

Misleading Information in the Credit Card Processing Industry

By Jennifer Nieto, Best Card

Many practices are receiving misleading information regarding the following matters that we wanted to bring to your attention:

1. You may have received a fax from First National Merchant Services telling you that your credit card processing terminal is no longer “compliant.” It then offers to sell you new equipment for \$379. (There is no phone number for contacting the company.) This is a marketing ploy to try to get you to purchase a new terminal that has an internal pin pad. Very few dental offices use a pin pad, because patients tend to not want to enter their PIN number. However, if your office does have a pin pad, call your merchant to verify that it is compliant with current standards.
2. You may have received a notice from your current credit card processor indicating that you need to document that you are compliant with Payment Card Industry (PCI) Data Security Standards for your credit card processing merchant account. Many processors have started charging a \$19.95 or higher monthly fee to their clients who have not faxed it verification of a written document relating to client compliance. Many other processors also have a PCI monthly fee. PCI compliance is complex, but for the most part, it focuses on protecting patients’ credit card numbers (the lowest level of compliance is required for merchants that process less than \$1 million in credit cards annually, and use a terminal (not an online system.) Nearly all dental offices process less than this amount.) Security documentation is especially necessary for those offices who use an online processing system for their credit cards instead of a terminal. If your online system stores the credit card number (whether you host the number or a third party hosts the number,) security measures need to be taken to ensure that those credit card numbers are protected from a security breach where an outsider can “obtain your patients’ credit card numbers and use them for identity theft purposes.” Please go to <https://www.pcisecuritystandards.org> for more information about PCI compliance requirements. For the average office that uses a credit card terminal and closes its batch daily, one can meet these requirements by completing the self-assessment questionnaire available at the above mentioned website, and preparing a simple written document that states that: (a) all patient records that show the patients credit card number are properly secured and not available to others, such as patients in the office, cleaning services, etc.; (b) credit card receipts and related records are properly shredded after the three-year bookkeeping retention time (or whatever the office’s policy is); and (c) credit card processing batches are closed daily (this process deletes any merchant numbers stored in the terminal.)
3. Please also be aware of the following:
 - Two states now require both merchant and customer copies of printed credit card receipts be truncated (i.e., all but the last four digits of the credit card number are removed from the receipt.) If, for security purposes, you would like to truncate both receipts now, please call your merchant processor with this request, and your processor will have you do a partial download.
 - If you accept American Express, recent programming changes necessitate you re-downloading your terminal to become compliant.

Best Card Company is a credit card processing company and a TDA Perks Program partner. For more information regarding the Best Card program, please contact Rose McKee, Jennifer Nieto or any of the Best Card team at (877) 739-3952. For information on other TDA Perks Programs, visit tdaperks.com, or call the TDA Perks Program office at (512) 443-3675.