How Serious Are You About Identity Theft?

Avoiding Costly Mistakes

By Jaymi Curley

A great restaurateur is constantly thinking about his customers and what will serve them best. Sourcing the freshest ingredients, innovating with new recipes, ensuring that the service is top flight and the décor is inviting. There are a million details that compete for attention in the mind of the restaurateur, but often one of the most important services to customers is overlooked: the protection of the customer from ID theft.

Identity theft is a hot issue across the retail world. In 2006 alone, the number of adult victims of identity fraud in the U.S. was in excess of 8 million, according to a survey by Javelin Strategy & Research. Most consumers are acutely aware of the problem, but many associate it with Internet usage. Data collected by Ambiron TrustWave suggests that approximately three out of every four instances in which payment card data is compromised happen in a brick-and-mortar retailer. According to Visa U.S.A., four in 10 instances of this type of fraud can be traced back to restaurants.

The most common form of internal threat to a restaurant is through a process called "skimming." Using an easily obtained $300 device called a skimmer, an employee who gains access to a patron's credit card can quickly steal the credit information embedded in the magnetic stripe on the reverse of the card. This information is more than enough to print duplicate credit cards and is very valuable to a criminal enterprise. It is estimated that around 70% of the more than $1 billion a year that is lost due to skimming occurs in restaurants.

The remedies for this type of fraud are second nature to a good restaurant owner. In the first place, a thorough background check needs to be conducted on any potential hire. Before the employee begins work, it is advisable to have a one-on-one discussion with each employee conveying the restaurants safeguards to prevent fraud. In addition, the restaurant's policies regarding employee theft or fraud should be outlined in detail in the employee manual, with emphasis given on the penalties for such behavior, most commonly immediate dismissal and prosecution to the fullest extent of law. All of these measures can work to discourage criminal behavior from within, as the greatest targets of this type of crime are those restaurants that appear to have evident vulnerabilities in their security measures.

ID theft can happen in a split second. Protect your customers from ID Theft.

One way of minimizing internal theft is through the use of wireless pay-at-table technology. A relatively new technology in the United States, the use of this small handheld allows the customer to retain his credit card and simply swipe it through to pay the bill at the end of a meal. The devices operate on a secured local-area wireless network and are being touted as the next great innovation in payment-card security. Currently, the penetration of these devices into the restaurant market has been minimal. While a few larger chains are beginning to adopt the pay-at-table device, the cost of the system — which may run as

high as $500 per terminal — gives the average independent restaurateur pause, and may still not address an even greater threat. "Pay-at-table devices may thwart skimmers," said Joe Finizio, Executive Director of the Retail Solutions Provider Association (RSPA). "But the biggest criminals are getting in from the outside."

Charles Hoff, an officer of the Georgia Restaurant Association, agrees, "The external threat to restaurants is much greater. Employee skimming makes the news, but an external hack can compromise the data of thousands of cardholders in one fell swoop."

Sadly, smaller restaurants and retailers have become the favorite targets of professional thieves interested in attacking vulnerable systems. Larger restaurant chains can afford dedicated IT teams to maintain a constant vigilance over their point-of-sale (POS) systems, firewalls and networks. But for the small restaurant the cost can be prohibitive. "Independents worry about the day-to-day operations," said Finizio. "Most don't have the resources for a personal IT staff. They have to go it alone."

Unfortunately for the restaurant owner, a system compromise can occur before they are even aware of it. A system that has been breached gives no outward sign that criminal activity is taking place. Carla Yarborough, owner of Spanky's Marshside, of Brunswick, GA, was a victim of an external hack beginning in August 2006. Speaking out about her experience on a DVD produced by the RSPA as a part of its merchant education efforts, Yarborough relates her story, every restaurant owner's nightmare. "What had happened in our case was we were hacked into and the magnetic data, which I didn't even know that we were storing in the hard drive, was taken, and then new cards were made and sold over the Internet." Like many victims, Yarborough did not learn of the thefts until almost seven months later, when she was

contacted by her merchant bank to make her aware of the breach. "I just felt like I had been blindsided by something," said Yarborough, "because I was just not aware that could ever happen to me, or to us."

Preventive measures are available to restaurant owners, but efforts on the part of solutions providers to bring restaurant POS systems into compliance have been met with some resistance. Finizio says, "Often there is a pushback on the part of the business owner. If they feel the system they have is running great, they see no reason to upgrade." However, according to Ambiron TrustWave, in nearly 60% of the cases where a merchant's system was compromised, the merchant was relying on an outdated version of solution software of hardware for protection. "On average, the cost of compliance, including hardware, software and a service agreement that allows for upgrades may cost up to $10,000," said Finizio. Some merchants may feel the cost of a newer system is too high and may be in denial about their restaurant's vulnerability. However, the potential costs after a security incident can be much higher in the long run.

"There are substantial fines and penalties involved if the restaurant is found to be out of PCI compliance," said Hoff. "No one is impenetrable, and the card companies are shifting full and complete responsibility to the restaurants." After a compromise is discovered and the restaurant owner is notified by the bank, he or she is first responsible for arranging an independent forensic audit of the POS system in question — to the sour tune of $10,000. Next, the bank can charge fines up to as much as $40 per card for the stolen numbers, whether or not the numbers were used to commit actual fraud. From there, the owner is expected to repay any actual fraudulent charges that may have been made due to the compromised data. In addition, the bank can place a hold on funds from each future credit card transaction in order to offset the costs of potential fines the restaurant owner may be unable to pay. "They can take money and hold it," said Yarborough, "because they [the merchant's bank] may be fined by Visa or MasterCard. They don't want to take the risk of getting their money back from you, so they are going to keep it over there and make sure those fines are taken care of."

Security Safeguards

By Charles Y. Hoff, Esq., Hospitality Practice Group, Taylor, Busch, Slipakoff & Duma, LLP

To protect your restaurant from ID theft you have ordered pay-at-table credit card devices and changed customer receipts to no longer show credit card numbers or expiration dates. Now you can relax and quit worrying about ID theft, right? WRONG. The greatest exposure still remains, putting restaurants out of business overnight.

All restaurants are at risk of misused credit card data and are targeted more than other retail establishments. Your problems usually begin when notified by the credit card processing company for Visa, MasterCard, American Express or Discover. Their fraud departments notice irregular patterns of consumer credit card usage picked up from your location. They suspect the security of your internal computer network system may have been compromised. Basically, they feel your system was hacked by intruders intent on stealing credit card information from your internal database or point of sale network.

Once this occurs, you don't have much time to think as your credit card processing firm advises you must promptly hire, at your expense, one of a select number of forensic inspection companies to come into your establishment and perform an investigation of your security system. Your contract with the credit card processing company typically states the merchant bank can also withhold up to six figures of credit card payment while they make their determination of the situation. This can lead to massive fines or penalties to your restaurant upwards of $600,000, regardless of whether there are any credit card chargebacks.

At this point, you may encounter some sleepless nights wondering if you can afford these penalties, what your cash flow situation will look like, if the card companies will cut the use of their cards and the potential adverse publicity resulting in eroded business.

How can this nightmare be avoided? Each restaurateur needs to select a reputable point-of-sale (POS) vendor and/or make sure your POS vendor has updated software by the Payment Card Industry Data Security Standards (PCI DSS). You also need to understand the contractual obligations imposed upon your restaurant by the PCI DSS. Their suggestions on how to build and maintain a secure network are outlined below:

1) Install and maintain a firewall configuration to protect cardholder data.
2) Do not use vendor-supplied defaults for system passwords.
3) Protect stored data.
4) Encrypt the transmission of cardholder data across open, public networks.
5) Use and regularly update anti-virus software.
6) Develop and maintain secure systems and applications.
7) Implement strong access control measures.
8) Restrict access to cardholder data by business need-to-know.
9) Assign a unique ID to each person with computer access.
10) Restrict physical access to cardholder data.
11) Regularly monitor and test network.
12) Track and monitor all access to network resources and cardholder data.
13) Maintain a policy that addresses information security.

What steps should you take when a victim of a credit card breach?

1) Do not alter the suspected system.
2) Attempt to isolate the system (if practical, unplug the system).
3) Change system and user passwords (but not "root" ones).
4) Change network passwords.
5) Preserve all logs and reports.
6) Contact your merchant acquirer and other card brands if they have not contacted you first.
7) Contact law enforcement.
8) Record in written form all actions taken and when.
9) Anticipate a forensic data investigation.
10) Consult with knowledgeable legal counsel.

Most importantly, become educated to this issue so that your establishment can be proactive. Don't let yourself, your patrons or your restaurant become one of many needless victims.

Not only does the owner stand to lose potentially hundreds of thousands of dollars, but there is also the additional worry about a loss of trade. T.J. Maxx, in a highly publicized case, lost $4 billion worth of capital following a massive security breech of their POS systems, which resulted in the compromise of over a million card numbers. Loyal customers may take their business elsewhere if they discover that their favorite lunch stop or family dinner restaurant hasn't done enough to protect their valuable personal financial information. Often times, a security problem is handled quietly to avoid tarnishing the public image of the eatery. "Restaurants have a tremendous sensitivity to this issue. No one wants to invite negative publicity," said Hoff, who has assisted restaurants in defending themselves in arbitrations with card processing companies.

Finizio emphasizes the need for restaurateurs to take immediate steps to ensure their systems are PCI DSS compliant. "The business owner has to first admit that there is a potential threat, then find a reputable vendor and work with them bringing your systems up to compliance. Find out what, if any, data is being stored on your system and try to eliminate the practice as much a possible. You don't need it."

Hoff agrees that the restaurant owner needs to "understand the issues, and get educated on the solutions," as well as to "collaborate" with a solutions provider. However, Hoff also charges the third-party vendors with doing more to help the restaurateur meet his compliance goals. "Vendors need to make sure they are spending the time with individuals, going over the fine print." Hoff further taxes the solutions vendors with offering service at a reasonable price point for the small restaurant owner. "The restaurant business is known for its slim margins. Most of the little guys don't get into it to get rich. Vendors need to recognize this and try to provide good service at a fair price for the little guy."

At any rate, the problem of payment-card theft is unlikely to diminish in years to come, so it is important that restaurant owners take their security needs into account as part of the cost of doing business. The risks are too great to ignore the problem.

"It's sad," said Yarborough, "because it's like the small businessperson is taking the brunt of the whole thing because somebody is out there breaking the law. We're the ones who have to pay for it. One way or the other." ■