Management

NEWSLOG

JetBlue Airways and Singapore Airlines announced a codeshare agreement
Air Canada named airline industry vet Duncan Bureau to serve as vice president of global sales

STORIES

Cisco Developing Cloud-Based Virtual Meeting Rooms
Newly Combined Cendyn Arcaneo Unveils Meetings Tech Platform

Travel Management

NEWS FOR TRAVEL MANAGERS

Plugging The Breach: Recent Violations Of Data Security At Major Retailers Raise Concerns About Travel Industry Vulnerabilities And Strategies To Limit Them

May 28, 2014 - 02:10 PM ET

By **JoAnn DeLuna**

The recent spate of high-profile credit card data breaches, most notably at retail giant Target, primarily has affected consumer cardholders. But business travel suppliers haven't been immune to similar breaches, to which such hotel companies as Wyndham and White Lodging could attest.

Travel managers, like consumers, to some extent must rely on faith that their suppliers are effectively thwarting any effort by scammers to swipe their travelers' data. But they do have some opportunity to require suppliers to clarify their plans, and can help themselves by ensuring their payment processes are as secure as possible.

"Data privacy is more than just credit card numbers that we need to be concerned about," said DHL category manager of travel services Michelle

Hunt. "It involves phone numbers, access to emails and any personal information we provide through loyalty programs and to the hotelier making the reservation."

Even before the high-profile cases came to light, advertising holding company Interpublic Group already was in talks with its suppliers to ensure data-privacy policies were up to date to protect both intellectual and personal employee data. IPG also is requiring suppliers to indemnify the company with $10 million in the case of a data breach, said Fran McClarnon, Interpublic Group executive director of global travel and corporate credit card services.

"Some vendors within the industry have not reached the point where they're worried about [data breaches] because they claim they haven't had any and don't expect to have a breach—but, of course, nobody ever knows," McClarnon said.

"It doesn't have to be malicious," she continued. "You only have to have one angry employee or an employee who doesn't do [his or her] job properly and sends the data to someone else. Whether it's a mistake or malicious, it doesn't make a difference once you've been affected."

McClarnon said data-infringement cases are complicated because all countries have different laws and requirements for data protection. A data breach can cost a company in the "high six figures," in addition to the cost of lawsuits and hiring companies that ensure employees' personal data are not used in fraudulent ways after a violation occurs. "It's a very complex subject," she said. "We're taking the stand that if you want to be one of our vendors, we have to be protected."

Credit Card Fraud

Global credit, debit and prepaid card fraud losses in 2012 totaled $11.27 billion, according to The Nilson Report's latest figures. Several banks, corporate card issuers and payment networks recently told *Business Travel News* that they continually monitor the payments landscape to prevent such breaches as well as to establish measures that control fraud and keep personal data secure. However, they declined to comment on specific efforts so as not to educate hackers on their initiatives.

"We normally never talk about whether or not we have breaches, as we don't want to tip our hats to fraudsters," said Steve Pedersen, BMO vice president of corporate payment products for Canada and corporate cards for North America. "Those are all things we monitor vigorously and continuously as an institution."

A preliminary White Lodging investigation revealed that malicious software during the period of March 20 to Dec. 16 last year was used to steal credit and debit card information on point-of-sale terminals used at food and beverage outlets at 14 hotel brands, according to a February 2014 statement from the company.

Compromised hotel brands included Marriott, Holiday Inn, Sheraton, Westin, Renaissance and Radisson, from which stolen data contained such customer information as names, credit and debit card numbers, security codes and card expiration dates, according to White Lodging's statement. The investigation is ongoing, and White Lodging did not respond to a request for comment.

"[The White Lodging incident] is incredibly relevant and business travel could be affected," said John Buzzard, product manager for fraud banking at analytics software provider Fico. "On many occasions—my own included—you fly in to a remote location for a meeting, eat at the hotel or have a meeting in the lounge. What are the odds that business travelers were not affected?"

The U.S. Federal Trade Commission in 2012 filed a lawsuit against Wyndham Worldwide Corp. and three subsidiaries over the computer security lapses that allowed hackers to steal data on more than 619,000 consumer credit card accounts. Wyndham requested a case dismissal, but a U.S. district judge last month rejected the request.

As investigations continue, Buzzard said he wouldn't be surprised if investigators discover more affected organizations, and wondered whether all the incidents, including the Target and Neiman Marcus cases, were related.

"It feels like a full-on assault and rather extreme," Buzzard said. "I don't know if we'll finish the year with more revelations in terms of more data breaches, but it seems like such an evolving environment right now," he said.

The Evolution Of Fraud

In the late 1990s, the average age of credit card fraudsters was about 15, according to Dave Britton, vice president of industry solutions at online fraud prevention provider 41st Parameter. "They were mainly dumpster-diving for credit card numbers from receipts and then buying online," Britton said. "But now it's turned into highly industrialized organizations of fraudsters where different groups specialize in what they do."

In the "fraudster underground" one group may be responsible solely for building malicious software (or malware), a different group will perform the attack, another group will purchase the data or act as an "underground broker" for the stolen data, while yet another group might be responsible for creating the counterfeit cards and transacting online, Britton explained.

Offenders typically aren't based in the same country where the theft occurs and often operate in Eastern Europe or Southeast Asia, which further complicates tracking the perpetrators, according to Britton.

In such operations the stolen card numbers may not be used immediately, so a customer's card may be compromised without the user realizing it, according to Volker Huber, then AirPlus executive director of marketing. (Huber since has departed AirPlus.)

From 2005 through 2014, 4,246 payment card fraud and hacking breaches have compromised more than 864 million data records, according to figures from Privacy Rights Clearinghouse.

"There's a lot of data out there in the underground and it's gotten cheaper to trade complete sets of privacy data, including card numbers, 3D Secure codes—they have it all," said Britton. "Not all cards will be used, but the focus is on high-value payment cards."

As corporate cards tend to have higher spending limits with "stranger spending patterns" than do consumer cards, "you can see why fraudsters might target those cards," Britton said.

Typically, when a breach is discovered, the card immediately is closed and a new card is sent to the user. However, because replacement cards can cost between $17 and $25 each, Britton said card issuers don't always "proactively reissue cards."

"They could, but the costs would be so prohibitive," Britton said. "So, they do what good managers do and balance the possibility of fraud or risk happening on cards with the cost of reissuing the entire batch."

BMO's Pederson said: "As an industry, we look at analytics and spend patterns, and when we start to see a pattern that looks incongruent, it triggers red flags.

"If we get suspicious of a breach we reach out to customers, and even if it's not fraudulent activity we may still initiate a card replacement."

Similarly, AirPlus also immediately closes and exchanges cards when it discovers a card has been compromised. "Even if there's no fraud on the card, we want to make sure we have a clean card," Huber said.

The Case For EMV

Card issuers and payment networks have championed chip-and-PIN or EuroPay MasterCard Visa (EMV) technology as the primary solution to credit card fraud. These cards have embedded microchips that authenticate transactions and which users verify with personal identification numbers, making the transaction process more secure than with magnetic swipe cards.

While the United States is set to fully transition to chip-and-PIN cards by October 2015, other countries adopted the technology as early as 2001. Some U.S. banks began issuing chip-enabled cards in North America in 2011, but typically they only were issued to senior executives who frequently traveled overseas. In efforts to speed EMV adoption, Bank of America Merrill Lynch in April began issuing chip-and-PIN cards for all newly created corporate travel and expense accounts, with existing cards set to be replaced with chip-and-PIN at the time of renewal.

AirPlus claims chip-and-PIN cards reduce its fraud by about 90 percent. "We previously were confronted with [fraud], and the first thing we did was introduce chip a few years ago," said Huber. "Chip tremendously reduced fraud even when the data was hacked."

Online Protection Needed

While chip-and-PIN helps reduce in-person fraud, it consequently drives fraud online to so-called card-not-present transactions. CNP represented 23 percent of the United Kingdom's 2007 card fraud volume, comprising skimmed and cloned cards, of £144.3 million ($241.7 million), according to U.K. Card Association figures. While total U.K. card fraud by 2011 declined 70 percent to £42.1 million, CNP's share spiked to 65 percent.

"In every country that has implemented chip technology, their counterfeit card [rate] drops, but the path of least resistance is online and it's the only way fraudsters can get what they want and transact," said Fico's Buzzard. "The whole purpose of chip-and-PIN is to prevent a card-present customer in front of ATMs or retailers from a counterfeit purchase. Will chip-and-PIN stop fraud for card-not-present transactions? No, it won't."

Card transaction processor TSYS in a 2013 white paper suggested combining EMV technology with 3D Secure, a Visa-created technology that allows users to authenticate themselves for online purchases using three domains. Visa's product is branded as Verified by Visa, while Secure Code and SafeKey are the MasterCard and American Express versions, respectively.

Before users complete an online purchase, the card network prompts them to enroll in 3D Secure by creating a password authentication. Enrolling is optional, but some merchants don't allow customers to complete a purchase without enrolling. This extra protection has increased the abandonment rate for merchants, according to Britton. "Adoption rates [of 3D Secure] are so low, and it has not proved to be useful," he said.

That consumers aren't liable for online card losses is a major reason 3D Secure adoption rates are so low, according to Britton. In North America and Europe, issuers are liable for fraud loss in card-present transactions, while merchants are liable in CNP transactions, Britton explained. "As a consumer, you're not liable for card loss either way and are perfectly protected, so why should we bother with extra hurdles?" he said.

Liability

Although consumers are protected, corporations typically become liable in cases of employee misuse, which DHL defines as employees using a corporate card for unauthorized or personal purposes, or any purpose that violates a company's policy. Fraud is classified as someone other than the cardholder unlawfully obtaining the credit card or credit card number without authorization.

"Most (theft) instances on company card programs are not fraudulent use—it's misuse by the employee," DHL's Hunt said. "Travel managers need to query suppliers during the RFP process to ask about misuse and what coverage card providers have [for] employees in those situations."

While corporations typically are responsible for charges in such situations, some card issuers will assume some or all liability if the organization fulfills certain requirements, such as reporting the incident within a specified time frame and terminating the offending employee, Hunt explained.

Additionally, travel managers should remember that merchants are also customers of payment networks, so the networks have a stake in protecting the merchants. "We had a situation where a person was misusing the card and we tried to do something about it, but the credit card protected the merchant," Hunt said. "That's very frustrating in a managed card program where we're doing everything we can and the card company is allowing

things to happen that we didn't authorize."

Pairing a card program with an automated expense system also helps prevent employee misuse, as employees have to report and classify every expense.

Other Measures

Unlike consumer credit cards, corporate T&E cards can have additional features to help organizations manage card usage. Depending on the card provider, program administrators can switch off usage for specific geographies, types of merchants and cash advances.

However, restricting individual merchants is limited by the classification of merchant categorization codes, according to Hunt. Although companies can restrict, say, retail purchases by turning off that merchant code, Hunt said some merchants register under any category they choose, and a single company can sign up for multiple codes. For example, DHL uses a European airline that is listed as retail.

"At least once every quarter I have one person who tries to buy a ticket and is declined," Hunt said. "It makes it more complicated than it should be to manage a corporate card program."

As with consumer cards, business travelers also can set personal preferences to receive alerts for large purchases or card-not-present transactions, among others. However, Buzzard cautioned against setting so many alerts that they become spam and results in travelers ignoring them. "It's important for business travelers to sit and question themselves on how they typically use the card and they want to construct alerts based on that," Buzzard advised. Travelers also should avoid using cards at questionable establishments.

Huber advises program managers to match card limits to the amount of traveling employees do—the less travel, the lower the limit. That way, even if a breach happens on a card for less-frequent travelers, the damage won't be extensive.

Prepaid and virtual one-time-use cards are other alternatives to credit cards: They limit the incidents of credit card fraud by allowing managers to add specific amounts of funds to the cards.

This report originally appeared in the May 12, 2014 edition of *Business Travel News*.

Leave your comment:

Comments