GEOLOCATION — FRAUD PREVENTION FOR ONLINE FINANCIAL SERVICES

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 proliferation of online banking has been predictably accompanied by the advent of the e-heist – the targeting of a financial institution by an Internet robber who may be halfway around the world. Gartner says that illegal access to checking accounts is the fastest growing type of consumer fraud – nearly two million US checking accounts were breached last year with losses totaling $2.4 billion – and online criminals are suspected in a significant percentage of those crimes.

An online crime against a financial institution devastates the reputation of the institution and the trust of its customers. The explosive growth of phishing and account fraud has made it critical for every online financial enterprise to develop and implement a fraud prevention strategy that leverages the best technology tools and methodologies available.

“Credibility is everything to a financial institution. Consumers must have absolute faith that their banks and credit providers are exercising the very best fraud prevention practices available, or the trust that is so vital to the relationship can be irreparably damaged.”
– Rick Broadhead, Consultant, Verified By Visa.

One tool that is rapidly becoming a worldwide standard for fraud prevention is the web geography technology known as geolocation – the ability to determine the true geographic location of the online customer. Geography is a proven fraud indicator, and geolocation has established itself as a critical underpinning technology to an integrated fraud prevention system that will enable the online financial enterprise to do business with confidence – and maintain the confidence of its customers.

**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.**
Financial Insights has estimated that worldwide online transaction fraud will cost $60 billion annually by the end of 2005. Banks and other financial services institutions offering online services are targeted by Internet fraudsters who use stolen identities to access customer accounts, apply for credit cards and loans, hack systems for confidential information or otherwise leverage their anonymity. They use data stolen from either the institution or the customer to steal money.

The fastest-growing form of fraud in the world, online or off, is phishing – the technique of using falsified e-mails and bogus websites to dupe users into surrendering personal data that can be used to steal their identities and access their accounts. The e-mails, which appear to come from trusted companies, steer recipients to startlingly realistic replicas of well-known websites, where they are solicited for credit card and bank account numbers, passwords and social security numbers.

MessageLabs, a UK security company, saw phishing attacks increase by **16,000 times in 14 months** – from 279 attacks in September 2003 to 4.5 million in November 2004. The Anti-Phishing Working Group, a consortium of major companies that monitor online phishing schemes, says attacks increased 4000% over a six-month period, and the number of phishing sites more than doubled in October 2004 alone, when 44 major brands were “hijacked” by phishers.

Gartner reports that 57 million Americans received phishing e-mails over a one-year period; 19% were lured to the phony site, and 3% surrendered personal data. Some of the world’s biggest online enterprises and their customers have been targeted – AOL, Citibank, Wells Fargo, SunTrust, eBay and PayPal, even the FDIC – and many enterprises are banding together to fight identity theft, in some cases with help from the US Secret Service and the FBI.

A commitment to identity theft prevention is now an absolute business imperative to every financial institution, not just for security reasons but for customer retention as well. In a recent survey by Unisys, 78% of respondents held their banks responsible for preventing fraud, and half said they would change banks if a competitor offered stronger protections. Wise financial services providers are committing to both stronger security measures and customer education efforts to prevent identity theft and account breaches.

---

**Vendor Solution: Cyota**

Cyota is the world’s leading provider of security and anti-fraud solutions for financial institutions, including anti-phishing and e-commerce fraud prevention services.

*Quova’s GeoPoint is embedded in Cyota’s new online fraud management solution, eVision.*
Online financial enterprises face other threats besides phishing – particularly credit card and application fraud schemes. Many banks have been swamped by fraudulent online credit card applications employing stolen identity data – once approved, the phony accounts can be quickly “maxed out” with fraudulent purchases and cash advances. Fraudulent online loan and mortgage applications based on falsified or stolen identity data have been used to generate millions of dollars in uncollectable loans. The Secret Service calls credit fraud “the bank robbery of the future” because criminals view banking and card systems as easy pickings.

The Geographic Risk Factor

All of the aforementioned threats are enabled by the geographic veil of the Internet – the targeted institution often has no verifiable data about the true identity or locale of a user attempting to access an account or submit an online credit application. If the user’s actual location is not the same as the address on the account, the likelihood of fraud increases exponentially – as does the risk to the financial enterprise and its customers – particularly if the user is in another country. About 50% of all phishing attacks come from overseas – many from organized crime rings in South America, Eastern Europe and Africa – and international terrorists have openly advocated phishing and other forms of online fraud against US institutions as fund-raising techniques.

The geographic risk factor in online fraud has been well known since 2002, when ClearCommerce identified 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.

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. Clearly, when an ostensibly American online user is actually outside the US, the risk of every brand of Internet fraud increases dramatically.

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.
To fight financial fraud in the physical world, bank employees are taught to spot false identification, counterfeit currency, fraudulent checks and other indicators of criminal activity through a combination of experience and awareness. Online banking services have protected themselves from unauthorized account access with similarly personal procedures, usually involving a customer sign-in process employing various combinations of account numbers, Social Security numbers and encrypted passwords. The protective level of these measures has dropped sharply because this sort of personal information has become so vulnerable to theft. The online fraud scoring and authentication engines currently in place at many banks now require updating with new techniques based on the changing trends and behaviors detected on the Internet.

No single technique is more critical to the success of the security process than IP geolocation, the science of determining in real time the true geographic location 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 banking operations, geographic information can provide clues to possible fraud – out-of-state checks invite additional scrutiny, as would a mailed credit application listing a US address but displaying an overseas postmark. Geolocation provides the same sort of data for online financial services, which can be of great value when certain locations are known fraud sources.

By enabling the financial institution to compare the user’s true location with the address on the account or application, geolocation serves as a vital fraud prevention tool. A user attempting to access a checking account from a mismatched or unknown location, for example, can be designated for an extra authentication process before being granted entry. This can protect the customer’s account even from a phisher who has succeeded in stealing the customer’s account number and password. If an online credit applicant’s true location doesn’t match the address provided, the application can be flagged for further investigation before the credit card or loan check is issued.

The value of knowing the location of the user and the cyber-location of the activity is rapidly proving itself in the financial services industry – a major US credit issuer reduced its fraud rate for credit card applications by 12% in the first 90 days after deploying a geolocation solution to flag overseas transactions.

---

**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 Premier Geolocation Solution — Quova’s GeoPoint

Quova’s patented geolocation solution, GeoPoint, is the premier technology in the world today for determining the physical location of web users in real time, from national origin down to zip code level, without invading the user’s privacy or revealing itself to customers – or fraudsters – in any way. Quova performs this function 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 transactions routed via satellite were fraudulent, as were 12.8% of the transactions routed through international and regional proxies.

Quova’s GeoPoint service provides that information in real time, so a financial services website can immediately flag suspicious visitors from high-risk overseas IP origination points or compare user location with the address on the account being accessed. The online banking system thus applies an additional layer of customer authentication before permitting account access – enabling both the enterprise and its customers to do business with greater confidence.

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.