



Geolocation - Knowing Your Enemy Detecting Card-Not-Present Fraud

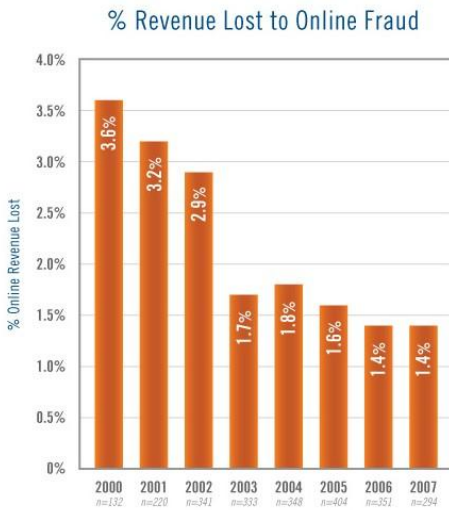
November 2008
Neustar Product Marketing

Geolocation – Knowing Your Enemy

Contents

Knowing Your Enemy	3
Online Credit Card Fraud: Every e-Merchant at Risk	4
How Geolocation Works: Five Ways to Detect Fraud, and Real-Life Examples of Geolocation in Action	4
Winning the Battle	7
About Neustar, Inc.	7

Geolocation - Knowing Your Enemy



© CyberSource Corporation, all rights reserved.

Knowing Your Enemy

Knowing your enemy is the start to fighting any battle. Online, the e-merchant's enemy is anyone out to order goods or services with stolen credit card numbers or to hack into a customer's account.

Take the real-life case of an online electronics merchant. In one day this East Coast merchant received orders for nearly \$500,000 in high-end 42-inch plasma televisions. A banner day perhaps? It looked that way at first glance. All of the orders were charged to different card numbers, different names, and different billing and shipping addresses. Everything there checked out. However, due to the unusual volume, the merchant's risk monitoring system flagged the orders for manual review. Each of the seemingly different orders was sent from the same time zone from a computer that was using Russian as its browser language setting. It could be a coincidence, albeit an unusual one. The chance of different customers all speaking Russian, all in the same time zone, all wanting 42-inch plasma TVs was getting slim. Then came the clincher. He checked the IP addresses, a unique number assigned to a particular computer or device to route messages. All of the orders came from the same IP address, even though the billing and shipping

address for each order was different.

This was no banner day, and had it not been for this merchant's geolocation service he'd have shipped out thousands of dollars worth of plasmas with little hope of ever seeing the money, or those products, again.

Knowing where your Web visitors are located is becoming increasingly important for online businesses to allow them to make real-time business decisions to prevent fraud, comply with regulations, manage digital content, execute localized marketing strategies and protect themselves from online attack. This report provides an overview of the actions online fraudsters are taking that hurt e-merchants and their customers, and outlines how geolocation has been established as one of the most effective tools for identifying fraudulent online activity.

Disclosures: This report, sponsored by IP geolocation provider Neustar, Inc., illustrates how companies are using geolocation to help detect card-not-present fraud, and includes information gathered from industry experts and Neustar customers. All charts are from 2008 Edition of the "Online Fraud Report" produced by CyberSource Corporation, a Neustar solution partner.

Geolocation - Knowing Your Enemy

Online Credit Card Fraud: Every e-Merchant at Risk

The results are in from the Ninth Annual 2008 Edition of the “Online Fraud Report” from CyberSource, a leading provider of electronic payment, risk and security management solutions. With 318 online sellers surveyed—from basement-run e-commerce start-ups to the largest e-retailers and digital distribution entities in the world—the report shows an average 1.4 percent of their orders lost to online fraud. The fraud often came from buyers who used credit card numbers later identified as stolen. Your enterprise is likely no different.

“We estimate that in 2007 \$3.6 billion in online revenues were lost to fraud,” says Doug Schwegman, director of customer and market intelligence for CyberSource Corporation. “And that’s only part of the problem. In that same year, U.S. and Canadian merchants rejected, on average, 4.2 percent of their orders on suspicion of fraud. You can be sure there were some valid orders in that group of rejects, representing significant additional lost revenue. For orders originating outside the U.S. and Canada, the percent of orders rejected on suspicion of fraud was 2.5 times higher.”

Many fraudulent transactions are caught these days, thanks to a wide variety of powerful detection tools. “The key thing we say to e-merchants is that no one tool is a silver bullet,” Schwegman says. “Merchants need to employ a whole arsenal of tools. The day of teenage fraudsters is largely over. The bad guys do this as a full-time job now and they’ve become sophisticated. We need to be more sophisticated to defeat them.”

Though geolocation is just one of the risk monitoring tools used (the average e-merchant online uses at least four tools), it provides an important line of defense. The geographic location of a proposed transaction can be a significant indicator of potential fraud, particularly when that location doesn’t match the physical address provided by the customer. In the physical

world, a bank credit card application listing a U.S. home address that arrives in an envelope with a Ukraine postmark would undoubtedly cause concern in the credit office. An attempted online purchase presenting a similar contradiction should raise a similar alarm: Experian research into identity fraud trends has determined that when a customer provides a registration address in one U.S. state but actually places the order from another, this is a predictive indicator of fraud. Transactions across national borders raise the red flag higher yet. International transactions represent nearly half of all credit-card chargebacks, and a short list of nations (Ghana, Vietnam and Lebanon among them) produces the most fraudulent transactions.

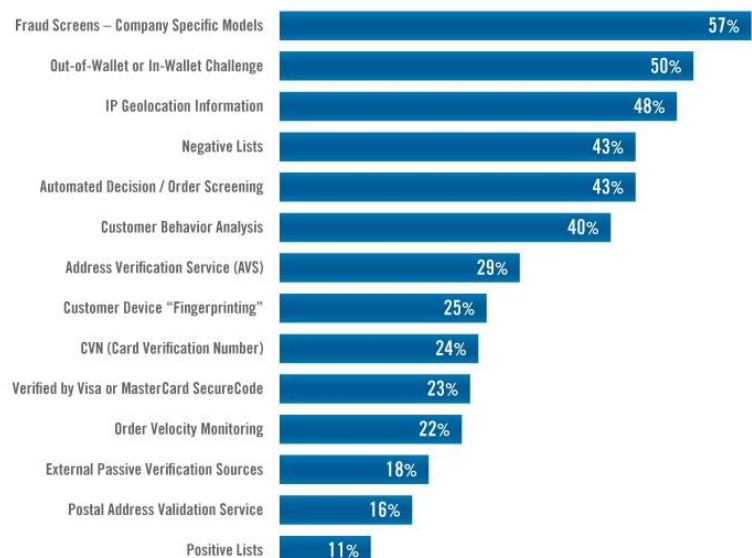
“In the world of fraud prevention we really just need to know where you are,” says the fraud project manager for a large Web portal and search engine site, a long-term user of Neustar’s geolocation service. “That’s been a critical tool.”

Knowing the level of risk, e-merchants can use geolocation to flag suspect transactions and address them individually. Where the risk from a particular location is extreme, that location can be blocked to all access—a step most enterprises hesitate to take because of the risk of blocking legitimate customers—often referred to as “false positives.” In light of the highly-publicized losses suffered by some online financial providers, however, the effort to address fraud risk serves not only to protect the enterprise’s bottom line but also to build consumers’ trust that the merchant is doing everything possible to keep fraudsters from using stolen credit cards.

How Geolocation Works: Five Ways to Detect Fraud, and Real-Life Examples of Geolocation in Action

None of the online fraud protections tools are failsafe. Each one, however, adds an extra layer of protection for e-merchants faced with potential fraud, and each one is bolstered by knowing a few e-merchant tricks of the trade.

Most Effective Fraud Management Tools
% of Merchants who selected tool as one of their three most effective*



© CyberSource Corporation, all rights reserved.

Geolocation - Knowing Your Enemy

“There’s a misconception that if you know where the IP address is, then you know where the user is,” says Kevin Ryan, Director of Client Solutions for Neustar, Inc., which uses IP addresses as part of its geolocation process. “But the user’s location can actually vary quite a bit.”

There are many ways that shoppers can connect to an e-commerce Website, from WiFi hotspots to home computers to laptops on the road. Each access method provides its own set of challenges in determining exactly where the shopper is coming from. When it comes to geolocation, e-merchants with the highest fraud-detection rates start with five key areas where fraudulent orders are likely to be caught.

Check for anonymous proxy servers and other location-masking systems: Proxy servers route communications between your computer and the Internet. While not all proxy servers are bad, the use of an anonymous proxy that hides or masks your unique IP address can be a fraud indicator. To use an anonymous proxy, a Web visitor would first connect to a server or Website like Anonymizer.com (where users pay \$19.99 to \$99.99 per month) or shopping-compatible free services like Proxify.com or The-Cloak.com before surfing the Net. This disguises his IP address by substituting the anonymizer’s own location IP instead.

Often this is done legitimately, by citizens concerned about maintaining their privacy or who wish to avoid cookies and scripts while on the Internet. These customers do miss out on the advantages of localized content, easier log-ins and personalized Web pages, but for many it’s an acceptable trade off. At other times it’s done by shoppers who want to circumvent their work or home browser connections, to keep their orders private from the company or their family members. Many high school students use anonymous proxies these days to get around the school filters placed on Facebook and YouTube. Too often, however, it’s done by predators and fraudsters trying to avoid detection.

“There are so many ways to spoof your IP address, either anonymous or paid for,” says the search-engine site fraud manager. “As such, it pays to take advantage of a geolocation provider’s anonymous proxy lists,” he says.

Lists of anonymous proxies that are abusing the system, provided by a select few geolocation vendors, notify the e-merchant when an order comes from one of the proxy servers. E-merchants using Neustar’s Gold GeoPoint Data Editions service, for example, can program their shopping cart software to decline or review orders forwarded by anonymous proxies.

Meanwhile, some shoppers may have their location masked through no real fault of their own. Orders placed with cell phones or mobile devices can be difficult to trace. “What you need to locate a non-GPS cell phone is access to the cell tower information,” says Ryan at Neustar. To fill the gap, several geolocation providers, including Neustar, partner with virtual-GPS providers like Mexens Technology, whose Navizon application tracks WiFi and cell tower positioning. “Through Navizon there’s the ability for merchants to get access to a large and growing database of WiFi and cell access points around the globe,” Ryan says. “We are able to ascertain the location of a handset by using either a small snippet of code inserted by the handset provider or an application running on top.”

That’s something e-merchants are excited about: “We’ve demoed some really wild technology using cell phones and pinpointing locations,” says the search engine site fraud manager. “Neustar is offering lots of additional features that definitely move the bar up, and keep their competitors on the edge.”

Dial-up connections present a different challenge. Orders placed with a dial-up Internet connection are first routed through the dial-up provider’s server first before hitting the merchant’s site. So an EarthLink user traveling in London, but using dial-up to connect with his California-based Internet Service Provider (ISP), will appear as if he is

in California —not 6,000 miles away.

WHITE PAPER

AOL's customers are also an exception, because AOL uses a central server, most AOL customers appear to be connecting from Herndon, Virginia, where a main AOL server is based (although this issue has become almost non-existent as AOL continues to lose AOL browser customers). "For many, dial-up is a way to communicate from the other side of the world while pretending to be local," Ryan says. Dial-up carriers are getting more sophisticated, however and many now show at least general area-code-based identifiers for their users.

Servers like these that mask the location, present a challenge for e-merchants using geolocation, but it's not insurmountable. Some merchants place business rules in their cart application to deny any orders from shoppers that aren't on fixed high-speed Internet lines. However, this strategy also eliminates many legitimate shoppers.

In order to improve acceptance rates, other merchants are opting to flag the orders from non-fixed Internet connections, as determined by geolocation, for manual risk review. If a distinct pattern for fraudulent orders is seen, only then will certain types of connections be allowed.

Check the distance between actual and expected user locations: It's a general rule of thumb that shoppers will be logging on the Internet within close proximity to their billing or shipping addresses. Geolocation provides an easy way to verify the customer's true location.

E-merchants using geolocation can also review the postal code and the latitude and longitude associated with the shopper's IP address. This information can be

cross-checked, not only against the order information provided by the shopper,

such as their billing and shipping address, but also against that users' previous sessions or registration information, to come up with a distance between the actual and expected location of the person placing that online order. Many Neustar customers report that orders coming from 500 miles or more away from the expected location have

Geolocation - Knowing Your Enemy

a higher probability of being fraudulent. With geolocation, e-merchants can elect to decline, or flag for review, orders falling X miles or more away from the shipping or billing address.

Here's how one Neustar customer, an online travel reservation site closing nearly \$1 billion in sales per year, does it: "Our fraud system sits outside of our purchase path," says its director of ecommerce risk and revenue. "We catch IP addresses at the purchase; we query the Neustar database for the geolocation of that IP address, and then factor that into the risk score. Every day we see mismatches of credit card billing addresses compared to where their IP address is located; it's a great indicator of fraud."

Use domain information to assess risk: Most geolocation data providers will provide the e-merchant with domain information gathered from the shopper's ISP, and will use this additional information to determine whether an order should be declined, accepted or flagged. For example, an order placed on a work computer and passed through the company's server will be tagged with the company's Website address, such as IBM.com. An order placed from a government office will come tagged with a .gov or .mil extension. An order placed by a consumer at home using an ISP, such as Comcast or British Telecom, will have a @comcast or @BT domain address. An e-merchant may also track user sessions and know that the customer frequently connects from work and from home. "For consumer and small business traffic, for home search connections, you will typically see just the email provider's information, such as johnsmith@cox.net. For larger businesses, in addition to the company domain name, you will, among other things, typically see the company information as part of the email domain name, such as IBM.com, and in the geolocation connection data provided you will probably see a higher speed connection such as an OCX or T1 or higher connection, says Ryan" Work domains can also confirm that a request for shipping to that work location is legitimate.

Though some domains can be used to confirm a shopper's identity, other domains can raise red flags. For example, fraud often can be tracked to university servers, where anyone who has registered for a class—even distant learners or drop-outs—can get a free .edu address in the U.S. or a free ac.uk address in the United Kingdom. High fraud rates also have been tracked to copy center servers with rentable computer time, such as Kinkos.com. "There are potential risks associated with some of these," Ryan says. "Depending on your business and the type of product you sell, some domains might be a bit more risky than others. For example, copy centers that rent out server time, like Kinkos.com, may be cause for concern for an e-merchant selling high-ticket items like enterprise hardware, but not for a merchant selling low-priced consumer items like CDs and books. A consumer using a rented computer to place an order for a CD makes sense, but why would someone use a rented computer to place an order for enterprise hardware?" With geolocation, the merchant can take that information and program their shopping cart system to decline or flag orders with the .edu, "copycenter".com or other problematic domain extensions.

Build user profiles: Geolocation provides a simple way for merchants to expand their user profiles behind the scenes. "We use it to compare where that consumer is coming from, compared to the customer data entered such as: billing address and shipping address," says the travel site's risk director. "It provides us with more consumer data to validate who the customer really is."

Geolocation data can be saved right alongside the information provided by shoppers at registration. Customer registrations can be tied to incoming domain extensions, IP addresses, latitude and longitude information, zip codes, even the amount of time a recognized user spends at the merchant's Website in the order process. Each time someone uses that shopper's account, the geolocation service enables a check to see if the connection is coming from the same location as where the legitimate shopper

was when he or she registered. Granted, the geolocation profile may change based upon Internet café use or traveling, but the system assumes that most valid orders will follow the same pattern. If several different domain extensions or ISPs are used in one day, chance are those orders may be fraudulent.

Once a profile is built, e-merchants can look for changes—differences between the observed behaviors they see online and what they have on file. "For example, if the user is still coming in from the same ISP but his or her location has suddenly changed by 50 miles, then this could be cause for concern," Ryan says. "And for fixed-routing-type systems, anyone outside of a 50 mile radius, generally considered as the largest metro area, could be an indication that the user has either physically moved from one home to another, switched jobs, or has had their credit card stolen or customer account broken into."

Some e-merchants are addressing this by creating user profiles for home, work and on-the-road, so valid orders will be automatically matched to these valid profiles. This helps to avoid many of what could be accidental declines. If a user has moved, it's a good practice for the e-merchant to initiate contact with the user to request and verify their new address or to hold the order until the new address is verified.

Use time-zone information to track the transaction "velocity": "If a user is connecting to a Website in relatively short periods of time and the log-ins are more than 1,000 miles away from each other, this is a major red flag," Ryan says. "Though it could be someone on the road, or sharing an account with their spouse or kids, it's also quite possible that someone has compromised that account."

For each shopper, e-merchants can use geolocation data to enable business rules that 1) request the current local time at the shopper's location; 2) alert them to potential "time-zone hopping" within a short period of time, where the same account is accessed from multiple geographic locations; and 3) alert them to orders placed at times of the

Geolocation - Knowing Your Enemy

day that aren't consistent with previous orders stored in the user's profile.

Some merchants take all of these scenarios, and create software systems that use geolocation data to detect even further fraud risks. Take one Neustar customer, a U.S. financial company offering online applications for private-label credit cards, personal loans, bank cards, and credit insurance. "The way we are using Neustar's geolocation data is very advanced; it has to be," says its fraud strategy manager. "It gives us a real competitive advantage in our Internet work."

Winning the Battle

It's not unusual for a Web site to keep track of user behavior, such as which pages they click on and which products they purchase. This is called behavioral targeting and some privacy experts are concerned it goes a bit too far. With geolocation the customer's computer is never accessed. Geolocation is about security—protecting both the consumer and the merchant from fraudulent activity. Thanks to geolocation, the merchant also often knows generally where to notify local law enforcement to catch the culprit in the act.

In the end, geolocation is "just one of many things you can check in the fraud cycle. It's just one of the things you have available," says the search engine site fraud manager. "But we use it, and we look at the fraud that gets through by reviewing the chargebacks (those credit card orders that are contested). Our fraud rate is pretty low—we're below 0.5 percent from a total company perspective."

About Neustar IP Intelligence

Neustar, Inc. enables online businesses to instantly identify where a visitor to their Web site is geographically located. Online companies, including broadcasters, e-retailers, ad networks, banks, and government agencies, integrate Neustar's IP geolocation data into their Web applications to geotarget their advertising and content, detect card-not-present fraud, manage distribution of digital content, comply with local laws, and more. Neustar delivers detailed demographic and network characteristic data about an IP address and the data is 99.9% accurate at the country level and up to 98.2% accurate at the US state level (attested to by Pricewaterhouse Coopers). <http://www.neustar.biz/ipintel>