

Using Location as a Weapon in the Fight against Card Not Present Fraud

By Kerry Langstaff, vice president of marketing, Quova, Inc.

Knowing your enemy is the start to fighting any battle. Online, the merchant's enemy is anyone who fraudulently orders goods or services either with stolen credit card numbers or by hacking into a customer's account.

The merchants surveyed in the CyberSource 2008 Online Fraud Report reported an average 1.4 % of their orders lost to online fraud, often resulting from buyers who used credit card numbers later identified as stolen. The report also said that U.S. and Canadian merchants rejected, on average, 4.2 percent of their orders on suspicion of fraud, probably eliminating many valid orders, which represents even more lost revenue.

Although these fraud statistics may seem daunting, many fraudulent transactions are caught these days thanks to a wide variety of powerful risk analysis tools. Merchants need to employ a whole arsenal of tools to fight this war, in fact, the average e-merchant uses at least four fraud detection tools.

The geographic location of a proposed transaction can be a significant indicator of potential fraud, particularly when that physical location doesn't match the credit card billing 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 charge backs, and a short list of nations (Ghana, Vietnam and Lebanon among them) produces the most fraudulent transactions.

Internet Protocol (IP) geolocation is just one of the risk monitoring tools used by merchants, but can provide an important line of defense. IP geolocation is a Web technology that can accurately identify the real-world geographic location of an Internet-connected device - the moment the user clicks into a Web site. Using only the IP address assigned to their computer, the country, state or even city can be identified reliably. IP geolocation is usually implemented as part of a back-end fraud or authentication system where merchants use the data to build business rules into their Web application which can flag suspect transactions and address them individually.

Fighting the Battle

Armed with geographic and network connection data provided by an IP geolocation service provider, merchants can set up rules that detect and prevent potential fraud. In analyzing IP geolocation data, some of the key attributes a merchant might look for are:

1. Check the distance between the actual and expected user locations.

It's a general rule of thumb that shoppers will log onto the Internet within close proximity to their billing or shipping addresses. Orders coming from 500+ miles away from the billing location have a higher probability of being fraudulent. A merchant could set up a rule in their fraud system that if an order falling 50 miles or more away from the shipping address then flag the order for manual review. Transactions across national borders raises the red flag even higher. International transactions represent nearly half of all credit-card charge backs.

2. Use the top and second level domain information of the email address to assess risk.

The top-level domain is the group of letters that follow the final dot of any domain name. For example, in the domain name www.retailsolutionsonline.com the top-level domain is [com](http://www.com) and the second-level domain, which commonly refers to the organization that registered the domain name, is [retailsolutionsonline](http://www.retailsolutionsonline.com). There are potential risks associated with certain domain info. Merchants might use this information to check the domain of the IP address observed at registration time with that used during other sessions, or check if the user utilizes different Internet Service Providers (ISPs) in a single day. They also could check for "unsafe" or "risky" top-level-domains (e.g., "edu") vs. "safe" ones (e.g., ".gov" or ".mil" in some contexts) and "unsafe" second-level-domains (e.g., Kinko's, which rents computer time by the hour to users)

3. Build user profiles. Then detect or track any changes in those profiles

A merchant might keep an electronic profile of a customer and log normal behaviors. Then when the customer visits the site again they could look for any inconsistencies in the behavior. A user profile might contain information on the country, state, and city the user usually logs in from. It might contain the average distance from the ship-to address to the bill-to address. They might look to see if they are using the same Internet Service Provider and that the domains are the same. If the patterns do not match the transaction can be flagged for further review.

4. Use time zone information when tracking connection "velocity"

If a user is connecting to a Web site in relatively short periods of time and the log-ins are 1,000+ miles away from each other, this is a major red flag for an online merchant. A merchant might determine the current time at the user's billing address location and compare that to the IP geolocation data gathered for time to check for mismatches. They also might be on the look out for "time-zone hopping", where the same account is accessed from multiple geographic locations within a very short period of time – distances greater than the person could drive.

5. Is the customer using an anonymous proxy server to access the Web site??

An anonymous proxy server is generally used to anonymize Web surfing. Because they are typically difficult to track, these types of proxies are especially useful to those computer criminals seeking online anonymity. While not all proxy servers are bad, the use of an anonymous proxy can be a fraud indicator. A merchant might create a rule to

check if the customer is using a proxy server and score that order as a higher risk.
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, but many fraud managers feel it gives them real competitive advantage over the enemy.