

Law Offices of Charles Y. Hoff, PC



110 High Point Walk
Atlanta, GA 30342
Phone (404) 245-6751

PCI Compliance - Avoid Visa/MC penalties & fines

DEFUSING THE ID THEFT TIME BOMB

By Charles Hoff

As you have been concerned about the prospect of employees fraudulently skimming customer credit card information at the table to engage in ID theft, you have ordered “pay at the table” devices. You can also pat yourself on the back for ensuring that you are in compliance with federal law by seeing that your customers’ receipts no longer show their credit card numbers or card expiration dates. Now you can relax and quit worrying about ID theft, right? WRONG. The greatest exposure still remains, and it is putting restaurants out of business overnight throughout the country.

All restaurants are at risk of credit card security data and are being targeted more than other retail establishments. You normally learn that you have a problem when you are notified by your card processing company that your credit card company (Visa, MasterCard, AMEX, Discover, etc) fraud departments through their monitoring systems suspect that the security of your internal computer network system has been compromised in light of irregular patterns of consumer credit card usage picked up from your store location. In other words, they feel that your system may have been hacked into by intruders intent on stealing the credit card information from your database or point of sale network. You don't have much time to think about it as your card processing firm notifies you that 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. They will also remind you that you have signed contracts that permit the card processing company on behalf of the merchant bank to withhold six figures of credit card payments while the card company makes its determination of how much in the way of fines and penalties to impose upon you. We have seen card processing companies advise their restaurant clients that egregious security infractions can bring a fine of as high as \$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: 1) the penalties assessed by the card companies; 2) will there be any credit card chargebacks; 3) cash flow problems

encountered as a result of the card processing company's withholdings; 4) will the card companies cut off the use of their cards, and 4) the potential adverse publicity that could result and undermine the public trust in your restaurant and erode business.

How could this nightmare be avoided? You need to select a reputable POS vendor and make sure that their software has been updated to the latest PCI DSS compliant versions. However, this is not enough as you need to understand the contractual obligations imposed upon your restaurant by the Payment Card Industry Data Security Standards (PCI DSS) as shown below:

Build and Maintain a Secure Network

- 1) Install and maintain a firewall configuration to protect cardholder data
- 2) Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

- 3) Protect stored data – at all times
- 4) Encrypt transmission of cardholder data and sensitive information sent across public networks.

Maintain a Vulnerability Management Program:

- 5) Use and regularly update anti-virus software
- 6) Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- 7) Restrict access to cardholder data by a "need-to-know" basis
- 8) Assign a unique ID to each person with computer access
- 9) Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- 10) Track and monitor all access to network resources and cardholder data using a user unique ID
- 11) Regularly test security systems and processes

Maintain an Information Security Policy

- 12) Implement and maintain an information security policy

What do you do when you are a victim of a breach involving payment card data:

- A) Do not alter the suspected system
 - 1) Attempt to isolate the system (if practical, unplug the system)
 - 2) Change systems; user passwords, yet not "root" ones
 - 3) Change network passwords
 - 4) Preserve all logs and reports

- B) Contact your merchant acquirer and other card brands if they have not contacted you first
- C) Contact law enforcement
- D) Record in written form all actions taken and when
- E) Anticipate a forensic data investigation
- F) Consult with knowledgeable legal counsel

Most importantly, become educated to this issue so that you may be proactive. Don't let yourself, your patrons, or your restaurant become needless victims.