

# PCI—and “Why”

First you had OSHA, then HIPAA; more recently, Red-Flag laws, and now PCI?

**What is it?** PCI stands for **Payment Card Industry Data Security Standards**. For the most part, PCI focuses on protecting credit card numbers, and compliance with these regulations are required of every merchant that accepts credit cards as a form of payment. (You may want to go to [pcisecuritystandards.org](http://pcisecuritystandards.org) to learn more.) The main impetus of the new regulations is deterring identity theft. Keep in mind that dental staff are often privy to patient birthdates, social-security and credit card numbers. In the wrong hands, this information makes patients easy targets.

If you have not been contacted by your credit card processor yet, you probably will be before January 2010. Most processors are charging an annual fee of \$25 to \$179. In order to meet PCI-security requirements, you'll most likely be asked to log on to an authorized PCI website, and answer questions. To determine what level of compliance will be required of you, you'll be asked some questions regarding whether you use a terminal (lowest level of compliance required) or an Internet-based system (which requires a higher level of compliance). Most dental offices that use a credit card terminal will only need to complete the questionnaire, write a short policy about how it protects its patients' credit card information, and assign a designated PCI-security contact person. Having more effective security measures in place in your office will mean fewer questions will be asked of you. If you use a system that connects to the Internet for processing payments, you'll need to provide the same documentation as above, but your questionnaire will be much longer. You should also begin receiving quarterly scans to verify that your patients' credit card data cannot be compromised via the Internet.

## **Your written policy should, at minimum, reflect that:**

- **All patient records containing credit-card numbers are properly secured.** They should be unavailable to others, such as other patients and your cleaning service.
- **Credit card receipts and related records are properly shredded after your retention period expires.** You may want to keep signed receipts at least six months, in case you receive a chargeback and need to provide a signed copy.
- **Credit card processing batches are closed daily.** Most processors have updated their software to truncate (show only the first and last four digits of a credit card number) both the merchant and customer copies of a receipt. This may have required a software download. Truncating both copies of a receipt is mandatory in California and Tennessee only. At this time, Texas law only requires that the customer copy be truncated.

Several credit card processing companies are faxing and/or calling dental practices and telling them that their equipment is not PCI-compliant, and that they need to call them. These companies will not know what kind of equipment the offices have. They are simply using a marketing ploy to try to become their merchant processor. Nearly all credit card terminals are PCI-compliant, or are able to take a software download to become so. However, some pin pads will not be, because of their ability to store pin numbers (four-digit codes for debit cards). Most dental practices don't have a pin pad. If yours does, please call your merchant processor to find out if it's compliant.

**If you have additional questions regarding PCI, you may call your present processor, or you can call the TDA Perks Program-endorsed credit card processing company, Best Card, at (877) 739-3952.**