

THE ONLINE FRAUD LANDSCAPE

THE ARMS RACE TO PROTECT AGAINST ONLINE FRAUDSTERS



As long as there has been e-commerce, there have been online fraudsters. But now the stakes have been raised. The online business environment has reached a new level, where the war on cybercrime is a 24/7 battle that simply can't be ignored. While yesterday's criminals focused on a handful of high-value accounts, today's break-ins can impact the identity and financial security of millions of consumers.

Today's headlines are full of massive data breaches affecting some of the world's largest and most-respected financial institutions and e-commerce brands. Even government institutions, the military and their contractors have fallen victim to increasingly sophisticated cyber-criminals operating both next door and halfway around the world.

"All types of businesses engaged in e-commerce are fighting an arms race to protect against online fraudsters," says Akif Khan, director of products and services for CyberSource, a Mountain View, Calif.-based payment management company and fully owned subsidiary of Visa, Inc.

In most instances, businesses are able to thwart predatory attacks. However, when they lose the battle, the consequences can be stunning.

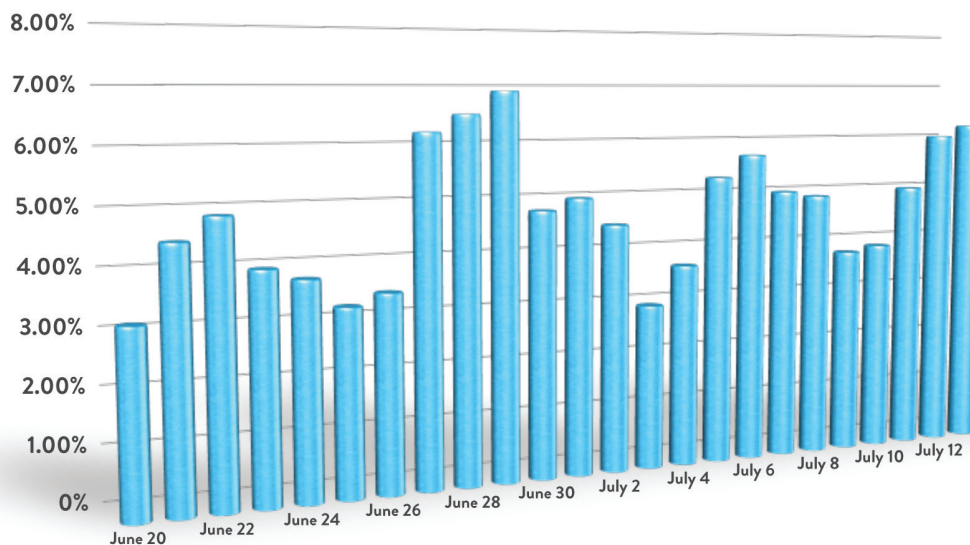
The result? Millions of individuals have experienced compromised finances and credit histories. Angry consumers, who once entrusted their personal information to companies and organizations, are becoming less confident in their ability to safely perform business transactions online as they question whether companies can confidentially keep sensitive electronic financial records.

In 2010, online e-commerce revenue loss in the U.S. and Canada due to fraud amounted to an astounding \$2.7 billion, according to the 2011 Fraud Report by CyberSource. This estimate doesn't even include the cost of charge-backs and other losses that the merchant ultimately pays for. For example, for every \$100 involved in a fraudulent transaction, a merchant actually loses \$310, according to a study for LexisNexis conducted by Javelin Strategy and Research.¹ For companies that have millions of transactions on a monthly basis, this can amount to significant losses in overall revenue and earnings.

Indeed, organizations impacted by online transactional fraud are further forced to pay hundreds of millions of dollars to rectify the breaches to customers, upgrade their information security systems, conduct audits, and pay pending lawsuits and possible regulatory fines.

¹ <http://www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1304025350760844>

Percent of Devices With Cookies Wiped



The chart above depicts the percentage of transactions that have come from devices that are known to have wiped their cookies during a recent 24-day period. Using less-sophisticated solutions, 3% to 7% of all transactions would appear to be coming from new, unknown devices. However, with Threatmetrix SmartID™, these transactions can be easily flagged for additional inspection.

The Evolution of Fraud Detection Solutions

Over the years, businesses have tried a variety of methods to identify fraudulent orders. Merchants dealing with “card-not-present” (CNP) purchases—such as orders placed over the Internet—started by verifying the card number and the CVV code, as well as comparing the billing location and shipping address, says Avivah Litan, vice president and distinguished analyst at Gartner Research. Meanwhile, financial institutions initially sought simple solutions recommended in 2005 by government regulators to safeguard customer accounts.

Once the cyber-criminals outsmarted those techniques, Litan continues, companies incorporated device identification to assess the status of visiting computers. Initially, this started with basic identification using Internet protocol (IP) addresses, and later it evolved into more-advanced tagging devices with cookies or Flash objects.

While these more sophisticated approaches to detect online fraud worked for a short time, criminals can now easily

thwart solutions using simple IP address checking and cookie tagging. Fraudsters are adept at hiding IP addresses behind proxy servers, or behind a bot computer that is within a legitimate IP range for that supposed customer. “Cookie-based authentication can also be easily circumvented using relatively simple techniques,” notes Stephen Northcutt, president of the SANS Technology Institute, a postgraduate computer security college based in Bethesda, Md.

“People erase their own cookies, or their computers can be attacked to modify cookies without them knowing,” Northcutt explains. “Other forms of fraud include using technology to get in the middle of the browser session and proceeding to commit the act once the user’s been authenticated through the cookie.”

“In the face of increasingly sophisticated system attacks, the first and best line of defense to detect fraud is through profiling the device initiating the transaction,” says Reed Taussig, president and CEO of ThreatMetrix, a leading provider of Internet fraud detection and prevention solutions.

The Device Whisperer: Finding Signs Hidden in Device Attributes

What’s most important when conducting business on the Internet is to have the means to immediately identify whether a transaction can be trusted, says Taussig. The goal is to eliminate both first-time and repeat fraud while minimizing inconvenience to legitimate customers. In addition, companies must also minimize the number of transactions that must be sent for manual review, which is an expensive process typically costing between \$10 and \$15 per transaction.

Companies engaged in e-commerce and financial services, as well as social networks, have embraced the ability of ThreatMetrix to provide highly reliable, low-cost fraud screening. These organizations are successfully eliminating fraud from a variety of transactions including payments, new account originations and customer log-ins.

“Our clients want to be able to minimize fraudulent transactions as well as rapidly authenticate returning customers,” Taussig explains. “So they benefit from the fact that ThreatMetrix employs



third-generation device identification technology to discover fundamental attributes about the computer attempting the transaction. Rather than relying on personally identifiable information (PII) or other easily defeated technologies, ThreatMetrix uniquely employs both cookie-based and cookieless device identification, real-time proxy piercing, intelligent packet inspection, and a global fraud network to assess the risk associated with each transaction.

When an electronic device is used to access a business website protected by the ThreatMetrix solution, the system looks at more than 250 attributes in real-time to detect fraud and immediately warns customers if anomalies have been detected. Since criminals rely on maintaining their anonymity, device anomalies are a powerful way to uncover fraudulent transactions. For example, attributes such as the true geo-location of the device can indicate

when a fraudster is trying to circumvent its location-based screening. Cybercriminals may attempt to place orders in English from an IP address masked to look as if it's coming from an American location. However, ThreatMetrix can determine the true IP address of that device and discover that the computer is actually located in Russia. "That's a big tip-off that fraud is being attempted," Taussig says.

ThreatMetrix also investigates attributes from mobile devices or tablets, which are increasingly used for online transactions and access to social networks. The importance of mobile devices cannot be understated; such cases can make up 20% of the transactions screened for specific customers.

New solutions are being recommended to defeat today's more advanced fraudsters. An example of these are the new authentication guidelines recently issued by the Federal Financial Institutions

Examination Council (FFIEC), which aim to help financial institutions take stronger safeguards against online fraud. ThreatMetrix provides the critical technology necessary to meet this requirement for using smarter device identification as a component of a layered security approach for banking compliance.

When combating online fraud, speed is essential. Historically, the ability of most organizations to respond to fraudulent activity was limited by the agility of their IT organization. Now, however, cloud-based solutions have tipped the scales in favor of legitimate commerce. "The unique thing about ThreatMetrix is that it was designed from the beginning as a cloud-based service," says Gartner's Litan, who ranked ThreatMetrix high in the esteemed Visionaries quarter of her 2010 Magic Quadrant for Web Fraud Detection. "This design minimizes the setup and support requirements while giving customers the granular data they need to make decisions in real-time about whether to accept, deny or review a transaction."

With fraudsters becoming better funded and more sophisticated, businesses must adopt and deploy smarter technologies to combat them. Otherwise, they run the risk of losing the war against fraud and, more important, their customers' trust and loyalty. ■

ThreatMetrix™
www.threatmetrix.com

About ThreatMetrix

Product:

ThreatMetrix™ Cloud-Based Fraud Prevention Platform

Location:

Headquartered in Los Altos, Calif. (in the heart of Silicon Valley); sales offices around the world and research and development in Sydney, Australia, and in California

Background:

ThreatMetrix was originally founded in 2005 as a research/consulting project with Australia for the purpose of preventing unwanted intrusions into its

sensitive military, communications and financial websites. After proving to be commercially viable, the company has attracted leading venture capital investments in both the United States and Australia.

Since launching its cloud-based service in 2009, ThreatMetrix has been installed for more than 600 customers worldwide. Customers include leading financial services companies and alternative payment providers, industry-leading payment processors, social networking sites and hundreds of the world's largest e-commerce companies.