

Credit Card Fraud Prevention Using ASP and COM Technology

Hexa Software Development Center

Knowledge Service Group
NP 3D-27-04, Jalan Batu Uban,
11700 Gelugor,
Pulau Pinang, Malaysia.
URL: <http://www.ip2location.com>

{ sales@ip2location.com }

Credit card fraud has become pervasive on the Internet. According to MasterCard International, account takeover fraud has increased by 369% since 1995. It has become one of the fastest growing types of fraud, and one of the more difficult to combat. More than \$700 million in online sales were lost to fraud in 2001, representing 1.14 percent of total annual online sales of \$61.8 billion, according to GartnerG2. Even if the credit card company has given the authorization as to the validity of the card, there are several ways fraudulent cards can be used on your site. The card may have been lost or stolen, but the card owner is yet to report its loss. Or the number on the card (and not the card itself) may have been lifted without the knowledge of the owner. There is also a scam called identity theft, where the card has been issued under false pretenses using someone else's identity and data.

As an online merchant, you need to have a system to check the authenticity of orders placed to safeguard your business. While the effort may require additional time and money, it can save you the cost and stress caused by charge-backs for fraudulent orders. You lost your physical products; you lose the sale price; you lose another business opportunity; and you will be fined an additional \$15-\$50 charge-back fee. If you have a high percentage of charge-backs, your card services company can even blacklist you and cancel your merchant account. You will also spend time looking up the order and provide the requested information to your card services company. All of these hassles are things you can surely do without.

How can you protect your business from credit card frauds? Here are a few steps that can be taken to ensure that the transaction is being requested by the real cardholder.

Suspect shipping address.

According to ClearCommerce Corporation, a provider of payment processing and fraud protection software for e-commerce, orders from Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Turkey, Russia and Pakistan have a very high incidence of fraud, and often have unverifiable addresses.

Untraceable email address.

In many fraudulent orders, the customer's email address is often at one of the free email services, like hotmail.com and yahoo.com, which are relatively untraceable.

Expensive items.

Be wary of expensive orders, especially for expensive brand-name items.

Multiple items.

It can be a bad sign, for example, if someone orders three X-Box or three DVD players at once, especially where the items have a high resale value.

Express shipping.

Most fraudulent orders specify overnight or 1-day shipping without hesitation.

Shipping address differs from billing address.

Receiving point and billing address are different in fraud orders. If you are selling valuable items, it can be a good policy only to ship to the billing address of the card's holder.

Suspicious billing address.

The address looks too simple or invalid. If the billing address is 123 Main St, New York, the order is probably fraud. You can use or online location tool to see if the address can be verified.

Leave at door or post office box.

If the courier service cannot guarantee delivery of goods, the risk of fraud is very high.

The advancement of geo-targeting in the Internet allows us to pinpoint the geographical region for an order. The information can be used to reduce the fraud by verifying it with the billing address and delivery address. This method can identify the scenario where someone from country X has stolen the credit card data from country Y. The IP address lookup service will reveal the real country instead of relying on the country filled in the order form.

IP2Location™ provides technology to translate IP address to country origin. The lookup table is available in several formats such as database and COM. It is the perfect solution to automate the fraud detection using client side programming languages like C++ & Visual Basic; or service side programming languages like ASP, PHP, JSP and CFML.

For example, company XYZ received a credit-card order from IP address 161.139.12.3. The order details are as following:

Name: John Ma
Address: 123 Main St
City: New York
ZIP Code: 1111
Country: United States
Tel: (503) 111-1111
Credit Card No: 1234 5678 9012 3456
Expired Date: December 2010

Credit card merchant processor will authorize this order if the billing address matches the order details. Unluckily, the credit card data has been stolen earlier by Mr. ABC from another country through the Internet. Later, he made a purchase of digital products from company XYZ using the information. His order approved by the merchant because all the details matched John's record in the bank's database. IP2Location™ technology can filter the difference between order's country and record's country upfront to protect your business. You can classify this kind of order for manual inspection before delivering the goods. You will be surprise how much this method will help in identifying fraud orders.

For the implementation, we use a fully functional IP2Location™ ActiveX component available at <http://www.ip2location.com/ip2location-country.zip> to query country by visitor's IP address. The unregistered version has a 5-second delay in each query.

First, install the ActiveX component in IIS web server. It could be as simple as running a command in DOS prompt.

```
C:\> regsvr32 ip2location.dll
```

We create a script to compare the lookup country and data given in the order authorization flow. It serves as a filter to reduce fraud. All rejected orders will be manual verify by merchants.

verify.asp

```
<%
    ' Country info filled in the form (US is only an example)
    BillingCountry = "US"

    ' Create server-side object
    Set ipObj = Server.CreateObject("IP2Location.Country")

    ' Initialize IP2Location object
    If ipObj.Initialize("demo") <> "OK" Then
        response.write "IP2Location Initialization Failed."
    End If

    ' Get visitor's IP address
    IPAddr = Request.ServerVariables("REMOTE_ADDR")

    ' Detect visitor's country of origin by IP address
    CountryName = ipObj.LookUpShortName(IPAddr)

    ' Free IP2Location object
    Set ipObj = nothing

    If CountryName = BillingCountry Then
        ' IP address originates from country in billing address
        ' Low Fraud Risk
    Else
        ' IP address different from country in billing address
        ' High Fraud Risk
    End If
%>
```