10 Measures to Reduce Credit Card Fraud for Internet Merchants

FRAUDLABS - PREVENTING CREDIT CARD FRAUD

Introduction

During the last few years there has been an increase in online fraud of global scope and geometrically increasing proportions. There are now actual companies that specialize in spam and other illegal marketing techniques, like Phishing and Hacking, that take every opportunity to make a few pennies. Even though their net income per person is miniscule, it becomes significant when multiplied by hundreds of thousands or even millions. Added to this threat are the man amateur fraud artists around the world who troll the Internet for credit card and financial information to use for fraudulent purposes. Finally, identity thieves are reaping high rewards at the expense of both the target and the online retailer.

Credit card fraud on the Internet has reached gigantic proportions, and the merchants providing goods and services over the net are suffering tremendous losses through chargebacks from the financial institutions who serve the targeted credit card holders. Merchants who offer a product or service online have to take the risk of losing the cost of the product sold online, plus the added cost of chargeback fees, and they even face the possibility of having their merchant account terminated by the financial institutions serving them. While this cost can ultimately be passed on to the consumer, the development of this environment hurts business as a whole, and particularly hurts the small business owner. The Cybersource® Online Fraud Report showed Internet fraud had cost merchants $2.6 billion, or 1.8% of total online revenues, in 2004.

The purpose of this document is to introduce ***10 preventative measures*** that merchants can take in order to minimize credit card fraud. In addition, we would like to take this opportunity to introduce a complete suite of FraudLabs™ Web Services specializing in the analysis of credit card fraud risk for Internet merchants.

1. Geolocation by IP address

In the world of e-commerce, knowing the online buyers geographic information can help to prevent fraud. Geolocation technology provides the absolute geographic location by IP address of the computer from which the order is made in real-time e-commerce transactions, which can identify locations where the probability of fraud is the highest.

Geolocation by IP address can identify the user's exact location or calculate the distance between billing address of online buyers and actual location of persons entering the orders. As a result, it allows the merchants to apply additional authentication measures or identification for those transactions which show a great difference of distance. As a result, Geolocation technology delivers data that helps merchants determine which transactions to review and which to allow. This creates a beneficial balance between the risk of fraud losses and that of blocking legitimate customers. Legitimate customers will actually welcome legitimate authentication measures, which will protect them from credit card fraud also and keep the costs of doing business on the Internet down, especially if the customer is properly informed and advised by the merchant of these protection measures. Using a service such as that provided by FraudLabs™ can keep the cost of authentication down as you can target the authentication toward the most probably geographic locations for fraud.

2. Comparison of the IP address country with the billing address country

An IP address is a unique network identifier issued by an Internet Service Provider to a user's computer every time they are logged on to the Internet. Make sure the IP address country and the billing address country are the same. By using fraud detection web services like FraudLabs™, you can detect the IP address country for the customers that are placing the orders. If the customers billing and shipping addresses are in the US, but the person placing the order is logged in from an IP in Russia, this will require closer scrutiny, and will often trigger anti-fraud precautions. Although this situation could be legitimate, but it's probably worth a phone call to the customer's US phone number or other measures to confirm the order and the identity of the credit card user.

3. Check whether the country is a "high risk" country

Always require closer inspection for orders that being shipped to an international address. Pay more attention if the card or the shipping address is in an area prone to credit card fraud. According to a ClearCommerce® survey, the top 12 international sources for online fraud are Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Turkey, Russia, Pakistan, Malaysia, and Israel. The same survey also showed that the 12 countries with the lowest fraud rates are Austria, New Zealand, Taiwan, Norway, Spain, Japan, Switzerland, South Africa, Hong Kong, the UK, France, and Australia. FraudLabs™ IP Geolocation service can identify the country of origin for businesses who need this information. While the fact that an order originates or is being delivered to one of the high risk countries is not, in itself, an indication of fraud, nor is the indication that the order originates in a low risk country any guarantee of its legitimacy, the trends and statistics are there, and merchants must use information about the origin and delivery addresses as a guide to how much authentication they should require from customers.

4. Check whether a free or anonymous e-mail address was used

Be aware that online buyers using free anonymous e-mail providers such as hotmail.com or yahoo.com are virtually untraceable. There is a much higher incidence of fraud coming from free email services than from paid service providers. Virtually everyone who has a free, web-based email address or forwarding address also has a traceable ISP address. While many legitimate customers use free email addresses, because they are convenient and economical. It is also true that most fraudsters use free email addresses in order to remain anonymous. However, most businesses purchasing a business product have their own domain names and even if they do not, they would not use a free email address. For these reasons, you need to have some way to get additional information when a free email address is used, such as the ability to locate the customer geographically when they place their order, so you will know which orders need further checking for authenticity. Keep an eye out for newly registered domain names. This is because fraudsters can register a new domain easily using the stolen credit card to pose as a new business entity. FraudLabs™ can provide the free email detection to help you make these decisions.

5. Check whether an anonymous proxy server was used to place the order

Anonymous proxy servers allow Internet users to hide their actual IP address. The main purpose using a proxy server is to remain anonymous or to avoid being detected. While well known businesses use this to protect internal networks, fraudsters hide themselves behind anonymous proxy servers. It is not easy to detect anonymous proxy servers because they appear and disappear from time to time. FraudLabs™ provides a hassle free method to keep the always up-to-date anonymous proxy server list as web service.

6. Check whether the mailing address is a mailbox or ship-forward service

Fraudsters prefer to stay untraceable but still need to collect physical merchandise. One way is to use a public P.O.Box, a private mailbox, or a drop shipment forwarding address as a temporary point of receiving. Never send merchandise to a public rented mailbox, a P.O. Box (except for those you identify as legitimate major companies by phoning their listed number), or shipping forwarder, because the actual location and identity of the receiver is undetectable.

7. Check whether the phone number is valid and located within the correct ZIP code

Often, merchant will discover orders with invalid zip codes or a mismatch between the zip code and area code will produce fraud rates that are significantly higher than usual. They may wish to apply more rigorous fraud prevention standards by verifying the validity of zip code and the area code. In addition, if the phone is identified as a V.O.I.P phone, offered by many services these days, a delay in shipment until the payment clears may be in order, especially for non-times sensitive items.

8. Compare the credit card issuing bank's country with the billing address country

Another key point to bear in mind is to check the issuing country and the billing address. Make sure the issuing country and billing address country are the same. This is especially important, because minor banks may not have rigorous identification procedures.

9. Call the credit card issuing bank to verify the validity of credit card

If online merchants have any suspicions about an order and need to confirm the details of the order, they can call the issuing bank and ask to confirm the general account details. This is to make sure that the card is not stolen. The issuing bank phone number is based on the first 6 digits of credit card number known as the Bank Identification Number (BIN).

10. Request more identification if in doubt

While consumers value their privacy and require quick web site ordering facilities, it is important to gather sufficient customer identity details during the ordering process. The customers' name, credit card number and expiry date is not enough. Merchants should call them for verification through phone or request a photo ID to be faxed if they have any doubts.

In Summary

Every merchant should aware of online credit card fraud, although it is something that can never be completely eliminated, but rather something that must be managed. One of the most important factors in controlling fraud is understanding the customer and implementing security measures that can adapt to the level of risk in each transaction. Applying fraud detection web services such as FraudLabs™ supplies in the order management can greatly reduce credit card fraud. This white paper focuses on preventative methods and procedures that merchants can perform in order to limit credit card fraud.

For more information about the FraudLabs™ Credit Card Fraud Detection Web Service, please visit http://www.fraudlabs.com or email sales@fraudlabs.com.