

Hackers increasingly wreak havoc on industry

BY RON RUGGLESS

DALLAS — The criminal hacking of credit card data from restaurants' point-of-sale systems has been increasing, despite the industry's adoption of standards to protect customers' personal information.

Federal prosecutors this month indicted three suspects, two of whom were in jails in Turkey and Germany awaiting extradition, for allegedly stealing customers' charge card data from computers at 11 of the Dave & Buster's chain's

49 units. The data from just one branch was blamed by authorities for banks' losses of more than \$600,000.

Not Your Average Joe's, the 16-unit chain based in Dartmouth, Mass., still is dealing with the costly fallout from a data breach last year.

And the management of Fat City Inc. of Sacramento, Calif., remains mystified about how hackers apparently pilfered information about at least 20 customers and led to a \$90,000

fine against the restaurant group by a credit card issuer.

Some operators have paid a bigger price, experts say.

"The combination of hard costs and damaged reputation associated with these incidents has literally put restaurants out of business," said David Denney, a lawyer in Dallas who deals with many restaurant clients.

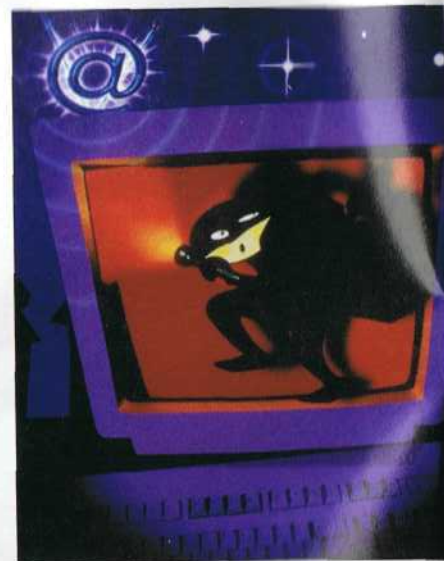
Hacking incidents have increased even as the foodservice companies have applied the controversial Payment Card Industry

Hackers and identity thieves have attacked many restaurant brands, even though the industry adheres to thorough PCI DSS standards.

Data Security Standards, or PCI DSS, which took effect in September 2006 and are undergoing a revision.

Restaurants have not been alone in being attacked by hackers, some of whom are said to have targeted foodservice firms after doing damage to other kinds of businesses.

(See **HACKERS**, page 58)



IHOP Corp. chief executive Julia Stewart said the Applebee's brand would transition to a mostly franchised business soon.



IHOP chief Stewart plans for Applebee's turnaround via major franchise growth

BY LISA JENNINGS

Also this week, Applebee's new employees were employed after taking over at

Restaurants get mixed reviews in survey of gay, lesbian consumers

BY ELISSA ELAN

With buying power estimated to exceed \$600 billion a year, the gay and lesbian community represents a potentially lucrative market for restaurateurs to tap. But some operators are doing a better job than others at attracting that audience as customers and employees, according to a recent survey of gay and lesbian consumer habits and brand perceptions.

Sponsored by Prime Access, an advertising agency specializing in reaching lesbian, gay, bisexual and transgender groups, and PlanetOut Inc., a media entertainment organization also serving the LGBT community, the survey found Seattle-based Starbucks to be among the country's most gay-

were perceived by respondents to be less gay-friendly.

The study, which was conducted by marketing research firm Clark, Martire & Bartolomeo, polled nearly 6,000 adults between the ages of 18 and 64. Respondents were broken up into three categories: a total of 757 came from the gay and lesbian community, another 1,502 were culled from the general population, and an additional 3,156 were PlanetOut subscribers and readers.

"There's been a lot of research over the years that showed gays and lesbians are highly loyal to brands they buy," said Howard Buford, president of Prime Access, "and our statistics show that between 68 percent and 72 percent of gay and lesbian consumers are

Hackers increasingly wreak havoc on restaurant industry

(Continued from page 4)

The suspect being held in Turkey in the Dave & Buster's case was identified as Maksym Yastremskiy of the Ukraine, who also is a key suspect in one of the largest hacker attacks ever. Massachusetts authorities have linked him to the breach of the computer system of TJX Cos. Inc. of Framingham, Mass., parent of the T.J. Maxx and Marshalls retail chains. Hackers in that attack, disclosed in January 2007, stole information from about 45 million credit cards and may be responsible for \$197 million in illegal purchases. TJX has so far tentatively agreed to pay MasterCard as much as \$24 million in possible losses and Visa as much as \$40 million.

Lawyer Denney said: "Any agreement signed with a credit card processor [or] merchant bank will require the operator to comply with PCI-DSS. After the restaurant pays for a full audit of the POS system — about \$10,000 — it will retain virtually all liability for cardholder damages, the cost of re-issuing cards [of] \$25 to \$30 per card, the credit card company's attorneys' fees, and fines and penalties charged by both the credit card



Not Your Average Joe's, which still is dealing with the fallout of a security breach last year, has a warning on its website apprising customers of the situation.

company and the credit card processor."

In addition, Denney said, "if a breach has occurred, the credit card processor can take from your bank account or withhold from processing upwards of \$100,000 based on its estimate of what its loss,

Not Your Average Joe's

NOT YOUR AVERAGE JOE'S
Credit Card Fraud Update

In late September, Not Your Average Joe's learned that our Massachusetts restaurants were targeted by an individual or individuals seeking to illegally obtain credit card data. We quickly took steps to further secure our system, notify the public and work with external investigators to identify the cause of the security breach. As a result, are confident that all credit card transactions happening at Not Your Average Joe's today are secure.

Based on our investigation, there are several important things our customers should know:

- The data was illegally obtained between early August and late September, impacted some customers who dined at a Not Your Average Joe's during that period; however, the information could be used at any time.
- The only information our company has access to are the credit card number, expiration date and name associated with the card.
- Though Not Your Average Joe's does not have any other identifying data (such as social security number, address, date of birth), you should still treat this issue seriously and carefully monitor your credit report for possible identity theft. To do so, you should contact one of the three major credit reporting agencies.
- We have been informed that some customers whose data was obtained have had fraudulent charges placed on their credit cards.
- If a customer had fraudulent charges placed on his or her card, he or she should not be held responsible for those charges; the problem can be resolved by calling your credit card company, reporting the issue and cancelling the card.

We encourage all customers who dined in our restaurant during the August and September timeframe to check both past and future credit card invoices carefully for unrecognized charges, which could indicate fraudulent activity.

fines and/or penalties might be."

Dave & Buster's, in a statement, said it was alerted to the hacking last August and immediately contacted the U.S. Secret Service. While Dave & Buster's aided

the government investigations, the company said, it also retained outside security experts who identified the source of the misused data. The company said it had implemented additional security measures to prevent any more such incident from occurring.

The 11 Dave & Buster's that were compromised are two units in Dallas and branches in Westminster, Colo.; Islandia, N.Y.; West Nyack, N.Y.; Utica, Mich.; downtown Chicago; Columbus, Ohio; Jacksonville, Fla; Austin, Texas; and Frisco, Texas.

Neither the company nor the government indicated the full extent of losses from the data breach. The Justice Department said that from one restaurant alone, "packet sniffer" code was used to capture data taken from about 5,000 credit cards, which then was sold to others who made purchases on the accounts. The theft from that indi-

vidual restaurant eventually caused losses of at least \$600,000 to issuing financial institutions, authorities indicated.

Dave & Buster's said it does not store credit or debit card numbers or customer names. It said information to help in the identification of affected cardholders was provided to the credit card companies by Dave & Buster's and Chase Paymentech Solutions LLC.

"As soon as we became aware of the breach in August 2007, we took steps to secure our systems and remain confident that they are safe today," said Steve King, chief executive of Dave & Buster's. "We thank the Secret Service and the Department of Justice for their diligence in arresting and prosecuting those responsible for this crime and look forward to working closely with them during the pendency of this criminal matter."

In addition to charges against Yastremskiy, the 27-count indictment also charged Aleksandr Suvorov of Estonia with wire fraud, identity theft and intercepts of electronic communications. Albert Gonzalez of Miami was charged with wire fraud conspiracy related to the scheme.

Not Your Average Joe's, which still warns customers about the data breach at its website, said it has upgraded its computer security but that some customers have had fraudulent charges placed on their credit cards.

The chain indicated that it couldn't describe its safeguards "without compromising ongoing security," but that it believes all data transmittals now are secure.

Bravo! Development Inc. of Columbus, Ohio, recently upgraded its computer security system for its 71 Bravo! Cucina Italiana, Brio Tuscan Grille and Bon Vie Bistro locations.

Kathleen L. Chugh, Bravo's vice president of information technology, said: "We are concerned about protection of our consumer data. There are new threats and approaches to gain access to the data that are a threat to all of us."

She said the new "universal threat management" device that Bravo installed "provides us the intrusion prevention and alerting that we need to address potential threats or security concerns."

On May 14, the PCI Security Standards Council, a group of credit card issuers and processors, announced that it will be releasing a new version of the PCI Data Security Standard, version 1.2, in October.

The upgrade should "minimize the risk of data breaches that can challenge the positive public perception of the security practices of merchants and financial institutions," said the council's general manager, Bob Russo.

As more restaurants offer free Wi-Fi Internet access, that "can be an open door to hackers if your POS

delete it. Furthermore, if you are storing old credit card slips that contain sensitive data, shred them or ensure they are secure."

The fallout from a data breach not only costs money but also depletes the good will of patrons and financial backers, he warned.

"Shaken investor confidence can decimate the stock value of public companies just as easily as broken trust can destroy an independent's good will within a community," Denney said. "The real question is whether to keep the breach quiet or go public.

"While most restaurants would prefer that the information remain undisclosed, the ramifications would likely be even worse if it looked like the restaurant was trying to cover it up.

"If a security breach is discovered, you should take steps to rem-

edy it and protect against future hacks, and any press release disclosing the breach should always be accompanied by a statement of what's being done to protect customers." ■

rruggles@nrn.com

Once you get involved, you'll understand.



Why is this man such a fan? Is it because his SIFE students just won an award for their contributions to the community? Maybe it's because of the tremendous emotional gratification that he gets from participating in the experience. Perhaps it's due to the fact he found a couple of future employees. Or maybe it's just because he likes to be on a winning team. No

FS/TEC panel offers insights into revised PCI security standards

BY PAUL FRUMKIN

ORLANDO, FLA. — Even as the foodservice industry and other businesses digest the latest version of the Payment Card Industry Data Security Standards, experts agree that operators will have difficulty achieving full PCI compliance and completely protecting credit and debit card information.



Payment card security stakeholders speaking at the 14th annual International Foodservice Technology Exposition, or FS/TEC, here in February acknowledged that PCI DSS Version 1.2, while improving on the initial release, nonetheless is no silver bullet.

"One-hundred-percent compliance is almost impossible, at least as far as I'm concerned," said Ci-

han Cobanoglu, associate professor of hospitality technology at the University of Delaware.

The standards were established to help ensure the adoption of consistent data security measures and enhance payment account security. Noncompliance by businesses accepting card payments can result in stiff financial penalties from card organizations.

Underscoring the difficulty businesses have protecting sensitive credit-card data from hackers

and other thieves, Cobanoglu cited a study that found the number of events in which card data were compromised more than doubled in 2007 compared with 2006. The vast majority of those problems, he continued, involved track data, which has a credit card number and an expiration date.

Other experts taking part in the payment card security panel discussion pointed to the recent breach of Heartland Payment Systems. In that breach, intruders

hacked into the computers used by Heartland to process payment card transactions for 175,000 merchants, including approximately 60,000 restaurants.

They also referred to an earlier breach at the Dallas-based Dave & Buster's casual-dining chain, in which three men allegedly hacked into multiple cash registers to steal data from thousands of credit and debit cards. Associated losses from that breach have been estimated at \$600,000.

Cobanoglu said fine-dining restaurants suffered the most in the restaurant industry from not being PCI-compliant. He pointed out some common barriers to compliance, including limited budget, lack of education, lack of tools to manage PCI, lack of qualified staff, and lack of details with the standards.

PCI DSS Version 1.2 clarifies some of the confusion among merchants raised by the initial release, but not all of it, observed David Starmer, vice president of information technology for Back Bay Restaurant Group in Boston.

The largest rewrite, he said, occurs in Requirement 1 — the standards have 12 requirements or standards — which states that routers are now included and should be treated the same as firewalls. Moreover, the new requirement restricts WEP, or wired equivalent privacy, deployments. According to the new regulations, new WEP implementation was banned as of March 31, 2009, while current implementation is banned after June 30, 2010.

Under the first release of PCI DSS Requirement 6, patches to software needed to be applied in 30 days. Now the standards condone a risk-based approach, which Starmer called “a little more prudent and realistic.” At the same time, he noted, “they tell you that you have to validate input, proper error handling, secure storage and others.” What’s more, the BBRG executive indicated, Requirement 6 now requires code review for common vulnerabilities or an application layer firewall in front of any Web-facing application.

Other changes incorporated into Version 1.2 mandate that operators set up cameras or other access control mechanisms in any data center or server room, and test for the presence of wireless points using a wireless analyzer on at least a quarterly basis, Starmer said.

David Denney, a practicing restaurant and hospitality industry attorney with The Law Offices of David Denney in Dallas, warned attendees, “The cost of noncompli-



From left: David Starmer, Back Bay Restaurant Group; David Denney, hospitality attorney; and Cihan Cobanoglu, University of Delaware.

ance is incredibly high.”

He said that under the standards, restaurateurs retain virtually all liabilities, including responsibility for charge backs, cardholder damages, the cost of reissuing stolen cards, credit card company attorneys fees, and fines and penalties for not being compliant.

“It can end up costing hundreds of thousands of dollars,” Denney said. “You know things are bad when insurance companies are writing policies for the problem.”

Denney advised attendees to

conduct a background check on employees who have access to cardholder data, but acknowledged that the practice can become “a paperwork mess” because of turnover. He also said franchise agreements generally shift the burden of compliance to the franchisee, but often franchisors fail to sufficiently educate the licensee about credit card security.

If a credit card system is breached, Denney advised, operators should immediately inform their legal counsel or counsel for

their franchisor, begin an investigation, take immediate steps to remedy the perceived threat and draft a press release utilizing the counsel’s input.

In general, though, panel participants advised attendees to review the policies and procedures in Version 1.2, and make sure they have adopted the changes.

“If you’re not compliant, you’re probably in good company because that’s most organizations,” Starmer said. “If you’re compliant today, you may not be tomorrow. It’s a moving target we’re after.” ■

pfrumkin@nrn.com

**Scenes or words from the annual International Foodservice Technology Exposition, or FS/TEC, produced and managed by Nation’s Restaurant News with Robert N. Grimes of Accuvia. FS/TEC 2010 is Feb. 21-24 at the Long Beach Convention & Entertainment Center in Long Beach, Calif. More information is available at www.fstec.com*