

## Security Safeguards

*November/December 2007*

*By Charles Y. Hoff, Esq.*

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 chargeback's.

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 vendor (POS) 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.