

The Fraud Challenge for E-retailers

Highlights

- Reduce online fraud by finding mismatches between customers' IP locations and their home addresses. One Quova customer reduced his fraud by over \$100,000 a month with this one comparison.
- Pre-emptively block Website access to certain locales or IP origination points known to be frequent sources of fraud. A major US credit issuer, and Quova customer, reduced its fraud rate for credit applications 12% in the first 90 days after deploying geolocation to flag overseas transactions.
- Protect your business by detecting fraudulent behavior from those applying for a card or banking service online before the card or check is issued. A Quova customer providing banking, insurance, and investments was able to identify more than 70% of potentially fraudulent transactions in just hours after installing Quova's Internet geolocation data

The combination of the Internet's anonymity, reach and speed and the necessity for "card-not-present" credit transactions makes the e-commerce process vulnerable to fraud. Online credit card fraud cost e-commerce businesses an estimated \$10 billion in 2007, and researchers say 60% of all credit card fraud now occurs online. And it's not just online retailers that are vulnerable—financial institutions with Web presences are regularly targeted by online thieves with fraudulent credit card and loan applications. The U.S. Secret Service calls credit card fraud "the bank robbery of the future."

One of the online criminal's best weapons is geographic anonymity—any enterprise can be targeted from anywhere in the world, and without knowing where the crook is, preventing the crime can be virtually impossible. Overseas-based transactions represent nearly half of all credit card chargebacks.

How Quova Prevents Fraud

E-retailers already use a number of tools to predict online fraud, but one tool frequently overlooked is reviewing a customer's location when they place an order online. If you know WHERE a customer is when he comes to your Website, you can immediately decide how to interact with him. Quova's Internet geolocation technology instantly determines a Web visitor's real-world location—from country level down to a city area, if desired, by identifying the Internet protocol (IP) domain of origin.

By comparing the billing and shipping addresses provided by the customer during the transaction with the actual location data provided by Quova, the business can immediately detect any inconsistencies, flag the transaction as potentially fraudulent and take the appropriate action.

Quova can show you the specific IP address elements you need to review for every transaction and we'll work with you to design rules to activate the data. You'll be able to detect and prevent more online fraud than ever before. All without adversely affecting your legitimate customers.

Quova's Internet Location Intelligence platform deploys real-time techniques to help online businesses locate virtually any visitor to their Website, regardless of the network connection or device they use for Internet access. Quova provides geographic information for IP addresses including continent, country, region (US only), time zone, state, city, postal code, longitude/latitude and phone prefix (US and Canada only). We also provide demographic identifiers for IP addresses within the United States including DMA codes (Nielsen Designated Market Areas). Finally we provide network connection information for IP addresses, including connection type and speed and an AOL flag.

Halt Fraudulent Transactions

In the real world, a credit application listing a home address in Utah that arrives in an envelope postmarked from Ukraine would certainly look suspicious. Quova adds a "return address" to every potential online transaction that enables the financial institution or

APPLICATION BRIEF

The Fraud Challenge for E-retailers

merchant to pull the plug on, or even pre-emptively block, a transaction that appears likely to be fraudulent—particularly if the geo-data indicates a customer listing a U.S. address is actually overseas.

ClearCommerce has identified 15 nations that serve as origination points for some 60% of those fraudulent transactions, led by Nigeria, where over 10% of transactions in the latter half of 2007 turned out to be fraud. From specific locations, the fraud

incidence is even higher—38% from one IP domain in Indonesia, for example. Automatically flagging or blocking transactions from those locations can reduce fraud losses at least 10% on all online transactions, and up to 25% on overseas transactions in particular.



bankinter.



BillMeLater®



ClickandBuy®



copernic®



EverBank®



ingenio® Pay Per Call™



www.luckyskills.com



State of Alaska
Department of
Revenue



wirecard

YOOX