

New Credit Card Processing Guidelines to Take Effect in October

There has been a lot of press this year about new technologies in the credit card processing industry. And since most dentists accept credit card payments, they should understand what's taking place. Much of the press has to do with the new "EMV" chip on credit cards.

What is "EMV"?

EMV stands for Europay, Mastercard and Visa, and is the global standard for credit card security that uses encrypted chips on credit cards, rather than magnetic stripes, to process transactions. EMV-chip cards are designed to decrease credit card counterfeiting by making them more difficult to copy. Unlike magnetic-stripe cards, which store unchanging data in their stripes, EMV-chip cards generate a new code for every transaction. Cardholders also have to verify their EMV card purchases with either a signature or by entering a PIN. That being said, the new EMV cards will still have the magnetic stripes on them.

Is EMV Required by the Government?

No. The federal government, however, has pushed the industry in this direction and the credit card industry has responded with their own requirements. Banks have begun issuing cards with the new EMV chip and processing companies are now prodding merchants (including dentists) to buy the new terminals that read these chips.

So if It's Not Mandatory, Why Should I Buy a New Terminal?

Although the major card processing companies (VISA, Mastercard, AMEX, etc.) are not requiring merchants to upgrade their terminals to comply with EMV, they will be instituting a **Fraud Liability Shift**. This means any fraud occurring from a card-present transaction will shift to whichever party is the least EMV-compliant.

Currently, if an in-office transaction is conducted using a counterfeit, stolen or otherwise compromised card, consumer losses from that transaction will likely fall back on the payment processor or issuing bank, depending on the card's terms and conditions.

On October 1, that liability will shift to whichever party is the least EMV-compliant. So, if you, as a merchant, do not have an EMV-compliant terminal, you are liable if the transacted amount is unrecoverable due to fraud. This means that if you are presented with a fraudulent (counterfeit or stolen) credit card, and IF that card has an EMV chip in it, but you process it via the magnetic stripe, you will lose that chargeback.

Is There a Deadline?

October 1, 2015 is when this liability shift will occur for all merchants (except gas stations) and to-date there is no indication that this will be delayed.

If I Don't Upgrade, Can I Still Process Credit Cards With My Old Terminal?

Yes. You can choose not to replace your non-EMV terminal and continue to process even the new EMV cards by swiping them. If the card is fraudulent, however, you will be responsible for covering the transacted amount. Reported cases of fraudulent credit card activity in dental offices are low, but it can and does happen.

Will the New EMV Terminal Completely Protect me Against Fraudulent Credit Cards?

Hopefully. You still need to follow proper protocols for securely handling credit card information and complete your processor's PCI compliance procedures. Beyond that, the EMV terminal insulates you from most chargebacks due to the card being fraudulent.

What if a Card Doesn't Have an EMV Chip on It? Should I Refuse It?

No. The new EMV terminals will still be swipe-capable so that you can process non-EMV cards. When you swipe a transaction for a non-EMV card, you are not usually responsible if that card is fraudulent – provided your staff has performed the usual due diligence. It is likely that some credit cards and most debit cards will still not have the EMV chip by October 1.

Exceptions?

EMV only applies to card-present, face-to-face transactions. Card-not-present (CNP) transactions won't be affected by the liability shift. Any fraud in these transactions will follow normal chargeback procedures and will typically be the responsibility of the issuing bank or processor.

What About Apple Pay?

"Near Field Communication" (NFC) is the official term for contact-less payment technologies that don't require you to swipe or insert a card into the terminal. For example, people can wave their smartphone next to a terminal and pay with their Apple Pay or Google Wallet accounts. Some credit cards also have this feature and are typically marked with the picture of a sound wave.

NFC is not required, but when you upgrade your terminal for EMV, you want to be sure that it also works with NFC.

Staff Reminders

To minimize liability to the practice there are some important things staff need to be mindful of.

First, with any face-to-face transaction, it is important that you match the name on the card with the person presenting it. Also be sure the signature matches the name on the card.

It is very important that when you are keying in a credit card that you require the 3-digit CVV code and verify that the address and zip code match the cardholder's account.

You should also note that EMV-compliant charges require customers to insert the card in the reader and leave it there until the transaction is complete. Employees should get in the habit of reminding customers to take their cards out of the EMV reader at the end of the transaction.

Also, make sure that your equipment is PIN-enabled in case the issuer of the EMV card requires a 4-digit code – even on credit.

Questions?

The experts on this issue are the credit card processing companies. Lean on your processor for any questions you have or support you need.

- *Michael J. Herrmann, Executive Director, NYSSOMS*