



# PCI Compliance—fact or fiction?

by Tracy Blalock

**PCI COMPLIANCE** is no longer a suggestion—it's a necessary "evil" if you accept credit cards. According to the Federal Trade Commission, as of 2008, nearly one-fourth of all identify theft cases involved a credit card. Reports of data theft are rampant, including a recent case involving 130 million credit and debit card numbers. Now, more than ever, you need to reassure your customers you're taking every precaution when it comes to securing their personal information.

## What is PCI Compliance?

PCI Compliance is the process of verifying that your business processes adhere to the Payment Card Industry Data Security Standard (PCI DSS). These 12 requirements, managed by the Payment Card Industry Security Standards Council (PCI SSC) are designed to ensure all companies that accept, transmit, process or store credit card information maintain a secure environment that protects customer account data. Specifically, it applies to debit, credit and pre-paid cards branded with a Visa, MasterCard, American Express, Discover or JCB logo. After several years of recommending compliance, the card brands are now enforcing compliance—to the tune of up to \$150 or more per year in annual compliance fees.

## Debunking the Compliance 'Myths'

While the intent of PCI compliance is to keep businesses and their customers' data safer, getting there has challenged even the bravest of merchants. The first step is getting the facts.

"The Internet, including tanning forums such as TanToday.com, are an invaluable resource," says Pawel Blaz, sales and business development manager for Gulf Management Systems, a company specializing in credit cards and other electronic payment solutions. "The danger is that much of what's out there regarding PCI compliance is outdated or incomplete, putting merchants and their customers at significant risk."

Here are the most common PCI compliance myths:

▶ **PCI compliance doesn't apply to me.** Do you accept credit cards? Then PCI compliance applies to you. The five major payment brands have collectively adopted PCI DSS as the requirement for any organization that processes, stores or transmits cardholder data. This includes home-based businesses—and these may be the most vulnerable because they are typically not well

protected: owners often have broadband connections that are always "on," and many use chat functions. In hacker-speak, that spells prime target.

▶ **I only process a small number of transactions, so it's not necessary.** All merchants that accept cards, regardless of company size or number of transactions, need to be PCI compliant.

▶ **I only store the last four digits of the account number, so I'm compliant.** There are 12 requirements that define a basic level of security. Doing some, or none, simply won't fly. One-hundred percent is required for compliance.

▶ **I completed the questionnaire and scan (if applicable), so I'm done.** Beware of one-time, Band-Aid solutions, such as a free scan. Scans are required quarterly, and to become and stay compliant, there are fees involved—typically between \$100 and \$150 per year. Make sure you know your total costs. Plus, many services don't include the Self-Assessment Questionnaire (SAQ), which is a requirement for all merchants.

▶ **Breaches only happen to large retailers.** While it may seem that way based on media coverage, the reality is that small- to medium-size merchants are more frequent targets. In general, these merchants are also more vulnerable since most have less sophisticated technology and security measures. And remember, you not only face external threats from hackers, but internal ones in regard to employees that obtain files they shouldn't.

## So, What's a Merchant to Do?

Doing nothing is clearly not an option given the serious, and costly, consequences. The card brands categorize merchants into four levels based on how card data is handled and Internet connectivity. The actions you must take depend on your level, but there are three fundamental steps involved in compliance.

First, all merchants—regardless of size or level—need to complete an SAQ, which will assess the environment. There are four different versions, so be sure to complete the correct one. (And, please note that just saying "yes" to every question without factually assessing your business puts your entire salon at risk should a breach occur.) Next, you may need a network scan from an Approved Scanning Vendor (ASV) to identify vulnerabilities—and you must fix anything that shows up. Finally, the results of both must be reported to the card brands (SAQs are required annually; scans are required quarterly).

### What if I Don't Comply?

For starters, look out for a \$19.95 monthly fine for every month you don't comply. If fined, chances are great the bank will either terminate your relationship or increase transaction fees. Card replacement fees range from \$50 to \$90 per card. You can also expect costly remediation if a breach occurs while you are not compliant. Brand and reputation damage are difficult to measure, but can devastate a small business. Suffice it to say, the penalties can be catastrophic.

### Can I Do it Myself?

Achieving compliance isn't some kind of super-human feat; unfortunately, the volumes of information (and misinformation) you must sort through can make it feel like one. Can you do it yourself? Sure. But a better question is how much time you're willing (and can afford) to spend sorting through 10-pound documents and making phone calls to multiple vendors.

Google "PCI compliance" and you'll get almost 2 million search results. And, unfortunately, you don't have a lot of time to sift through all of that data—technically, you've already missed the first deadline for compliance.

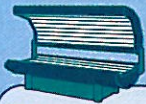
Plus, PCI compliance is an on-going process that requires managing your SAQ and scan deadlines, and keeping up with changing regulations. And, any location with a unique merchant

ID must comply as a separate entity—so, if you own multiple locations, the time can really add up. According to reports from Kark and Forrester Research, compliance is constantly changing and "if you are compliant today, it doesn't necessarily mean you will be compliant tomorrow."

The moral of the story is that PCI compliance is real, and will evolve to keep up with the evil lurking in the hearts of relentless hackers. That's as good an argument as any for finding a trusted partner that is willing to scan your network in a single keystroke to keep you and your customers safe today—and tomorrow. ☺

Tracy Blalock has been the marketing manager for Gulf Management Systems (GMS) for the past two years, and has spent more than 20 years helping high-tech companies achieve and maintain software compliance. GMS, named on Looking Fit's "Industry's Coolest" list for its creative marketing programs, has been helping salon owners build strong customer relationships for more than 16 years with easy and affordable solutions that include both ACH and credit card EFT, POS, gift cards, remote deposit and direct deposit. Keeping current with changing industry regulations is business as usual for GMS, and is accomplished through NACHA and ECC memberships, participation in all major industry tradeshows and by having three accredited ACH professionals on staff. For more information, call 800.947.3156 or visit [www.gulfmanagementsystems.com](http://www.gulfmanagementsystems.com).

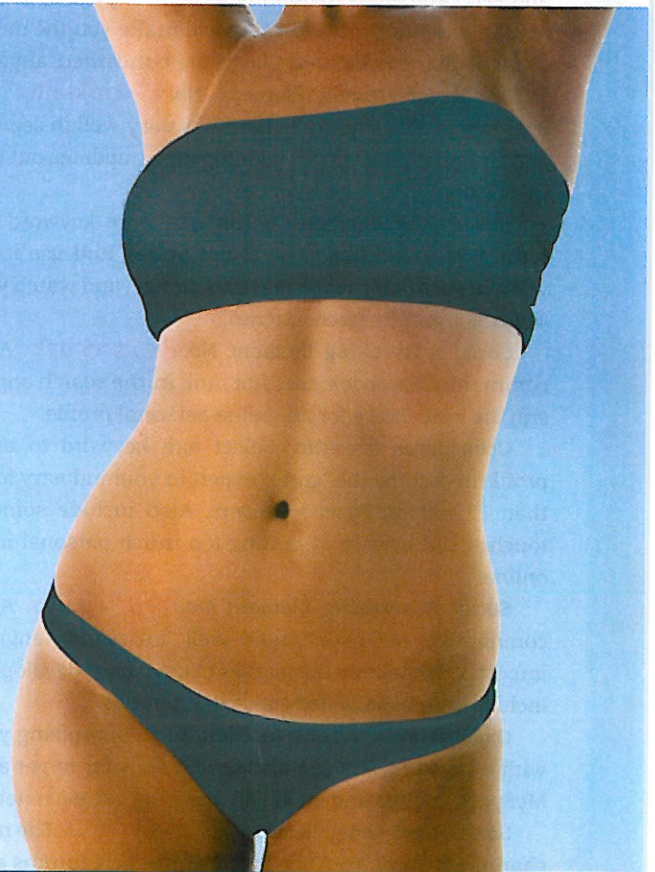
# Insurance Designed For Tanning Salons



## Tan Pro

**THOMCO's Tan Pro**, brings you reliable and affordable Insurance coverage with industry exclusive enhancements just for your Tanning Salon!

- "A" Rated by A.M. Best
- Discounts on Training Certification
- Workers' Compensation Now Available Industry Exclusive!
- Fast & Easy Quotes Available Over the Phone
- Equipment Breakdown Covered up to Policy Limits Industry Exclusive!
- General Liability Limits up to \$5,000,000 per Occurrence
- Professional Liability Limits Available Up To \$3,000,000, No Deductible
- Discounts on Premiums for Multiple Locations & Loss Free Accounts
- Total Access to Our Valuable Risk Management Resource Center
- Excellent Customer Service Representatives
- Per Location Aggregate Automatically Included
- Ask About Automatic Property Enhancement and Package Discount When You Purchase Your Policy



Call or Visit Our Website for More Info & Get Your Quote Today!

[www.TanProins.com](http://www.TanProins.com) | 888.969.8030

Visit Our Website to Sign-up for Your Complimentary Insurance Guide.

