

A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business

Nucharee Premchaiswadi*, James G. Williams** and Wichian Premchaiswadi***

*Faculty of Information Technology
Dhurakij Pundit University, Bangkok 10210, Thailand
E-mail: nucharee@dpu.ac.th

** Professor Emeritus, University of Pittsburgh,
Pittsburgh, Pa., USA

E-mail: jellybeanjw@atmc.net

***Graduate School of Information Technology,
Siam University, Bangkok 10163, Thailand

E-mail: wichian@siam.edu

Abstract: Nowadays, an on-line credit card payment of purchasing products and services on the Internet has increased. Therefore, e-commerce merchants must be capable of accepting such payment methods. Unfortunately, cyber-criminals have found ways to steal personal information found on credit cards and debit cards and fraudulently use this information to purchase products and services which costs merchants lost revenue and fees for chargebacks. This article discusses the process by which credit card payments are processed beginning with the e-commerce merchant's web site to a credit card processor or service gateway to the credit card company's network to the issuing bank's network with an accept or decline response being returned to the merchant's shopping cart system via the same networks. The article addresses the issue of credit card fraud in terms of how the cyber-criminals function and the potential solutions used to deter these attempts by the cybercriminals. A list of preventive measures that should be used by e-commerce merchants is provided.

I. Introduction

Accepting credit cards is essential for any e-commerce Web site. Processing credit cards over the Internet is one of the fastest growing segments of transactions today. Consumers in the United States spend nearly 1 trillion dollars each year using a credit card over the internet (Woolsey and Schulz, 2009). This type of transaction or "card-not-present" transaction requires a special type of merchant account. In the early days of credit card usage, to accept credit cards, a merchant needed a merchant account through a bank. But today there are a number of services, generally referred to as credit card processors or merchant account services, which will let a merchant accept credit card payments online without their own merchant account. There are actually three different methods for processing credit card payments using a merchant account service. These are:

1. Real-Time Processing

Real-time processing allows e-commerce merchants to link their e-commerce shopping cart with a gateway merchant service which will automatically process credit card payments.

2. Virtual Terminal (Online Interface)

An e-commerce merchant can also process credit card transactions, manually, 24 hours a day by logging in online and submitting a secure form through a merchant account interface. A merchant can use this to process credit card payments while taking the customer's information over the phone if the merchant is able to access the Internet at high speed while talking to the customer.

3. Automated Recurring Billing (ARB)

Some e-commerce merchant services need to charge customers on a monthly or account threshold basis. Some merchant account services allow the merchant to set the time interval or account threshold level and some services allow a merchant to upload multiple subscriptions using a batch file like Microsoft Excel.

PayPal is generally accepted as the most widely used online merchant account service with more than 150 million users across the world. VeriSign operates a competing service called Payflow that is typically used by merchants with a high volume of transactions each month. Although the number of merchant account service providers continues to increase, some of the more popular one are listed and Figure1 below (TopTenReviews, 2009):

- Flagship Merchant Services
- MerchantWarehouse
- goMerchant Merchant Accounts
- Chase Paymentech
- The Transaction Group
- Merchant Accounts Express
- First Date
- Electronic Transfer Inc.
- Charge
- Free AuthNet

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
	Flagship Merchant Services	Merchant Warehouse	goMerchant Accounts	Chase Paymentech	The Transaction Group	Merchant Accounts Express	First Date	Electronic Transfer Inc.	Charge	Free AuthNet
	★★★★ Excellent	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good	★★★★ Very Good

Figure 1. 2009 Credit card processing review comparisons (TopTenReviews, 2009).

Companies that sell merchandise and services over the Internet are referred to as e-tailers or e-commerce merchants. These credit card processing services make it easy for e-tailers to start accepting credit cards for purchases of their products and services.

II. The Players in On-Line Credit Card Purchases?

Consumers and Merchants

The consumer is an individual or organization that has the intent of making a purchase. They have money or credit and they desire goods and services. The merchant is the one with the goods and services and is looking to sell them to consumers. The consumer can be motivated to select a particular merchant by things such as price, service, selection or preference. But the merchant’s primary motivation is to make money.

Issuing Bank

Consumers get their credit cards from a bank or credit union, called the “issuing bank.” Sometimes an issuing bank is simply called an “issuer.” An issuing bank may not just be associated with major credit card brands such as American Express, MasterCard and Visa, but also with credit cards called “private label credit cards.” These are the ones that department stores or shops offer, such as Sears and Target cards. Issuing banks are lending institutions that support these credit cards by granting and managing extended credit. Some examples of these are Bank of America, Citibank, MBNA, Household Financial, GE and Wells Fargo. The purpose of the issuing bank is to grant

credit directly to a consumer. The issuing bank is the one that decides what a consumer's credit limit is, based on credit history and current debt load. Issuing banks make money on the interest the consumer pays on outstanding balances from previous purchases, and they get a portion of every purchase a consumer makes with the card from a merchant.

Acquiring Bank

The acquiring bank represents the e-commerce merchant. The acquiring bank processes all of the merchant's credit card payments with the associations (American Express, MasterCard, Visa, etc.), and provide the merchant with reconciliation data and tools. The acquiring bank also makes money on every transaction a merchant processes. There are many acquiring banks in the United States and abroad, and merchants are free to move from one acquirer to another. Merchants typically select their acquiring bank based on the amount of money, called basis points, they charge per transaction.

Payment Processors and Gateway Services

Theoretically, e-commerce merchants can connect directly to their acquiring bank, but there are a number of reasons why they may not want, or be able to. There are technical and business requirements in conducting the payment process for credit cards and most merchants don't want to have to deal with these requirements. As an alternative, they use a third party to process credit card payments for them and their acquiring banks. These third parties are called payment processors and gateway services. Credit card payment processors offer the physical infrastructure for the merchant to communicate with the acquiring banks and the credit card associations. They connect all the credit card payment players together. This permits even very small banks to offer merchant services that they could not provide by themselves. Payment processors make their money by charging a flat transaction fee or by charging basis points to the merchant.

Gateway services provide merchants physical infrastructure as well. They generally offer technology and integration services among all the players. The gateway service providers charge the merchant a transaction fee or basis points for their services. These fees are in addition to the payment processor fees the merchant is already paying.

Credit Card Associations

The card associations such as Visa, MasterCard International, American Express, Discover, etc. are responsible for establishing the procedures and policies for how transactions, services and disputes are to be handled. They are bound by national banking laws and provide the money that covers some of the fraud that occurs within their membership. Each of the credit card associations operate somewhat differently and even within the same association they may operate differently in different parts of the world. Each of these credit card associations has their own network of systems, policies for use and payment processing. Each of these associations develops fraud-prevention tools and attempt to get merchants to utilize them.

III. How the On-line Credit Card Payment Process Works

When a merchant makes a sale over the internet; the card number, the amount of the sale, and the merchant identification (ID) are transmitted from the merchant's establishment or the internet Web site over the credit card processor's computer network. The credit card processor can either be a bank or a merchant account service company called a credit card processor that does nothing but provide credit card processing services as discussed above (Quick Start GA Dept. of Technical and Adult Education, 1996).

From the credit card processor's network the transaction goes to the credit card company's computer network. If the customer is using MasterCard, for example, the transaction will go to MasterCard's computer network. Then, the electronic transaction is sent to the bank that issued the credit card to the customer. The bank's computer system then checks the account and verifies that the customer has adequate credit to cover the purchase. The bank's computer system then sends the merchant an authorization over the network. Although the sale is complete, the transaction is not complete since no actual money has been exchanged.

At the end of the business day the merchant account service (credit card processor) sends that day's charges to the credit card network, e.g. MasterCard, for processing. The transactions travel via the merchant's credit card processor service to the credit card network, e.g. MasterCard. Individual transactions are then stripped out and sent back to the individual cardholders' banks. Banks then debit cardholders' accounts and make appropriate payments to the merchant's credit card processor through the Federal Reserve Bank's Automated Clearing House. The credit card processor then credits the merchant's bank account for the transaction amount, minus its fees for the transaction. Those fees also go toward paying transaction fees to the issuing bank and the credit card network.

Opening a Merchant Account

In order to accept credit cards, a merchant can open a merchant account with a bank. However, many banks have gotten out of the credit card processing business, and those that remain are often reluctant to service small businesses, particularly ones with limited operating histories. Many small businesses must therefore go through a specialized credit card processor or an independent sales organization, commonly referred to as an "ISO." Whether a merchant uses a bank or a credit card processor, they need a merchant account to accept credit card payments. An ISO or an Independent Sales Organization is an entity that acts more or less as a middle man, helping formulate a Bank or Bank/Processor alliance. Within such an arrangement, an ISO has an agreement to sell the services of the Bank or Bank/Processor alliance, and is allowed to mark up the Fees and sign up merchants. Most merchants buy their processing services from an ISO and the ISOs buy their processing services from a backend processor.

IV. Technology Requirements for Processing Credit Cards on Web Sites

The following are considered to be the technology requirements and best practices for e-commerce Web Sites that accept credit card payments (Authorize.com, 2009).

Create a Secure Payment Site. This is needed to protect credit card data and other sensitive information from hackers during the credit card transaction process. Identity theft and credit card fraud are occurring more frequently on the Internet, and merchants must ensure that their customers are protected from internet criminals

Develop a compatible shopping cart application. Make sure the merchant's shopping cart application can "talk to" the merchant's credit card payment-processing gateway. There are several of different types of payment gateways, and each one has a specific set of standards. Many free shopping cart applications do not support all of the available payment gateways. If a merchant would rather not install shopping cart software, there are a number of third-party options available. When a merchant utilizes third-party shopping cart software, the merchant must place a link on his web site. This link takes customers to the merchant's offsite shopping cart software.

Provide E-mail Message Encryption. If a merchant plans on accepting orders and sending or receiving credit card information via email, the merchant will need to encrypt the information that is sent. PGP, which stands for "Pretty Good Privacy," is the most common form of email encryption and it is required at the sending and receiving end. Utilize a Firewall. If a merchant stores customer data or credit card numbers on his server, it is necessary to have a site-wide firewall to protect this information.

V. How Credit Cards Payments are Accepted and Processed Online

If most of a merchant's business is conducted on the Internet, Real-Time processing is the appropriate solution. When a customer who is using a merchant's Web site is finished shopping and is ready to pay, typically the customer simply clicks on a "Check Out" button which is a link to a secure page where the customer types in their credit card information. After a few seconds, a message will then appear showing whether the credit card has been accepted or declined. Two days later the money will be transferred into the merchant's business checking account. Most Real-Time solutions are coupled with a "Virtual Terminal" that allows a merchant to process Mail Order/Telephone Order (MOTO) orders manually via a web browser from any location that has access to the Internet.

The steps below illustrate how credit card transactions are typically processed using a Real-Time credit card processing service (Smith, 2009; Murdock, 2006):

1. Using the merchant's shopping cart Web interface, the customer selects "check out" with the items they placed into their shopping cart or selected from an order form on a merchant's Website.
2. The customer then selects "credit card" as their method of payment.
3. The customer's Web browser then connects to the Merchant's website host's secure server, and brings up the secure payment form.
4. The customer enters in his or her credit card information on the secure payment form, and authorizes the transaction by clicking a "Complete Order" or "Continue" type of button.
5. The credit card transaction information is transmitted to the Website host's secure server using SSL encryption.
6. The merchant's secure server connects to the merchant's processing bank either via a secure payment gateway (a third party which provides the connection to the processing bank), or directly (some credit card processors have their own proprietary secure payment gateway and therefore do not require a third party to provide this service).
7. The credit card processor service polls the credit card network, such as Visa or MasterCard, directly, and the validity of the card and availability of funds is confirmed.
8. If the credit card transaction is approved, an authorization code is returned to the credit card processor service, or to the Secure Payment Gateway from the credit card network.
9. The authorization is encrypted by the Payment Gateway or credit card processor and transmitted in encrypted form to the secure Web server of the merchant, which permits fulfillment of the order.
10. The merchant's secure Web server then sends the customer's Web browser a confirmation receipt.
11. The amount due for the credit card transaction is moved from the card holder's bank to the merchant's credit card processing bank. The merchant's credit card processing bank transfers the money to the merchant's local bank within 2 to 3 business days.

Figure 2, below, illustrates the technological components of a typical credit card processing system.

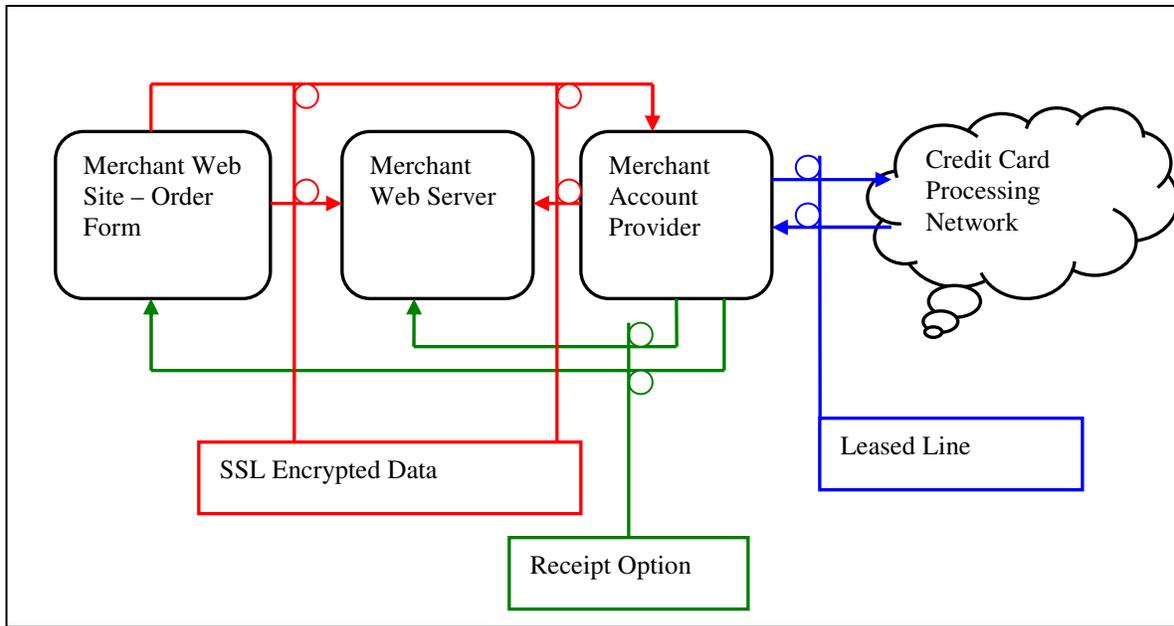


Figure 1. Typical Credit Card Processing System

VI. Minimizing Internet Credit Card Fraud

Payment gateways in the US have developed sophisticated fraud checking, but it has not halted credit card fraud. To protect themselves, merchants can capture IP addresses of purchasers (tell them that they are doing so), carefully examine purchases made from free e-mail addresses, those with different shipping and billing addresses, bounced e-mail order confirmations, no-existent telephone numbers, and large middle-of-the-night transactions. Merchants must also be cautious about shipping to Eastern European countries with a history of fraudulent transactions and telephone the buyer before shipping high ticket items.

Fraud Solution Approaches

While there does not appear to be any simple solutions, experts believe that potential cyber-criminals will soon begin to reconsider committing credit card fraud. This type of activity has, for a long time, been considered too small to bother with, but using credit cards fraudulently is quickly becoming "identity theft" -- which was recently defined as a serious federal felony. Cyber-criminals do leave digital fingerprints and can get caught. There are a number of approaches used by criminals to commit credit card fraud and there are a number of procedures implemented to deter their attempts at credit card fraud. These are discussed below.

Security codes

An important Internet security feature that now appears on the back of most Visa/MasterCard and Discover cards, and on the front of American Express cards is security code. This code is a three or four-digit number which provides a cryptographic check of the information embossed on the card. The security code helps validate that the customer placing the online order actually has the credit card in his/her possession, and that the credit/debit card account is legitimate. The security code is only printed on the card and it is not contained in the magnetic stripe information nor does it appear on sales receipts or billing statements. The goal is to make certain that the customer must have the card in his/her possession in order to use this code. Since Card Security Codes are not scanned into standard credit card readers, in theory, these numbers are only visible to the customer.

Credit Card "Skimming"

Criminal gangs recruit individuals who work within restaurants, hotels and retail outlets. The recruits are given battery powered electronic devices known as "skimmers" that read and capture all of the credit or debit card's details in the few seconds that it takes to swipe the card through the credit card reader machine. When customers pay their bill, their card is first swiped through the legitimate credit card machine, but then it is also swiped through the "skimmer" reader. The recruits then pass the "skimmer" machines onto counterfeiters, who pay the recruits for their part in the crime. Once the "skimmer" machines have been given to the counterfeiters, they download the information onto a computer and produce a fake clone of the credit card. The "cloned" card is embossed with the details of the victim's credit card and passed on to gang members who may sell it for between \$400 and \$700, depending on the perceived credit limit (Fraud Guides, 2009).

Skimming Prevention

1. Subscribe to stolen credit card checking systems
2. Verify the address
3. Verify the telephone number
4. Call the credit card issuing bank
5. Examine the email address - hotmail and yahoo mail can be easily faked
6. Call the cardholder
7. Be cautious of bulk orders
8. Shipping and billing address should match
9. Single-use credit card numbers
10. Smart Cards

Single Use Credit Card Numbers

Some credit card companies have a new security and privacy offering which utilizes the concept of disposable credit card numbers. With this system, customers can get unique credit card numbers linked to their credit card account each time they make a purchase online.

Smart Card Technology for On-Line Purchasing

Newer "smart cards" are embedded with a computer chip containing a digital certificate. A digital certificate consists of basic information about your digital identity. It contains elementary personal information such as your individual or company name, your e-mail address and your digital signature. The digital signature is nothing more than a series of numbers called a public key which forms the basis of all encryption algorithms. Unlike a written signature, a digital signature has two functions: it not only authenticates who you are legally, it also allows your messages to be mathematically encoded.

Address Verification System (AVS)

E-commerce merchants can use an Address Verification System (AVS) for shoppers in the United States. This system takes the consumer's ZIP code and the numbers in the street address, and compares them with the numbers in the credit card billing address. If they agree, the transaction is authorized; if they do not, the transaction is flagged or perhaps not allowed, depending upon the merchant's preference.

Telephone Number Authentication

A Telephone Verification service can provide a decrease in the number of fraudulent transactions that pass through an on-line ecommerce web site. There are a number of services that will provide real time telephone number verification. These services can determine whether a telephone number is real, no longer in service, stolen or a legitimate working number at the address given by the user.

Telephone Verification

Telephone Verification works by automatically calling an online end-user's telephone number at the same time the end-user is making a transaction on a website. The user while on the website answers the phone and is provided a one-time personal identification number (PIN) presented via the web interface; an otherwise anonymous online end-user will be able to confirm that the person who received the phone call and the person who is interacting on the website are the same person.

Customer Transaction Databases Checks

Another approach for detecting online fraud is to compare a transaction with previous transactions made for a given credit card number and make sure it fits the pattern of use. There are companies that provide real time checks of credit cards with databases of millions and, in some cases billions, of records to detect anomalies.

VII. Conclusion

Based on past performance and predictions for the future, it seems safe to say that purchasing goods and services over the internet will continue to increase. This is because it is more efficient for the merchants and they can reach a much larger audience than using the face-to-face, in-store methods of the past. But like most uses of technology, there are individuals who find ways to use the technology for criminal purposes. This has been the case when utilizing credit or debit cards for purchasing goods and services over the internet. The process by which credit card payments are processed beginning with the e-commerce merchant's web site to a credit card processor or service gateway to the credit card company's network to the issuing bank's network with an accept or decline response being returned to the merchant's shopping cart system via the same networks is discussed. The issue of credit card fraud in terms of how the cyber-criminals function and the potential solutions used to deter these attempts by the cybercriminals are addressed. A list of preventive measures that should be used by e-commerce merchants is provided.

References

1. Authorize.com (2009). Security Best Practices (2009). Retrieved January 21, 2009 from Web Site: http://www.authorize.net/upload/images/Files/White%20Papers/Security_0604.pdf
2. Fraud Guides (2009). Credit Card Skimming. Jan. 2009 From Web Site: <http://www.fraudguides.com/business-credit-card-skimming.asp>
3. Murdock, Kerry (2006). Credit Card Processing: How It All Works. Retrieved January 21, 2009 from Web Site: <http://www.practicalecommerce.com/articles/168-Credit-Card-Processing-How-It-All-Works>
4. Quick Start GA Dept. of Technical and Adult Education (Editor) (1996). Credit Card Processing Overview, GA Dept of Tech & Adult Education, Quick Start, 1996.
5. Smith, Robert (2009). How Credit Card Processing Works. Review. Retrieved January 21, 2009 from Web Site: <http://www.smithfam.com/news/nov99d.html>
6. TopTenReviews (2009). Credit Card Processing Services Review (2009). Retrieved January 21, 2009 from Web Site: <http://credit-card-processing-review.toptenreviews.com/>
7. Woolsey, Ben and Schulz, Matt (2009). Credit Card Industry Facts, Debt Statistics 2006-2009. Retrieved January 12, 2009 from Web Site: <http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php>