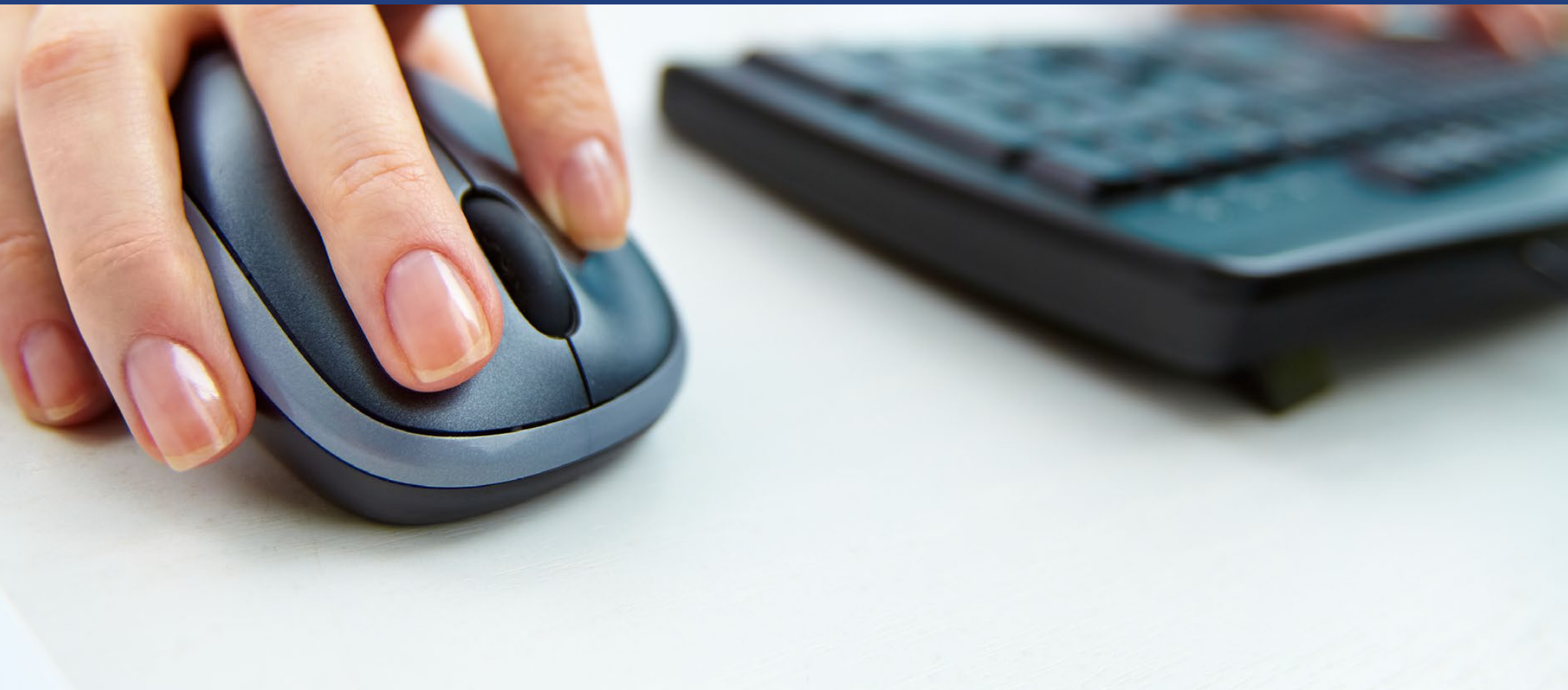
digital element®

Location is Elemental ™

How Retailers Can Automate the Screening Process for Online Fraud While Preserving the Customer Shopping Experience



digital element
Location is Elemental ™

Managing Online Payments Fraud Is a Balancing Act

Today's online world is a place where identities are filched in the blink of an eye and financial details are bought, sold and used before unsuspecting consumers clue in to the loss. While revenue for the online retail sector continues to grow—painting a seemingly rosy picture—merchants, behind the scenes, must deal with the escalating costs of managing fraud.

When processing online orders, organizations must decide whether to accept, reject or review a given order. They are also faced with the unsettling fact that a certain number of orders accepted could be fraudulent and lead to chargebacks; and, conversely, some rejected orders might be valid and that revenue will not be realized—nor will the purchaser be likely to return.

With record numbers of global e-commerce transactions—projected estimates are near $2.197 trillion for 2017[1]—leveraging the right tools to help verify online identities and transactions is more important than ever. The impact of online payment fraud affects profits across a number of key inflexion points. In addition to direct revenue losses plus the price of stolen goods and associated delivery/fulfillment costs, there are the additional costs of rejecting valid orders, staffing manual review teams, administration of fraud claims, as well as challenges associated with business scalability. And, that may simply be exhaust when compared to the millions it could cost a merchant if there was, in fact, a security breach. Possible attorney fees, customer notification costs, fines and the cost of paying for credit monitoring for affected customers can quickly add up to six figures or more.

Minimizing online fraud while managing the delicate balance between valid order acceptance and false-positive rejects can quickly become complicated and costly. Typically, companies initially rely on manual review of a disproportionate number of orders, chewing up both time and resources that could otherwise be dedicated to increasing sales and customer satisfaction. According to CyberSource, merchants spend 52 percent of their fraud-management budgets on manual review staff.[2]

Rather than consume human resources with labor-intensive fraud-prevention activities, companies need a cost-effective, front-line defense that marries virtual- and physical-world knowledge to improve, protect and automate order processing.

This paper discusses how retailers can leverage Internet Protocol (IP) Intelligence—the wealth of information gleaned from a customer's IP address—into order decision-making to reduce fraud, automate the review process, and increase the number of valid, accepted orders. This, in turn, enables organizations to improve profits, build consumer confidence, and preserve the shopping experience for the online channel.

With record numbers of global e-commerce transactions—projected estimates are near

$2.197 trillion

for 2017 —leveraging the right tools to help verify online identities and transactions is more important than ever.

The Greatest Threats for Digital Merchants:

Clean Fraud

ID Theft

Friendly Fraud

Phishing

Botnets

digital element
Location is Elemental ™

Online Identity Verification Lies at the Intersection of the Virtual and Physical Worlds

In the process of online identity verification during one-time transactions, such as card-not-present (CNP) purchases from an e-tailer, companies have adopted and deployed many methods to protect themselves from fraud. Some have implemented solutions such as risk-based decision engines that incorporate Address Verification Service (AVS) checks; third-party data verification solutions; and other variables that indicate risk in determining whether to approve or decline a transaction. While these systems are highly valuable within an overall fraud-prevention scheme, some also have a relatively high cost per transaction.

So how can merchants cost-effectively improve order acceptance rates and reduce fraud without incurring outrageous order verification and chargeback fees?

For the last several years, global studies of online merchants have consistently found that incorporating IP Intelligence (with its geolocation capabilities) was one of the top most effective tools for fighting online fraud in e-commerce.[3] Geolocation technology automatically identifies the geographic location of the device from which an order was placed. It provides additional data to compare against other order information and acceptance rules to help calculate the fraud risk associated with the transaction.

Today, the greatest threats for digital merchants are:

- **CLEAN FRAUD** - A transaction that passes a merchant's typical checks and appears legitimate, yet the transaction is actually fraudulent
- **ID THEFT** - When someone pretends to be someone else by assuming that person's identity, in order to obtain some kind of benefit
- **FRIENDLY FRAUD** - Occurs when consumers make an online purchase with their own credit card and then issue a chargeback after receiving the goods or services
- **PHISHING** - E-mails that trick people into providing personal information to unauthorized individuals who use it to commit identity theft
- **BOTNETS** - A collection of compromised computers under the remote command and control of a criminal, used as a vehicle to facilitate other online fraudulent activities

IP Intelligence delivers the data necessary to expose the anonymity or lift the cloak of fraudsters. By leveraging IP Intelligence within a fraud-prevention framework, companies can marry the virtual world and physical attributes to make real-time decisions on the validity of online customers and transactions.

digital element
Location is Elemental ™

NetAcuity Complements Multi-layer Fraud Management, Provides Early Intervention

At some point, each retailer must determine its own tolerance for risk and loss. A recent True Cost of Fraud℠ Study found that for every $100 in fraudulent transactions, it actually cost a merchant $308 in related expenses.[4] As an organization matures, it must understand that corporate goals and objectives will change so its tolerance for manual review, fraud, and lost orders will more than likely adjust as well. So how does a company balance the cost of these systems? The answer comes from two fronts: Reducing the number of transactions that flow to more costly transaction verification systems and streamlining the manual review process for suspect orders.

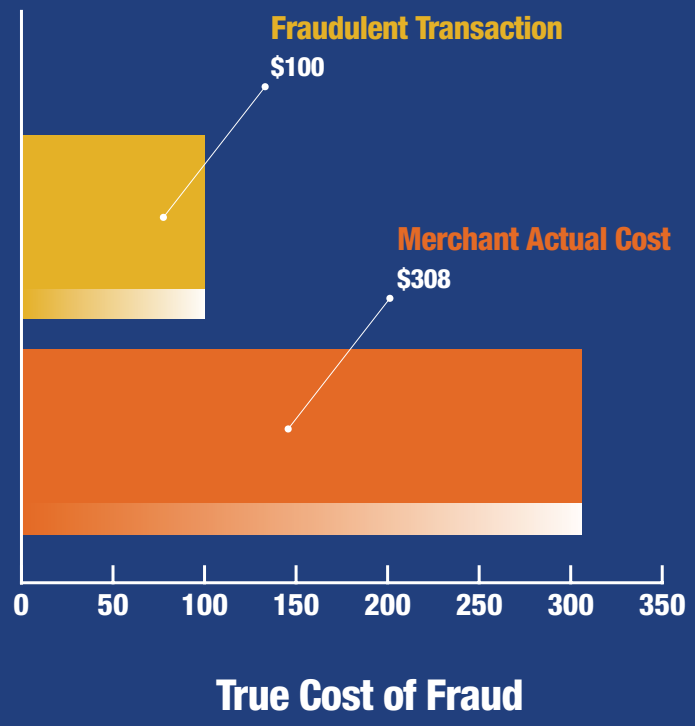
NetAcuity provides a solution that complements current multi-layered processes designed to stop fraudulent transactions. By filtering out a high percentage of transactions in real time based on an organization's risk tolerance threshold—and at a much lower cost per transaction—online merchants regardless of size can start to balance the inequity that exists between fraud losses and fraud-prevention costs. Most importantly, NetAcuity provides the information necessary for each retailer to determine the outcome of a transaction—whether blocking a transaction, moving it to the next step in identity verification, or sending a transaction to another review process.

IP Intelligence technology accurately and non-invasively identifies the location of website visitors down to a ZIP and postcode level worldwide in real time. Acting as a first line of defense against online fraud, NetAcuity uses a customer's unique identifier–an IP address–to uncover information including location, anonymous proxies, domain name and some other 30-plus attributes referred to as "IP Intelligence." Because NetAcuity relies on IP-based connections to return information about devices, it makes it an ideal fraud-prevention tool that works invisibly across multiple screens, without interfering with the online experience. By adding an additional layer of protection to validate or verify user location, NetAcuity is a key component of mission-critical fraud, compliance and security applications. This allows retailers to improve and automate decisioning on transaction risk by comparing the information customers enter about themselves against where they actually originate their transaction in the virtual world.

Smarter Rules Lead to Improved Decisioning

Building smarter rules around fraud detection and automating the process is proven to increase detection rates, reduce false positives and improve the customer experience. IP Intelligence can be used to automatically block suspect traffic, request verification (via email or SMS) or flag suspect activity for further internal review.

Geography is part of the fraud-detection landscape and smart merchants take it further than just location, by using NetAcuity's advanced intelligence parameters to identify proxies, virtual private networks (VPNs), anonymizers, tors, mobiles, Internet Service Providers (ISPs), domains and hosting centers. By providing more than just geography, NetAcuity's IP Intelligence can identify a greater number of suspicious connections.



True Cost of Fraud

For every $100 in fraudulent transactions, it actually cost a merchant $308 in related expenses.

Examples of rules that can be employed:

Country of Origin

Bill-to and Ship-to

Domain Names

Proxies

Hosting

Home, Business and ISP

digital element
Location is Elemental ™

Examples of rules that can be employed:

COUNTRY OF ORIGIN

A company trading internationally will often block common high-risk fraud countries such as Nigeria, India, Pakistan and Russia. Additionally, if a user is known to reside in a specific country, access to an account from another country could be deemed suspect. A basic "registry scraped" system will not be able to accurately determine the location of a user. Also, free IP data cannot identify if a visitor is masking the country he or she is accessing the Internet from (via a proxy or anonymizer), allowing potentially fraudulent activity to take place.

BILL-TO AND SHIP-TO

If the bill-to/ship-to locations and IP address do not match, an automated red flag can be passed for further review, or the account holder could be asked for verification via an email or text.

DOMAIN NAMES

Known fraud domains and suspicious Internet locations such as public Wi-Fi hotspots, Internet cafes and university/colleges should be taken into account.

PROXIES

Understanding the type of proxy a visitor is connecting to the Internet with, such as anonymous, transparent, corporate, public, education or AOL can trigger fraud alerts. Responses to the type of proxy can vary depending on what type of proxy it is, for example an anonymous proxy may warrant a greater score than a corporate proxy. By identifying connections that obscure the end user location or those that seek to portray a connection from an "acceptable" city or country can now be easily categorized.

HOSTING

End-user traffic should generally not be seen from hosting or data centers as these types of facilities are designed for traffic to pass through, not originate from. Some cloud browsers do use these centers, but services are patchy and not widely developed. A review with other customer relationship management (CRM) data is highly recommended before order acceptance is confirmed.

HOME, BUSINESS AND ISP

Additional layers of intelligence can be added that identify whether a connection is from a home or business as well as which ISP the customer uses. The data can be used to build profiles of previous connectivity to assess differences or anomalies over time.

Based on the results of these rules, educated decisions are made such as whether to: continue to process the transaction; proceed with additional identity checks such as out-of-wallet challenges; stop the transaction from further processing; or send the transaction for manual review.

digital element
Location is Elemental ™

As the first or an early step in the identity-verification process, deploying NetAcuity saves organizations time and money by identifying fraudulent activity before transactions are passed to more costly verification checks or sent for manual review. Customers deploying this solution have reported up to a 90-percent lift in identifying and stopping fraudulent activity before it happens.

IP Intelligence Cuts Online Fraud Losses and Reduces Prevention Costs

As mentioned previously, return on investment can come in many forms, from decreases in human capital costs by reducing the number of transactions that hit the manual review process to a straightforward reduction in fraud losses.

As demonstrated in the graphic, merchants processing 1 million transactions per year can save nearly $300,000 in total fraud-management costs by employing IP Intelligence. With reductions in both the fraud and manual review rates, organizations using IP Intelligence can expect significant savings in the related costs—reductions in fraud loss by $200,000 and manual review expenditures by $93,750. This type of return on investment provides organizations with the ammunition to justify the cost of new, upfront fraud-prevention tools.

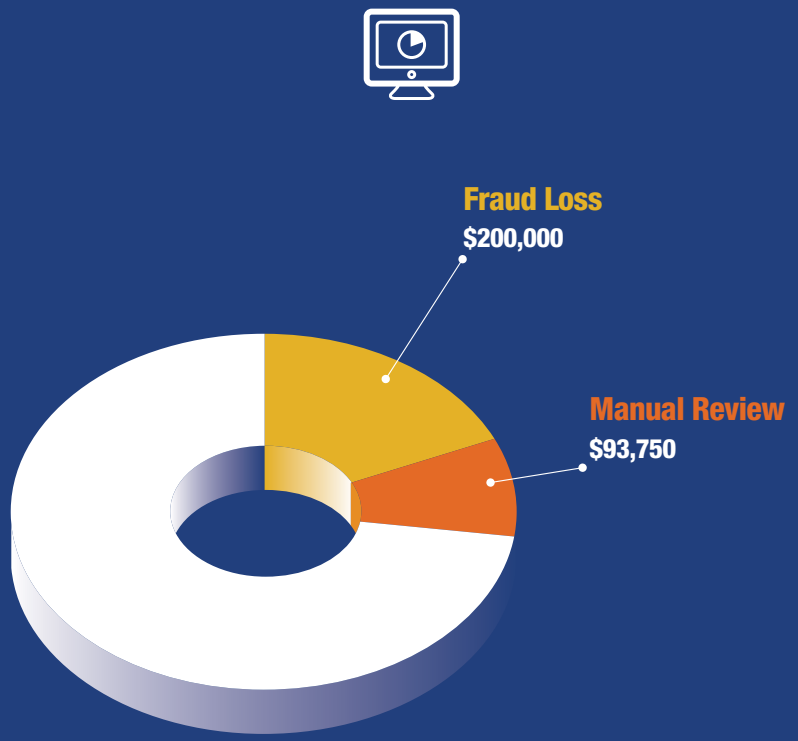
Mobile Is Driving Demand for Faster and More Efficient Check-outs

The continued rise in digital transactions will only result in more prolific data breaches than ever before, increasingly sophisticated fraud attacks, and new cashless and CNP payment methods. Younger demographics will drive online spending growth and will continue to press the envelope for faster checkout methods. And companies will find themselves at the crossroad of security and efficiency.

The challenge going forward, however, is to find equilibrium in an age where mobile is the way in which commerce online is happening. The Yankee Group projects mobile commerce will reach $906 billion by 2017.[5] With an ever-increasing share of online transactions moving to mobile, fraud in the mobile channel is affecting merchants more than ever before. New research indicates that companies are averaging more than $92 million in annual losses just from mobile fraud.[6]

Mobile subscribers currently outnumber Internet users by almost three to one. And, of those mobile users, 80 percent are more likely to be on a Wi-Fi network due to speed, convenience or cost, with approximately 20 percent connecting via 3G, 4G or LTE.[7]

Using a mobile device for ecommerce and completing the purchase still creates an IP connection, making NetAcuity a viable front-line fraud-management solution to help identify genuine customers at the earliest opportunity. NetAcuity can accurately determine the Wi-Fi location and the types of proxy being used, so the same rules apply. If connecting via 3G, 4G or LTE, then network characteristics identifying service providers and their connection hub are seen.



Merchants Processing
1 Million Transactions Per Year.

Merchants processing 1 million transactions per year can save nearly $300,000 in total fraud-management costs by employing IP Intelligence. This type of return on investment provides organizations with the ammunition to justify the cost of new, upfront fraud-prevention tools.

Contact Digital Element

Contact us to learn more about how we can help give your online initiatives the competitive edge.

(678)258-6327

www.digitalelement.com

digital element®
Location is Elemental ™

Merchants Must Continue to Build Defenses in Anonymous Online World

Huge retail revenue losses due to online fraud continue to rack up year after year. During the past 10 years, the volume of global fraud losses for online payments has increased at an average rate of 10 percent annually. At the end of 2014, the global losses due to fraud were expected to reach the astounding amount of $14 billion, which is the equivalent of 140,000 jobs.[8]

With the U.S. payment card industry undergoing an upgrade to the EMV standard (EMV stands for Europay, MasterCard, Visa, the three companies that developed the standard for the security chip), it is expected that the United States will experience a significant increase in online fraud as criminals migrate to CNP opportunities. According to leading research firm Aite Group, CNP fraud will account for about $2.9 billion in fraud losses to U.S. issuers this year. However, by 2018 when about 98 percent of payment cards in the United States will be enabled with the EMV capability, that number is expected to more than double to $6.4 billion in losses.[9]

Unfortunately, criminals are always going to look for ways to siphon money from a merchant's bottom line, which stresses the need to implement fraud-prevention strategies that not only stop those losses, but also do it in a cost-effective manner—managing the delicate balance between an efficient and seamless shopping experience and an accurate and secure transaction. Digital Element's NetAcuity solution is a cost-effective first step within a fraud-prevention framework and will provide retailers with the tools necessary to spot—and stop—fraud before it happens. Used in conjunction with traditional identification- and transaction-verification tools, NetAcuity will allow merchants to preserve the customer online shopping experience, reduce fraud losses and, ultimately, help increase their profitability.

[1] eMarketer, "Retail Sales Worldwide Will Top $22 Trillion This Year," Dec. 23, 2014.

[2] CyberSource, "2014-15 Online Fraud Management Benchmark Study," 2014.

[3] Ibid.

[4] LexisNexis, "Post-Recession Revenue Hampered by Fraud As All Merchants Face Higher Costs," 2014.

[5] The Yankee Group, "Mobile Metrics That Matter: Growing the New Mobile Economy," Feb. 6, 2014.

[6] TeleSign, "Enterprises Report Up to $240M in Annual Losses Each, Due to Mobile E-Commerce Fraud," Feb. 5, 2015.

[7] Informa, Mobidia Technology, "Smartphone Users Consume 80% of Mobile Data via WiFi," Feb. 22, 2013.

[8] Ubivar Risk Analytics, "Global Online Fraud Losses = 140,000 Jobs," 2014.

[9] EMC Corporation, "E-Commerce Fraud Trends 2014: Securing the Online Shopping Cart," 2014.