

THE NILSON REPORT

For 40 years, the leading publication covering payment systems worldwide.

January 2011 ■ Issue 964

THREATMETRIX FRAUD PREVENTION

Fraudsters can now go online to buy tool kits that let them sit on one side of the world and attack merchants repeatedly on the

ThreatMetrix™

other side with each attack looking like it's coming from a different computer. The software alters data about a computer's browser, fonts, operating system, etc. to thwart security schemes that use this type of data to recognize suspect devices. It can also make certain that the computer hasn't left a cookie from a previous attack that would trigger a merchant's fraud defense system.

To combat these latest generation attacks, Web merchants need to deploy the latest in device fingerprinting. These state-of-the-art fraud tools can also detect so-called "clean fraud" perpetrated by criminals able to create the impression that the cardholder's billing address, shipping address, and the IP address of the computer are all in the same geographic area. This makes a transaction appear acceptable to the merchant's fraud fighting system, when in fact the criminal is using the IP address of a botnet computer located in proximity to

stolen payment-card and billing-address data.

Threatmetrix has been offering device fingerprinting fraud protection since 2005. Unlike competitors, who license software for onsite installation, are focused only on devices, or only on payment card transactions, Threatmetrix covers all areas in which a merchant needs protection — registration, authentication, or authorization. It offers an enterprisewide rules engine that screens in all three areas. And it operates solely on a hosted or "cloud" basis.

One benefit to a hosted approach is that Threatmetrix sees transactions from all of the merchants that use its technology. This allows it to generate risk scores based on previous incidents of other merchants' fraud without relying on manual reporting. Its device-identification technology also works against fraudsters using mobile phones if those devices are browser-based.

Threatmetrix formerly sold its service based on a multiyear subscription model basis, but now sells only on a prepaid basis.

CONTACTS

■ **U.S.** Alisdair Faulkner is Chief Products Officer in Los Altos, California, (650) 796-5466, afaulkner@threatmetrix.com.

■ **Europe** Stephen Topliss is Head of Sales in the Hague, the Netherlands, 31 (70) 820-0508, stopliss@threatmetrix.com.

Merchants sign up for a fixed amount of protection, then renew for an additional period if they like the service. The company says it has a 95% renewal rate, and that the 5% who don't renew are mostly merchants who have gone out of business.

Threatmetrix opened an office in The Hague, the Netherlands in December 2010, and a data center in London in September 2010. The company has received three rounds of venture funding totaling \$24 million.

**AN OFFICE WAS
OPENED IN THE
NETHERLANDS
LAST YEAR.**

Threatmetrix resellers include CyberSource, Verify, Activeidentity, Neovia (U.K.), ExperCash (Germany), Moneris (Canada), PagosOnline (Mexico), and ClearSale (South America).

Posted with permission from
The Nilson Report, Carpinteria, California,
www.nilsonreport.com