

Restaurant Technology

Is Your Restaurant Secure?

By Christy White

You go out for dinner and leave with your identity stolen. It sounds crazy, but it happens every day — and it could very easily happen in your restaurant, too.

With new POS applications and equipment for the hospitality industry, however, the likelihood of credit card theft happening in your restaurant can be greatly reduced.

RESTAURANTS POPULAR FOR SKIMMING

According to Federal Trade Commission statistics, credit card fraud is now the most common form of identity theft.

Much of that fraud is due to a practice called skimming, which is when a restaurant employee swipes the credit card through a device that records the account information (*see sidebar on page 27*).

It's a practice that has been around for more than a decade, but as technology has led to smaller skimming devices, frequency has jumped dramatically in the past three years. Credit agency TransUnion estimates that 70% of all skimming takes place in the restaurant environment.

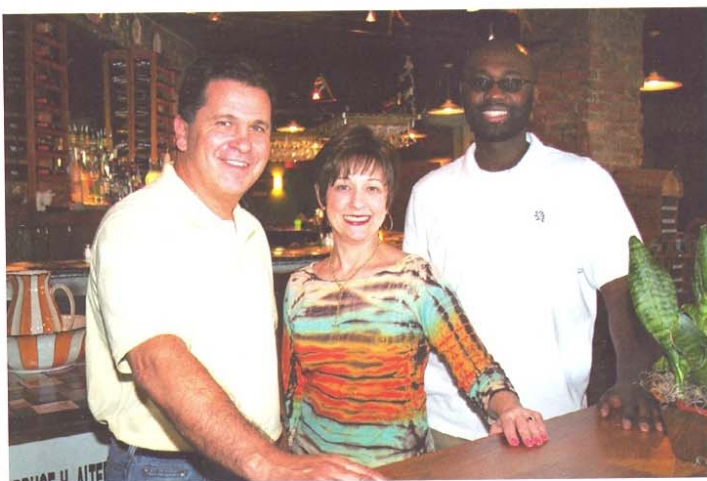
HANDEHDS HELP REDUCE LIABILITY RISK

So what can restaurants do? If even just one credit card number is stolen or compromised, the restaurant is liable for any losses.

Bruce Alterman is one restaurant owner concerned about protecting his patrons' credit card numbers. He decided to implement a handheld transaction device that processes credit cards at the table in full view of the customer to reduce the potential for credit card fraud. "There were two major components that were enticing. No. 1 is the security. The other is the hope that we'll turn tables. It's always a bottleneck when we're busy," says Alterman, who owns The Brickery in Sandy Springs.

The restaurant, which seats 135 and averages 2,500 patrons a

Bruce and Sally Alterman, owners of The Brickery Bar & Grill, along with David Nerquaye-Tehleh, the restaurant's manager.



week, has had the system in place since April 2007. Previously, The Brickery used two slide terminals, one at the bar and one on the floor. Now, there's one system hardwired at the bar and four handheld terminals.

By using a handheld device at the table, it not only speeds up the entire payment process and increases table turns, it also frees up server time. Most importantly, it gives an added layer of protection for patrons wary of identity and credit card theft.

Such handheld equipment has been around for years in Europe, but the trend is just now jumping the pond. Bruce is only one of four restaurant owners in Georgia using the handheld device.

The process mimics what is usually done away from the table, but he hopes to phase in the use of debit cards and the ability for patrons to slide their own cards through the machine. The equipment also has the capability to process tip percentages, so patrons simply push a button to add the desired tip to the total bill.

UPGRADE OR BUY NEW?

Many restaurants, whether large national chains or local family-owned restaurants, are still using POS systems that retain credit card data from its magnetic stripe, and it's only gotten easier for thieves to swipe that data without the restaurant or patron discovering it until it's too late.

POS manufacturers are well aware of the liability issues, and many have come out with software upgrades and new products that help restaurant owners avoid skimming all together.

To determine if you need to upgrade your POS system or purchase a compatible component, it's important to ask a few questions about your existing POS system. Does it retain information in the unit or send it to a remote server? How long is the information stored? Is the data encrypted?

According to Visa and MasterCard, restaurants are at high risk of being compromised if they use payment applications that store prohibited data or have security weaknesses. If a POS system stores full magnetic stripe data, CVV2 or PIN data following transaction authorization, it is in violation of the Payment Card Industry Data Security Standard (PCI DSS).

Handheld devices allow for scanning credit cards at the table, and many can be incorporated into a restaurant without the need to upgrade existing software. There are several handheld products already on the market, including Vantage Card System's On the Spot, used by The Brickery. The system uses special encryption to protect financial data transacted over a restaurant's WiFi network, and allows restaurant operators to take advantage of lower-cost PIN debit payment.

"It's all encrypted data, and there's nothing actually stored in the terminal," says Ty Hardison of Vantage Card Services, Inc. "Like a lot of POS systems out there, restaurants may unknowingly be storing

Skimming at a Glance

The art of skimming has been around for a decade, but with new technology and smaller devices, the number of incidents has risen dramatically over the past few years. Skim artists typically target gold or platinum cards because of their higher credit limit, which means it may take longer to discover what's happened. While the whole process can take less than a day, the victim is none the wiser since his own credit card is safely stored in his wallet. Here's how it works:

1. A customer uses a payment card to pay. The wait staff walks the credit card to the transaction station.
2. After leaving the table, the employee secretly swipes the credit card through a small, concealed handheld device to copy and store the account data. Many of these devices are so small they fit in the palm of the hand.
3. The stolen card information is later downloaded to a computer, and the wait staff is paid in cash for their part in the theft.
4. The details of the victim's credit card are encoded on a counterfeit card or re-encoded on a lost or stolen card and passed on to others, who may sell the card or use it for their own benefit.

How to Avoid Skimming Before it Occurs

Skimming is on the rise and restaurants are one of the most common locations for it to occur. Help protect your restaurant from liability by being proactive before identity theft occurs:

- Train your staff on what to look for in the workplace. Educate them on the various ways skimming can occur.
- Encourage your staff to report any signs of skimming at the restaurant. If they see anyone using a device that is not part of day-to-day activities or if anyone offers them money to record account information, they should let the restaurant owner and merchant processing center or company security know immediately.
- Screen restaurant applicants before you hire them. Skimming artists typically recruit others to pose as wait staff to collect credit card data or lure employees into their schemes by paying them for stolen data. The more you know about your new hires the better, especially those responsible for processing card transactions.



Server Katie Rosenberg demonstrates how the handheld payment device works.

cardholder data. In this situation, there is no data stored at The Brickery. Nobody can hack in and log into a server that's been unprotected in some way. Even if they could, there's no data here."

On the Spot has two main platforms: the Verifone Vx670, which allows at-the-table, curb or point-of-delivery payment for full-service and fine dining restaurants, and the QX720,

which is designed for use at drive-thru windows.

"You don't have to go in and try to do an integration with a POS, which can be very expensive and more complex," Hardison says. "We're finding that a lot of restaurants that may have security issues with their POS and would like to upgrade their system, but would have a huge bill, are going the route that [The Brickery] is."

ASI's Restaurant Manager POS system also prevents identify theft through skimming by allowing the complete payment transaction to occur in front of restaurant customers.

Restaurant Manager features Mobile Payment Processing, which protects restaurants from other forms of credit card fraud by encrypting credit card data according to standards set by the Cardholder Information Security Program (CISP).

"In this age of heightened security concerns, it is critical that POS applications are fully PCI-compliant," says Alex Malison, CEO of ASI. "CISP validation together with the Mobile Payment Processing offers even more safeguards against credit card fraud to both restaurants and diners alike."

Micros has upgraded its software to encrypt data in an effort to help protect restaurants from credit card fraud.

"They don't store full-track data at the restaurant site," says David Shaw of Postec, which distributes Micros. "It goes through a server and software called Transaction Vault, so it takes all the liability away."

Ultimately, handheld transaction equipment not only protects both the restaurant and its patrons from credit card fraud, it also helps turn-around times and keeps customer frustration levels at a minimum.

"You know, you do everything right — you market to the customer, you get them in here, you feed them great food, and then they're ready for the check and looking around for a server," The Brickery's Altman says. "The fact that the customer is now involved and seeing the process, and you're doing what you were doing in the back in front of him — the level of perceived customer service is so much better." ■