

GOOD RESTAURATEURS ARE ALWAYS LEARNING™

# Restaurant

APRIL 2005

## STARTUP & GROWTH™



### HE AIN'T **HEAVY** HE'S MY GUEST

Meeting the Demand  
for Healthy Fare to Boost  
the Fitness of Your  
New Restaurant  
page 22

Working the Floor  
to Build Guest and  
Employee Satisfaction  
page 32

Selecting Kitchen Staff Uniforms page 40

Restaurant Security Basics page 46

See Page 68 For a Complete List of Past Articles!

\$5.95 U.S. | \$7.95 CANADA



**TRAINING**  
KITCHEN MANAGEMENT  
Page 62

# Don't Let Skimmers Drive a Wedge Into Your Business

BY MELANIE G. SNYDER

Susan and Tom just finished dinner at their favorite restaurant. Susan hands her credit card to the waitress, who takes it to the credit card terminal and swipes it through — standard restaurant procedure. What happens next isn't. The waitress swipes Susan's card again, this time through a pager-sized device in her pocket called a "wedge," stealing data from the card's magnetic strip. The waitress daydreams about how she'll spend the hundreds of dollars she'll be paid for the credit card data she "skims" from dozens of customers during tonight's shift. After work, she'll transmit the data to counterfeiter and get her biggest "tip" of the evening. Within hours, criminals will use the skimmed data to charge thousands of dollars worth of purchases. Susan and other restaurant customers won't realize what's happened until their monthly credit card statements arrive.

Could this scenario happen in your restaurant? How could it affect your business? How would you know if your employees are involved? Most importantly, how can you prevent it?

"Business owners can be faced with both civil prosecution and, in cases of owner complicity, criminal prosecution," says Ross Federgreen, credit card security expert and executive vice president, CSRSI, a payment systems consulting company based in Florida. The Secret Service's Financial Crimes Division is working with credit card companies to find and investigate businesses where skimming has occurred. Merchant services banks regularly terminate accounts with businesses that have had problems with skimming.

Damage to the reputation of a business under investigation for skimming can be devastating. Just ask Yang Chen, owner of a small Chinese restaurant in the Midwest. Police seized Chen's business records and interrogated employees after receiving complaints about unauthorized credit card charges from nearly 60 local residents — all of whom had recently eaten at Chen's restaurant and paid by credit card. Local media reported the investigation, and Chen suffered an immediate, sharp decline in business, which took nearly a year to recover.

Federal authorities estimate that skimming now accounts for nearly 20 percent of all credit card fraud, costing U.S.

businesses \$1.2 billion annually. Technology has made skimming easier, as wedges can now be made small enough to hide in a pocket, under a shirt, inside a hem or on a belt.

If an employee takes longer than usual to process credit card transactions; disappears, even briefly, when processing credit cards; fumbles in pockets or "drops" things while handling credit cards; or asks patrons to provide a different credit card for payment, claiming the first one didn't go through, he or she may be skimming.

Jonathan Cherry, spokesman for the Secret Service, recommends that business owners monitor employee behavior for such warning signs and look for small devices that may be wedges. If you suspect an employee is skimming, report it to local police immediately. Don't confront the employee yourself. Users can press a "kill" button on the wedge to erase captured data instantly, removing all evidence of their crime.

## Preventing Skimming

Federgreen says that the best defense against skimming is a good offense, including these measures:

- ✓ Conduct thorough pre-employment background checks.
- ✓ Adopt a clear, written zero-tolerance policy on skimming and other credit card fraud, with consequences clearly articulated.
- ✓ Require all employees to read and sign the policy, acknowledging that they understand and agree to abide by it. Place the signed copy in the employee's personnel file.
- ✓ Ask your merchant services bank for information you can use to train employees.
- ✓ Educate supervisory staff and ask them to be on the alert for suspicious activity.
- ✓ Allow customers to pay at the register or invest in portable credit card terminals that can be used table-side.
- ✓ Advise your bank and your customers of steps you've taken to minimize the risk of skimming in your business.

With awareness and sound business practices, you can make sure credit card skimming doesn't drive a wedge into your business.

RS&G