AUGUST 2002 ISSUE #770

THE NILSON REPORT

FOR 32 YEARS, THE LEADING PUBLICATION COVERING CONSUMER PAYMENT SYSTEMS WORLDWIDE

VISA/MASTERCARD WEB AUTHENTICATION

Card issuers and acquirers of merchant transactions never anticipated the levels of fraud associated with purchases on the Web. In addition to … ***(turn to page 6)***

GENERAL PURPOSE CARDS — MID 2002

During the first six months of this year, $920.90 billion in purchases and cash volume was generated by Visa, MasterCard, American Express, … ***(turn to page 8)***

MASTERCARD CONTINUES TO GAIN ON VISA

MasterCard's market share of outstandings on bank credit cards in the U.S. increased to 49.26% at midyear 2002 — up from 46.00% at midyear … ***(turn to page 9)***

SAGEM POS TERMINALS Consolidation continues among manufacturers of POS terminals with the acquisition by Sagem of Ascom Monetel's Electronic Transactions Business Unit. ***(turn to page 5)***

OFFSHORE CARD ACCOUNTS — PART THREE

In an effort to identify U.S. citizens who might be using offshore credit and debit card accounts to avoid income taxes, the U.S. Treasury Department's … ***(turn to page 8)***

DEBIT CARD LOYALTY PROGRAMS Every year financial institutions lose up to 25% of their deposit account customers because of problems with customer service or because prices charged for … ***(turn to page 4)***

HIGHER RETURNS FROM DEBT SALES

Purchasers of credit card debt in the U.S. currently pay portfolio owners up-front. Payments average 3¢ on secondary charge-offs (12-18 months … ***(turn to page 4)***

CARDMETER FOR TAXICABS Privately held Centrodyne is the largest supplier of taxi meters in North America. The company's new Silent 600 CardMeter authorizes credit cards in … ***(turn to page 5)***

CYBERCROOKS AND BROWSER ATTACKS

Ninety percent of the more than 500 large U.S. companies surveyed recently by the FBI and the Computer Security Institute said they experienced some type of Internet fraud last year, whether it was a defaced Web site, a server infected with a worm or a virus, or some type of theft. The most publicized attacks are launched through viruses and worms that spread quickly and randomly throughout the Internet. But the … ***(turn to page 10)***

THE NILSON REPORT: 300 Esplanade Drive, Suite 1790, Oxnard, California 93036 • FAX (805) 983-0792 • PHONE (805) 983-0448 • nilsonreport.com

How Hackers Target Card Issuers

1 Parameter Tampering

CRIME: **Fraud**

DEFINITION: Parameters appear at the top of a Web page as part of a string of data that follows the Web site's URL address.

TECHNIQUE: Hackers type over data in the parameter string to raise a credit card's spending limit or change the interest rate.

2 Hidden Field Manipulation

CRIME: **Fraud**

DEFINITION: Hidden fields in HTML source code can also store information about credit limits and interest rates.

TECHNIQUE: As with Parameter Tampering, hackers can type over data in the source code to raise a credit card's spending limit or change the interest rate.

3 Cross-Site Scripting

CRIME: **Hijacking**

TECHNIQUE: Hackers write false scripts that first access cardholder data, and then forward that data to a hacker's computer.

4 Cookie Poisoning

CRIME: **Identity Theft**

DEFINITION: Cookies are used by Web sites to establish and track the identity of a user.

TECHNIQUE: Hackers manipulate the data in the cookie to assume the identity of another user. They can then access all of that cardholder's accounts.

Cybercrooks (from page 1) … greater threat is from attacks that are both targeted and purposeful, orchestrated not for high-tech notoriety but for financial gain.

Cybercrooks have three ways of getting at sensitive data residing on a company's Web site — by accessing a server, intercepting a data transmission, or by attacking a Web application through a browser such as Internet Explorer or Netscape Navigator. Most companies use encryption algorithms to scramble transmitted data, and have installed network firewalls to protect their servers. But very few have protected themselves from attacks via a browser.

Sanctum, founded in 1997, has 275 clients in Japan, Europe, and the U.S. where it has signed 8 of the 10 largest financial institutions. Audits conducted on client Web sites found 98% had major problems that could be exploited by a hacker within a matter of hours. Such audits are called "ethical hacks" because they're authorized and are actual cyber break-ins. Like the online crooks, Sanctum's audit team looks for holes and shortcuts left behind by the programmers who created the server software. While firewalls assure that Web and application servers are only being accessed through correct network paths and ports, they do not prevent a cybercrook from manipulating the Web applications through browsers.

Types of crimes include stealing credit card numbers, culling data for identity theft, and hijacking or defacing a site. During one ethical hack, Sanctum was able to maneuver a Web site into issuing preapproved credit cards to two of the company's top executives. Not only were those cards unauthorized, but credit lines were upped from $10,000 to $100,000, and the finance charge rate was shifted from 1.9% to minus 1.9% so that the cardholders could have actually earned money by maintaining an unpaid balance. Sanctum's research and development is conducted in Israel. Corporate headquarters are located in Santa Clara, California, where Diane Fraiman is VP Marketing, (408) 352-2015, *dfraiman@sanctuminc.com*.

Sanctum markets two software products:

AppScan automatically assesses the vulnerability of a client's Web site applications. Reports identify all vulnerabilities and ranks them by severity.

AppShield works like a firewall but for Web applications rather than the network. It sits behind a network's firewall and in front of a Web server where it monitors traffic through the browsers to the back-end systems. Whenever an attempt is made to use an application in an unauthorized manner, the attempt is stopped, logged, and the administrator is alerted.

Both products work with any Web application and do not have to be modified to accommodate updates or additions. Clients can buy AppScan and AppShield and operate them in-house, or contract to have audits conducted by other Sanctum clients such as PricewaterhouseCoopers, IBM Global Services, or KPMG.

August 30, 2002

David Robertson, Publisher