94 -95, 97
- [5] CyberSource®. *Annual Online Fraud Report – 2008 Edition*. page 4 (accessed June 15, 2008)
URL: <http://www.cybersource.com/cgi-bin/pages/prep.cgi?page=/promo/FraudReport2008NA/index.html>
- [6] MasterCard URL: <http://www.mastercard.com/securecode> (accessed June 16, 2008)
- [7] Visa Inc. URL: <http://www.visa.com/verified> (accessed June 16, 2008)
- [8] Online material: Efraim Turban, David King, Jae Lee, Dennis Viehland. *Electronic Commerce 2008 – A Managerial Perspective*.
http://wps.prenhall.com/wps/media/objects/5073/5195381/pdf/Turban_Online_W12.pdf

(accessed June 16, 2008)

[9] Pan-Western E-Business Team *(accessed June 12, 2008)*

URL: http://www.e-bc.ca/media/ebizguides/internet_payment_processing.pdf

[10] *URL: https://www.paypal.com/us/cgi-bin/webscr?cmd=_payflow-gateway-overview-outside (accessed June 12, 2008)*

[11] *URL: <http://checkout.google.com/support/sell/bin/topic.py?topic=8664> (accessed June 13, 2008)*

[12] *URL: <http://www.authorize.net/company/whatwedo/> (accessed June 15, 2008)*