



**IP Geolocation:**  
A Valuable Weapon to Fight  
Online Card-Not-Present  
Payment Fraud

## IP Geolocation: Fighting Online Card-Not-Present Fraud

**CNP fraud prevention showed significant progress in 2009 over 2008.**

### U.S.

- **Fraud loss \$3.3B, down from \$4B**
- **Est. 1.2% of overall sales; down from 1.4%**
- **Order acceptances up; no increase in fraud rates**

### U.K.

- **278£ (\$416M), down 15% from 328£ (\$491M)**
- **First decline in 5 years**
- **Another 5% drop seen for 2010**

## Overview

It's no surprise that the Internet world's combination of anonymity, reach and speed along with the necessity of card-not-present (CNP) credit transactions makes the e-commerce process vulnerable to fraud. Online credit card fraud cost e-commerce businesses in the U.S. an estimated \$3.3 billion in 2009 (down from \$4 billion in 2008) 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.”

In spite of this, according to the CyberSource Annual Online Fraud Report, 11th Annual Edition 2010, U.S. e-commerce fraud losses are not growing as rapidly as many perceive. In fact, from 2006 to 2008 the average percentage of online sales lost to fraud held steady at about 1.4%. And in 2009, the total estimated online revenues lost to fraud dropped for the first time since 2003 resulting in a lower percentage of overall sales of 1.2%. There was even more good news as fraud managers reported an increase in order acceptance rates for the second year in a row, with little or no increase in fraud rates.

In the U.K., card-not-present fraud fell 15% in 2009 to 278 million pounds (\$416 million) compared with 328 million pounds (\$491 million) in 2008, according to Retail Decisions, a provider of payment card issuing, processing and fraudprevention services. The findings mark the first decline in five years in CNP fraud and expectations are that that this trend will continue with a 5% decline in 2010 to 264 million pounds (\$395 million). Carl Clump, Retail Decisions CEO, attributes that decline to more retailers using some form of a fraud-prevention security program. However, as criminals continue to find new ways to navigate around security measures regulations, it is expected that these higher percentage drops in CNP fraud will level off in 2011.

## Strong forecast for online sales

In a study released in March 2010, entitled U.S. Online Retail Forecast, 2009 to 2014, by analysts Sucharita Mulpuru and Peter

## IP Geolocation: Fighting Online Card-Not-Present Fraud

Hult, Forrester Research forecast that online retail sales in the U.S. will grow to \$172 billion in 2010 (up 11% from \$155.2 billion in 2009) and increase an average of 10% per year for the next five years to reach \$248.7 billion by 2014. In addition, they predict that by 2014, the web will directly account for 8% of U.S. retail sales and influence 53% of consumer purchases.

In its 2010 UK Online Fraud Report issued in January, CyberSource reported that 69% of merchants surveyed expected online revenues to grow in 2010, with 40% of those expecting that figure to be as much as 20%. In fact, online sales increases are already evident. In a recent release, comScore, Inc., a leader in measuring the digital world, estimated retail e-commerce sales in Q3 2010 were up 9% versus one year ago, representing the fourth consecutive quarter of positive year-over-year growth. And in the U.K., the IMRG Cap Gemini Index, which tracks over 100 retailers across Britain, showed an 18 per cent increase in average consumer spending on internet shopping in July 2010 – a three year high – compared to the same period in 2009.

Although these strong growth indications are good news for e-commerce, the bad news is that online payment fraud will remain a major threat to the industry and fraud losses may potentially increase in numbers along with the increase in sales and become even more challenging and complex to combat.

### **Fraud vs. consumer convenience: a major challenge.**

The major challenge for online merchants is to detect and prevent payment fraud while increasing profitability and reducing operational costs. Both in the US and abroad, online merchants have the double challenge of addressing fraud prevention while at the same time making it easier for consumers to complete a transaction on their website. The majority of retailers in the US and the UK, however, believe that online fraud is one of their greatest business threats and that stopping online criminals in their attempts at fraud is the more important concern for their online business than improving the convenience of their website.

In spite of this focus, no e-commerce company realistically thinks they will eliminate all fraudulent transactions. According to Perry Tancredi, Senior Director of Product Development for geolocation provider Neustar IP Intelligence, every online merchant deals with

**Expert consensus within the fraud management industry estimates that for every fraudulent order a retailer receives, it rejects almost four –often valid – orders due to suspicion of fraud.**

## IP Geolocation: Fighting Online Card-Not-Present Fraud

a certain amount of acceptable fraud risk – and that amount will never be zero. Ultimately, preventing fraud is a question of balance for e-retailers – that is, keeping fraud at an acceptable level by spending the necessary amount of money on prevention tools and the security team to ensure that fraud limits are controlled.

### Consumer concerns

Recent research conducted by the Identity Theft Resource Center among 500 U.S. consumers who used the internet for banking or shopping showed that an alarming 87% expressed significant concerns about personal information data such as credit card information, passwords, usernames and social security numbers being stolen or lost by a business or financial institution in a data breach. Additionally, 81% also specifically mentioned being worried about getting phishing emails and 80% mentioned being worried about having their password stolen. 73% of those surveyed said they would no longer shop at a website that experienced a data breach.

Surveys show 87% of U.S. consumers and 71% of U.K. consumers express significant concerns about the risks of banking or shopping online.

Seventy-one percent of consumers surveyed in the U.K. stated they are concerned with the level of risk when purchasing online, an increase of 5% over 2008. And 50% of U.K. consumers still won't buy online.

With numbers such as these, online businesses must make efforts to protect their customers' personal data equally as important as protecting their business against monetary loss. And certainly the task in each case is not mutually exclusive.

### Geolocation an important tool

For merchants in the online world of e-commerce, there are no geographic boundaries. And with anonymity being one of the online criminal's best weapons, any enterprise can be targeted from anywhere in the world. Without knowing where the crook is, preventing the crime can be virtually impossible. Fortunately, there is a predictable and inexpensive tool called geolocation, which a merchant can apply to all of its transactions to help detect and eliminate only fraudulent ones while allowing legitimate transactions to go through.

As long as there is e-commerce there will be some types of fraud. However, adding IP geolocation data to their fraud prevention platform has helped many an online retailer stay ahead of

## IP Geolocation: Fighting Online Card-Not-Present Fraud

aggressive fraudsters, and enhance customer safety while reducing related operating loss and wrongly rejected orders – all of which can mean a significant increase in a retailer's bottom line and an important step toward building consumer loyalty.

In its October 2010 report, the APWG (Anti Phishing Workgroup) noted that in the first half of 2010, phishing attacks were down significantly to 48,244 from the record number of 126,697 observed in the second half of 2009. And just one criminal gang – called **Avalanche** by the APWG – was responsible for nearly two-thirds of those 2009 attacks. Although this year's lower number of phishing attacks appears to be good news, by the middle of 2010, **Avalanche** had moved on to a better tool – the **Zeus banking Trojan** – thus incorporating malware along with phishing, botnets, and spam into their work.

### Who is committing fraud and how they are doing it.

Although understanding the scope and monetary impact of cybercrime is important, it is also vital to gain insight into who the typical perpetrators are. One of the challenges of crimes committed via the Internet is that both the perpetrator and the victim may be located anywhere in the world. According to a report prepared by Accertify, an online fraud prevent solution provider, although individuals acting alone commit fraud, more frequently it is the work of criminal enterprises spanning national and international boundaries. Adding to the challenge is the cloak of anonymity in cyberspace, which can be difficult to penetrate.

It is often assumed that database hacking is one of the primary sources of criminal access to sensitive credit card data, however there are a variety of methods criminals use to gain access to this information that are more prevalent. Here are a few examples:

**Phishing** – This method incorporates the use of known brands in e-mail messages to lure consumers to counterfeit web sites that are designed to trick them into disclosing their credit card account numbers and other confidential information, which can later be used in fraudulent online transactions.

**Skimming** – This occurs when a dishonest employee of a legitimate merchant copies credit card information, or fits a disguised card reader over a legitimate slot on an ATM or other payment terminal to electronically capture personal card data, and maybe uses a hidden video camera to detect PIN numbers.

**Carding** – This is a term used by criminals for a process used to validate stolen credit card numbers – usually obtained by phishing or skimming. Criminals submit the credit card number and the cardholder's personal data on a website that has real-time transaction processing. Typically, small monetary purchases are made so as not to attract the attention of a merchant and to preserve the credit limit on the card. Once validated, the card

## A Real Life Example

*In one day an East Coast electronics merchant received orders for nearly \$500,000 worth of plasma TVs. Initially, it looked like a banner day. All the orders were charged to different card numbers, different names, and different billing and shipping addresses. Everything checked out. However, due to the unusual volume, the merchant's risk monitoring system flagged the orders for manual review. A look at the IP addresses used revealed that each of the seemingly different orders was sent from the same time zone. Further inspection showed that the orders came from a computer using Russian as its browser language setting. The chance of different customers all speaking Russian, all in the same time zone, all wanting 42-inch plasma TVs was slim. Then a check of the IP addresses showed all the orders came from the same IP address, even though the billing and shipping address for each order were different. 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*

## IP Geolocation: Fighting Online Card-Not-Present Fraud

number and related details will be sold to or exchanged with other criminals and/or used for larger transactions.

### The three main opportunities for online fraud

In a survey conducted among 185 payment executives at the NACHA – the Electronic Payments Association Payments 2010 Conference held in May, respondents pointed to payment account log-in as the type of web transaction at their business that was most in need of protection from fraud. It was followed by CNP payments and creation of new payment accounts. Here's what happens in each of these transactions:

**Authentication (e.g. log-in)** – a criminal obtains the individual's user name and password and sells that information to someone who will use it fraudulently to log in from wherever to enact a transaction.

**Transaction (e.g., purchase, wire transfer, stock trade)** – stolen credit card information is used to purchase items or trade money, or, once a fraudulent authentication is successful, money is transferred from one account to another.

**Account sign-up (e.g. credit card application)** – a criminal might phish the applicant's information (address, social security number, etc.), then go to another site, like American Express, for example, and apply for a new card using the phished applicant's credit; the new card would then be used for online transactions.

### Know your enemy

Knowing your enemy is the start to fighting any battle. Online, the e-merchant's enemy is anyone ready to ply malicious tactics when they log on to merchant sites to order goods or services with stolen credit card numbers or to hack into a customer's account.

As a result, it has become increasingly important for online businesses to know where their web visitors are located 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. Which is why a significant number of e-commerce companies have adopted geolocation as one of their most effective risk management tools for identifying fraudulent activity online in whatever guise it may appear and from wherever in the world it may originate.

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, with fraudulent international transactions more than two times higher than those for domestic orders.

## IP Geolocation: Fighting Online Card-Not-Present Fraud

### How merchants are fighting the fraudsters.

A wide variety of detection tools are available to help merchants evaluate incoming orders for potential fraud. Fraud detection tools are defined as those used during automated screening to identify the probability of risk associated with a transaction or to validate the identity of the purchaser. Results of tests carried out by detection tools are then interpreted by humans or rules systems to determine if a transaction should be accepted, rejected or reviewed. In the CyberSource survey, 70% of merchants reported using, on average, 4.7 detection tools for automated screening, with larger merchants, dealing with higher order volumes using an average of 7.3 detection tools.

None of the online fraud protection tools are fail safe, however each one adds an extra layer of protection for e-merchants faced with potential fraud. One tool that merchants may overlook is IP (Internet protocol) geolocation, which enables a merchant to review a customer's location when they place an order online. If a merchant knows where a customer is when he comes to a website, that merchant can immediately decide how to interact with him.

### How IP geolocation works

IP geolocation attempts to identify the geographic location of the device from which an online order is placed. It provides an additional piece of information to compare against other order information and order acceptance rules to help assess the fraud risk of an order. Fraudsters may also employ anonymizers/proxy servers to hide their true IP address and location.

IP geolocation technology instantly determines a web visitor's real-world location—from country level down to a city area, if desired—by providing location and other information associated with the IP address of the network connection or device they use for Internet access. By comparing the billing and shipping addresses provided by the customer during the transaction with the actual location device, the business can immediately detect any inconsistencies, flag the transaction as potentially fraudulent and take the appropriate action – all without adversely affecting legitimate customers.

An important consideration for consumers is privacy. With IP geolocation customer privacy is never compromised, nor is their behavior ever tracked; only the location from where the customer is

## IP Geolocation: Fighting Online Card-Not-Present Fraud

connecting to the internet and some connection characteristics are revealed in the geolocation data.

### More merchants adding geolocation

In 2009, half of larger U.S. online merchants employed IP geolocation tools in their automated fraud management process, with 36% of them selecting IP geolocation as one of their top three most effective tools. Geolocation was also high on the list for merchants who planned to add new fraud detection tools to their screening process. In the U.K., 26% of merchants surveyed are currently using or are planning to add geolocation as a fraud detection tool in 2010.

## The fraud fight is showing success.

With online revenue lost to fraud declining both in the U.S. and U.K. in 2009 over 2008 and e-merchants as a whole accepting a higher percentage of orders, efforts at detecting and preventing fraud are clearly showing success. And even with merchants posting a higher rate of order acceptance, the percentage of those orders later determined to be fraudulent also fell in 2009. However, how well a merchant succeeds in its fraud-fighting strategy is often determined by such elements as the fraud prevention tools a merchant uses, the size and type of its business and whether or not the merchant accepts international orders.

### Merchant size makes a difference

Although fraud rates have dropped overall, according to CyberSource, very large merchants who typically use more tools and have more experience and resources to manage online fraud have fraud rates that tend to be lower than the overall rate.

In the U.S., medium size online merchants suffered the highest percent of revenues lost to payment fraud in 2009 – with losses at 2.2% vs. the largest merchants at 0.9%. Medium size merchants are often targeted by fraudsters as they have enough online order volume to allow multiple fraud attempts but may not yet have the fraud management experience, or dedicated people or systems in place to defend against the professional criminals.

Smaller merchants have an even lower rate (0.8%) of revenue lost to payment fraud than medium-sized merchants, likely due to the volume of their business being less optimum targets for serious

*“We wanted to find a way in which we could reduce, as much as was feasible, any fraudulent credit card payments during the purchase process on any of our websites. By identifying a user’s location, not only could we quickly ascertain whether they were in the same country as that of the registered card owner, but we could also begin to set up specific strategies and rules to minimize fraud from certain countries.”*

**Pablo Vega,**  
Head of Engineering,  
eDreams

## IP Geolocation: Fighting Online Card-Not-Present Fraud

criminals. The very smallest businesses, however, especially those new to e-retailing, are extremely vulnerable to fraud with losses as a percentage of revenue often as much as five times greater than the merchant rate overall.

### International orders carry higher risk

Merchants made significant progress in selling internationally in 2009 with over 50 percent of those surveyed accepting orders from outside the U.S. and Canada. Most importantly, the increase in international sales, which was up 4% over 2008, did not result in an increase in fraud on those transactions. Indeed, as noted in the CyberSource report, the actual direct fraud rate on international orders for this group fell by half from 4% in 2008 to an average of 2% in 2009.

In the U.K., a large number of merchants have already embraced regional and global expansion opportunities as well, selling into Europe, the Americas and Asia Pacific. Indeed, France, Germany, Italy and Spain are already served by more than half the merchants that accept international orders. China, Brazil and Mexico are the top three countries merchants plan to sell into this year.

Despite this progress, international orders still have twice the overall fraud rate of domestic online orders and e-retailers must make sure that their fraud detection and management systems are robust enough to handle the additional risk involved. Online merchants who sell outside the U.S. and Canada reject international orders due to suspected fraud at over three times the rate of the U.S. and Canadian average of 2.4%. As a result, one out of five merchants who have been accepting international orders in 2009 stopped accepting them from one or more countries in the past year due to high fraud levels. Similarly, one in four merchants in the U.K. stopped accepting orders from specific countries, with over 60% of merchants citing Nigeria followed by Ghana, Malaysia, Indonesia and Russia among others.

### IP geolocation helps detect country-specific fraud

Although higher risk has deterred some online merchants from accepting international orders, many continue to accept them and are planning even further market expansion. With reports showing that specific countries are often the source of many of the fraudulent orders, adding IP geolocation as a detection tool in a

### Geolocation Results

- A major US credit issuer reduced its fraud rate for credit applications 12% in the first 90 days after deploying geolocation to flag overseas transactions
- An online retailer cut its fraud losses 15% by simply blocking orders from 15 overseas fraud hot spots
- A financial institution reduced credit card chargebacks by over \$100,000 a month by implementing country-level geolocation
- A US financial services company, providing banking, insurance and investments services online, was able to identify more than 70 percent of potentially fraudulent transactions within hours of deploying a geolocation service

## IP Geolocation: Fighting Online Card-Not-Present Fraud

merchant's fraud prevent platform has proven to significantly reduce the risk of online commerce in international markets.

One example of how successful a company has been in preventing fraudulent activity with geolocation data added to its platform is illustrated by the recent experience SafeCharge, an international leading payment service provider, had with an online merchant targeting France in its marketing. SafeCharge discovered that 50% of all the merchant's charge backs were being generated by just 5% of the traffic – which was coming from other countries. By blocking the identified countries using the IP data, SafeCharge reduced the charge back level of the merchant dramatically and were able to keep the merchant safe.

## Conclusion

The fight against card-not-present fraud is an ongoing battle and, though recent reports have been positive, there's no doubt that criminals will try harder and smarter to remain undetected. At the same time, online merchants are working just as hard to get ahead of the problem and are showing success. However, as e-commerce in both the U.S. and U.K. is showing signs of rebounding, the question remains whether last year's down economy slowed fraudsters as well, or whether merchants' prevention tools are getting better at putting them permanently out of work.

The answer is likely to be yes in both cases: the economy and powerful prevention tools have had an impact. However, as noted by the Anti Phishing Workgroup, it has also become evident that some determined criminals simply took a break to retool their arsenal of fraud-ware and attack strategies and are starting to renew their efforts once again.

Thus with more and more consumers turning to the internet for shopping, banking and personal activity, it's imperative that online merchants of all sizes have some types of fraud detection tools on their sites or risk escalating losses – and dwindling customers.

## IP geolocation delivers significant results

In the realm of cyberspace, both online consumers and online criminals can be located anywhere. And finding exactly where that location is can be the key to a merchant's determining if a transaction is fraudulent or legitimate. Which is why among the wide range of proven detection tools available, IP geolocation is

## IP Geolocation: Fighting Online Card-Not-Present Fraud

one of the top three tools many merchants currently use, with more planning to adopt it for their platforms.

Ultimately, the goal of online credit card fraud detection and prevention is not only to detect and prevent criminal actions, but also to ensure that the expanding world of e-commerce is safer and more convenient for legitimate consumers everywhere and more profitable and efficient for the merchants who serve them.

### About Neustar IP Intelligence

Neustar, Inc. provides a wide range of customers with high-quality, IP geolocation data. This data allows companies, large and small, to use detailed demographic and network characteristics to prevent fraud in online commerce; regulate online content (DRM) to stay compliant; and enables marketers to localize content and analyze traffic. Neustar is the only full-service IP intelligence provider with a team of analysts, customer technicians and developer advocates who add human IP to network IP to offer consultative services along with its data files.  
<http://www.neustar.biz/ipintel>