

# Get to Know the Fundamentals of EMV<sup>®</sup>

*Carl Mazzola, President TransFirst Health and Public Services*

There's been a lot of buzz surrounding EMV credit cards and how they're going to revolutionize our personal security in this country. But what does that really mean and how does it affect your practice?

Let's start with the basics, like what is EMV? It stands for Europay, MasterCard<sup>®</sup> and Visa<sup>®</sup>, and it's a security framework that defines the payment interaction at the physical, electrical, data and application levels between chip cards and payment devices. It's a card-present technology that facilitates a direct connection from a payment card to your POS system. There are two ways this connection can occur:

- Near-field communication (NFC) — tapping or waving the card within a few inches of the terminal; this is also known as “contactless” or “tap and go.”
- Chip-and-Personal Identification Number (PIN) — inserting the end of the card where the chip is located directly into a slot in the terminal, which “reads” the information from the chip.

In many cases, either of these options requires the cardholder to enter a PIN or provide a signature. The microprocessor chip creates a unique transaction code that cannot be used again each time an EMV card is used for payment. If a hacker tried to use stolen chip information from a specific point of sale, the stolen transaction number created for the fraudulent charge couldn't be used a second time, and the transaction would be declined.

This makes it much more challenging for criminals to produce and use counterfeit cards for point-of-sale fraud, diminishing the value of stolen customer information.

## **How does this affect your practice?**

Because of these advances, your liability is shifting. The expectation is that you'll upgrade your equipment to be EMV compliant by October 1, 2015. If you're given the chance to upgrade to EMV-capable equipment, but don't do so within the above timeframe, you will be held financially liable for security breaches after October 1. If your payment processor is *not* offering EMV-compliant equipment upgrades, the financial responsibility of a breach falls to them.

Using EMV-compatible equipment may also help lower your processing expenses by potentially reducing compliance fees.

## **How do you know if your equipment is compliant?**

If your terminal is more than a year old, it probably isn't EMV-ready. It's a good idea to check with your processor now about what your upgrade options are, so your practice is prepared for the October deadline.

While effective at reducing fraud, no technology will completely eliminate the risk of a security breach, and there are additional steps you can take to protect your practice and your patients.

- Be mindful of employees who handle patient payment data — consider running background checks on all new employees and limit the number of people with access to patient information.
- Take precautions with printed documents — shred the ones you no longer use and keep the ones with sensitive information secure, restricting access to them.

- Use smart security practices with computers — use password protection when possible, use and keep current anti-virus software and network firewalls.
- Implement ongoing risk assessment analysis — conduct regular security audits, hold periodic training sessions to educate staff on handling sensitive data, and establish security protocols to help prevent data security risks.

### **Become compliant today**

The EMV transition should be a smooth one for your practice. It requires a simple equipment upgrade and in return offers additional security that benefits both your practice and your patients, so get started today.

For additional information on the EMV switch, or about how TransFirst's EMV solutions can help improve your payment processing security and efficiency, please call 800.613.0148 today, or visit [www.TransFirstAssociation.com/MSDC](http://www.TransFirstAssociation.com/MSDC).

EMV is a registered trademark in the U.S. and other countries, and is an unregistered trademark in other countries, owned by EMVCo. Trademarks are the property of their respective owners and are not necessarily affiliated with TransFirst. TransFirst, LLC is a registered ISO/MSP of: Wells Fargo Bank, N.A., Walnut Creek, CA, and Synovus Bank, Columbus, GA, for Visa and MasterCard transactions only.

**TF3968c**