

**GEOLOCATION —
NEW WEAPON
FOR E-RETAIL FRAUD
PREVENTION**

January 2005

Quova, Inc.

333 West Evelyn Avenue
Mountain View, CA 94041
T: 650.528.3700
F: 650.625.9801
Email: info@quova.com
Web: <http://www.quova.com>

Jan Luijkenstraat 94
1071 CV Amsterdam
The Netherlands
T: 31.20.888.45.30
F: 31.20.888.45.31
Email: info-eu@quova.com

Introduction

The explosive growth of worldwide e-commerce has been predictably paralleled by the equally explosive proliferation of online fraud. CyberSource projects that e-retail merchants will lose \$2.6 billion to online payments fraud in 2005, an increase of 37% in just two years. It is therefore a business imperative for every online enterprise to develop and implement a fraud prevention strategy that leverages the best technology tools and methodologies available to manage risk in a way that protects and enhances the revenue stream.

One such tool that is rapidly becoming a worldwide standard is the web geography technology known as **geolocation** – the ability to determine the true geographic location of the online customer. In CyberSource’s 2005 Online Fraud Report, 31% of respondents indicated they had already deployed a geolocation solution as part of their overall fraud prevention strategy, and an additional 22% planned to implement geolocation in 2005. Geolocation has proven itself a critical underpinning technology to the development and deployment of a fraud prevention system that will enable the online enterprise and its customers to do business with confidence.

Quova is the world leader in the development and deployment of geolocation as a fraud detection solution. Quova’s flagship GeoPoint™ service identifies the geographic location of any online visitor to an e-commerce website in real time, from country of origin down to city-level precision if required. Quova’s patented, independently audited geolocation solutions have been proven to greatly enhance any integrated fraud prevention solution and significantly reduce online fraud.

The Sources of Fraud

The Internet Fraud Prevention Advisory Council estimates the incidence of online fraud, as a percentage of business revenues, at up to 40 times higher than in real-world, face-to-face transactions. VeriSign has estimated that 6.2% of the billion-plus transactions conducted on the web each year have been fraudulent. All card-not-present transactions present fraud risk, but the geographic anonymity of the online customer creates the greatest possible exposure for the Internet enterprise.

The geographic veil of the web is effectively leveraged by criminals placing fraudulent US orders from other countries. Overseas-based transactions represent nearly half of all credit-card chargebacks, and a recent study found that over 25% of all fraudulent orders originating offshore employed US-issued credit card numbers. The merchant is unaware that what appears to be a domestic order is being placed from overseas, and ships the merchandise to the US address on the order. The merchandise is sold and the funds transferred to the fraudster long before the merchant knows the transaction is fraudulent – the average lag time between the fraud act and the chargeback notification is 72 days.

Vendor Solution: Equifax

Equifax (NYSE:EFX) enables and secures global commerce through its information management, marketing services, direct to consumer, commercial and authentication businesses.

Equifax has incorporated Quova's GeoPoint into its InterConnect fraud decisioning platform.

Vendor Solution: LexisNexis

LexisNexis RiskWise is a leading provider of automated, real-time, fraud, identity verification, risk scoring and collection solutions.

LexisNexis has embedded Quova's GeoPoint into its FraudDetector risk scoring engine.

The geographic risk factor in online fraud has been well known since 2002, when ClearCommerce identified a short list of 15 nations – headed by Yugoslavia, Nigeria and Romania – that produced some 60% of all fraudulent transactions. More specific geographic data produced even more striking statistics – 25% of all transactions from St. Petersburg, Russia were fraudulent. The nexus of worldwide fraud tends to change quickly over time, and as 2005 begins, Nigeria is generally considered the most dangerous single source of online fraud.

In 2004, LexisNexis studied over 100,000 transactions executed by a major US online retailer, all with US credit card numbers. The study found that 75 percent of the identified fraudulent orders with US billing addresses had been placed from overseas. 97.9% of all transactions originating in Africa and 74.8% of all transactions originating in Asia (including Russia) were fraud.

LexisNexis also found striking state-level numbers, determining that in over 85% of fraudulent domestic transactions, the customer's billing address did not match the US state from which the order was actually placed. Fraud rates were 15 times higher in transactions displaying these mismatches. Experian has found a 68% fraud rate in transactions where the IP origination point of the order was in a different state from the customer's billing address.

Impact of Fraud on E-retail Merchants

According to VeriSign, online stores experience fraud 17 times more often than offline stores, and the online merchant traditionally bears substantial liability for fraud losses. In addition to the bank chargeback from the fraudulent transaction, the merchant will incur additional losses from shipping costs (often higher than usual in fraudulent transactions), administrative costs, card issuer penalties and bank processing fees. The result is that even merchants selling low-cost items may lose several hundred dollars for each fraudulent transaction, and for merchants of consumer electronics and jewelry, costs can quickly spiral into the thousands.

CyberSource reports that while 1.3% of all orders filled by e-retailers in 2004 were fraudulent, the percentage of revenues lost to online payment fraud was 1.8% – because the median dollar value of a fraudulent transaction is 50% higher than that of a valid transaction.

Of even greater concern than fraud losses to many e-retailers, according to a survey by the Merchant Risk Council, are the potential side effects of fraud prevention measures. The inadvertent blocking of a legitimate customer by a website fraud program can do more damage to an enterprise's revenue flow than a fraudulent transaction, because the customer's future business is probably lost as well. The financial health of the enterprise therefore depends on a fraud prevention solution that not only keeps the bad guys out, but lets the good guys in.

Integrated Fraud Solutions with Geolocation

The answer to the challenge of online fraud is an integrated, accurate fraud prevention system that can perform real-time automated assessments of incoming orders to flag suspicious transactions before they are completed. The most effective fraud prevention program is an end-to-end, best-practices solution integrating multiple technologies, each focused on a particular fraud indicator – one provider uses the term “verification engine” to describe such a system.

No single technology is more critical to the success of this engine than IP geolocation, the science of determining in real time the true geographic location

Vendor Solution: VeriSign

VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the Internet more intelligent, reliable and secure. VeriSign Fraud Protection Services provide multiple filters to determine the risk level of a transaction, including helping to identify the location of the customer, to protect online merchants against fraud.

Quova's GeoPoint service supports VeriSign's Fraud Protection Services offering.

of a website visitor. At its most sophisticated, geolocation employs a combination of technologies, data-gathering systems and human expertise to identify the user's location – from country level down to city precision if required – by pinpointing the IP domain of origin.

In real-world commerce, geographic information can provide clues to the possibility of illegal activity – out-of-state checks invite additional scrutiny, for example, as would a mailed credit application listing a US address but displaying an overseas postmark. Geolocation provides the same sort of data for e-commerce transactions, which can be of great value when certain locations are known fraud sources. (In the 2002 ClearCommerce study, more than 10% of the transactions originating from Yugoslavia, Nigeria and Romania were fraud). Geolocation enables the enterprise to strip away the online criminal's geographic anonymity by comparing IP data to the billing and shipping addresses provided during the transaction to flag suspicious orders.

Vendor Solution: CyberSource

CyberSource is the leader in automated e-commerce transaction solutions. CyberSource's Advanced Fraud Screen (AFS), enhanced by Visa®, calculates the risk of card-not-present orders and maximizes sales by screening for questionable orders while minimizing the risk of blocking valid transactions.

CyberSource uses Quova's GeoPoint service to power its Advanced Fraud Screen.

The technique is highly successful. A large US online merchant, discovering that more than half of its fraudulent transactions originated from 15 overseas cities, reduced its fraud losses 15% by simply blocking orders from those cities. A large US credit issuer cut its fraud rate for card applications 12% in the first 90 days after deploying a geolocation solution to flag overseas transactions. And a major global e-retailer has reduced its credit card chargebacks by over \$100,000 a month, or approximately \$2.5 million over the two years since it deployed country-level geolocation.

“Geolocation has proven itself to be a critical underpinning technology to every integrated fraud prevention solution. The real-time determination of the user's geographic location has become critical to virtually every fraud and security issue in the online world, from transaction fraud to phishing to forensic investigation.” – Ori Eisen, President and CEO, The 41st Parameter.

By incorporating geolocation into an integrated fraud prevention system, merchants can establish fraud rules systems for their websites specifically designed to allow, flag or block certain kinds of transactions. Nearly three-fourths of all e-retailers, according to CyberSource, manually review suspect transactions before completion, and on average they review a third of all their orders. Geolocation technology helps the merchant create a rules system balancing the dual risks of fraud losses and blocking legitimate customers.

The Premier Geolocation Solution — Quova's GeoPoint

Quova's patented flagship geolocation solution, GeoPoint, is the premier technology in the world today for determining the physical location of web users in real time without invading the user's privacy or revealing itself to customers – or fraudsters – in any way. Quova performs by mapping the 1.4 billion assignable IP addresses on the Internet using proprietary algorithms and a worldwide network of servers to produce data that is then processed, analyzed and enhanced by Quova's Network Geography Analysts. This database is further improved by Quova's unique feedback process, through which the quality and accuracy of its geolocation data is continuously enhanced.

GeoPoint also delivers sophisticated network and routing data – it identifies the Internet path of the transaction, which like geography can be a significant fraud indicator. The LexisNexis study found that 64.4% of all orders routed via satellite were fraudulent, as were 12.8% of the transactions routed through international and regional proxies.

The real-time data provided by Quova's GeoPoint service enables an e-commerce enterprise to flag suspicious transactions before completion or block orders from high-risk locations. The enterprise is thus adding a level of authentication that can also be used to admit a proven customer with more efficiency, enhancing the customer experience while minimizing the risk of rejecting legitimate business.

QUOVA'S AUDITED EXCELLENCE

The internationally respected auditor PricewaterhouseCoopers has audited and validated Quova's patented geolocation technology and processes for mapping of IP addresses. PWC specifically attested to the efficacy of Quova's method for evaluating data quality and the value of Quova's global data collection network and human research analysis. In audited tests using large, independent third-party data sets of actual web users, Quova's country-level accuracy was measured at 99.9% and its US state-level accuracy at 94.0% and 93.9%.

The PricewaterhouseCoopers audit is the first ever conducted by a Big 4 auditor of a geolocation provider.