The High Cost of Missing the EMV Chip Card Switch

Be prepared for this radical change in credit card technology.

BY JAMES D. KRICKETT

There is a potential storm cloud on the horizon for many podiatry practices that either accept credit or debit card payments or podiatrists who use those cards for practice-related purchases. In the wake of numerous large-scale data breaches and increasing rates of counterfeit card fraud, U.S. card issuers are migrating to new global bank cards based on EMV (Europay, MasterCard, and Visa) chip card technology, a world-wide standard for so-called integrated circuit cards, and the hardware necessary to accept these cards.

Ahead for anyone accepting credit card payments lies a so-called "liability shift," where banks and card issuers plan to shift liability for fraudulent card transactions to those who are not ready for a new, more secure card. For credit card users, it will be a new way of transacting card purchases.

Today, if a credit card transaction is conducted using a counterfeit, stolen, or otherwise compromised card, losses from that transaction usually fall back on the payment processor or issuing bank. After October 1, 2015, any practice or business that doesn't have an EMV processing device will find that the banks will no longer be liable.

Although it is estimated that 40 percent of debit cards and over 70 percent of credit cards that will be issued before the end of the year will employ the EMV technology, many podiatry practices, especially those with a relatively low volume of card transactions, may find the cost of upgrading to accept EMV cards could outstrip the potential future costs of fraud.

The New EMV System

EMV is a global standard for credit and debit cards equipped with a small integrated circuit (or "chip") that, along with the appropriate technology, is used to authenticate transactions. The EMV technology, often referred to as Chip and PIN, is widely used elsewhere in the world, and now experts are hoping it will help

Continued on page 60

EMV is a global standard for credit and debit cards equipped with a small integrated circuit (or "chip") that, along with the appropriate technology, is used to authenticate transactions.

EMV Chip (from page 59)

significantly reduce fraud in the U.S. Fraud has doubled in the past seven years as criminals have shied away from countries that already have transitioned to EMV cards,

For consumers, the switch means activating the new EMV cards and learning new payment processes. For podiatry practices or businesses, those so-called "merchants" and the financial institutions that process card transactions, it means adding new point-of-sale (POS) terminals, in-store technology, and internal processing systems.

EMV technology will not prevent data breaches from occurring, but it will make it much harder for criminals to successfully profit from what they steal. The magnetic stripes on traditional credit and debit cards contain unchanging data making traditional cards prime targets for counterfeiting. Whoever accesses the data on traditional cards has all of the sensitive card and cardholder information necessary to make a purchase. Setting apart the new generation of cards is a small, metallic square on new cards.

Unlike the traditional magnetic-stripe cards, every time an EMV card is used for payment, the card's chip creates a unique transaction code that cannot be used again. As with magnetic-stripe cards, EMV cards are processed for payment in two steps: card reading and transaction verification. With EMV cards, however, it is no longer necessary to master a quick, fluid card swipe in the right direction. Chip cards are read in a different way.

Instead of going to a register and swiping an EMV card, patients perform "card dipping", inserting the card into a terminal slot. When an EMV card is dipped, data flows between the card chip and the issuing financial institution to verify the card's legitimacy and create the unique transaction data. This process isn't as quick as a magnetic-stripe swipe.

Chip and Pin

The EMV, "chip-and-PIN" cards operate just like the checking-account debit cards that have been in use for years. Entering a PIN connects the payment terminal to the payment processor for real-time transaction verification and approval. Unfortunately, even at this late date, many payment processors are not equipped with the technology needed to handle EMV chip-and-PIN credit transactions, making it unlikely that new PINs will have to be memorized anytime soon.

There aren't going to be many issuers requiring a PIN. In fact, a vast majority will be issuing chip-and-signature cards, which aren't all that different from how credit cards now work. As with a magnetic-stripe credit card, a signature on the point-of-sale terminal with chip-and-signature transactions is all that is required.

The transition to EMV is underway and chip-and-PIN cards are already being transitioned in, with the process probably taking two to three years to fully convert to chip-and-pin.

The transition to EMV is underway and chip-and-PIN cards are already being transitioned in, with the process probably taking two to three years to fully convert to chip-and-pin. Despite what is expected to be a slow transition, those who get chip-and-PIN cards will be able to use them right away. If a terminal doesn't have the ability to accept a PIN, it will then step down to accepting a signature. In other words, there will always be a secondary option.

Thus, a podiatry practice can continue accepting cards with the magnetic stripe and ignore the EMV technology. No business will be lost since most cards will still have a magnetic stripe as backup. The only difference, an extremely important difference, is that starting in October 2015 the podiatry practice may find itself liable for any counterfeit or fraudulent card transactions, thanks to the so-called "liability shift."

Near But So Far

EMV cards can also support contactless card reading, often referred to as "near field communication" (NFC). Instead of dipping or swiping, NFC-equipped cards are tapped against a terminal scanner that picks up the card data from the embedded computer chip. Unfortunately, dual-interface cards and the equipment needed to scan them are expensive. So, currently, the emphasis is on successfully integrating EMV cards into the shopping process. Dual interface will arrive later.

Where no card is present, such as with online transactions, programs such as MasterCard's Chip Authentication Program (CAP) and Visa's Dynamic Passcode Authentication (DPA), allow EMV cards to be used for authentication. For an online transaction, the user inserts the EMV credit or debit card into a handheld reader. Once the user enters the PIN the reader displays a one-time password which can be used to validate the user's identity. The user enters the password in the appropriate field on the podiatry practice's remote checkout page (or online banking site) and the password is passed back to the issuer for authentication.

An EMV-based payments infrastrucure for mobile contactless payments has already been introduced in Europe. However, while continued growth is predicted for NFC-enabled mobile devices for contactless payments and other mobile applications in the U.S., as with duel-interface equipment, it will be a while.

PCI Compliant

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that everyone handling branded credit cards from the major credit card companies such as Visa, MasterCard, American Express, Discover, etc., and all "merchants,"

Continued on page 62

EMV Chip (from page 60)

whether large or small, must comply with. The credit card companies have collectively adopted PCI DSS as a requirement for everyone processing, storing, or transmitting cardholder data.

Rather than focusing on a specific category of fraud, PCI DSS was designed to protect the cardholder and sensitive authentication data anywhere this data is present within the payment process, thus limiting the potential for hacking and fraud. When used together, EMV chip technology and PCI DSS are expected to substantially reduce fraud and greatly enhance payment security.

The Issue of Liability

A key consideration for any podiatry practice adopting EMV cards is the so-called "liability shift." Liability shift means that issuers (banks, credit unions, and any other financial institution issuing credit or debit cards) and podiatry practices, the so-called "merchants," continuing to use non-EMV compliant devices and accept transactions made with EMV-compliant cards, will assume liability for any and all fraudulent transactions.

According to at least one expert, if a hacker stole the chip information from one specific point of sale, typical card duplication would never work because the stolen transaction number created in that instance wouldn't be usable again and the card would just get denied.

After the liability shift, a podiatry practice continuing to use the "swipe and signature" methodology will find themselves liable for fraudulent card payments. If the practice/merchant has the new EMV Chip and PIN technology but the bank hasn't issued the customer a Chip and PIN card, the bank is liable. If a merchant uses Chip and PIN technology on a patient/client/customer's smartcard and fraud still takes place, the credit card company bears the liability, as is the case today.

In other words, after the October 1, 2015 deadline created by major U.S. credit card companies, the liability for card-present fraud will shift to whichever party is the least EMV-compliant in the fraudulent transaction. Naturally, the capabilities of a podiatry practice's point-of-sale (POS) system will play a pivotal role in the success of the EMV card. Issuers can distribute EMV cards, but EMV's fraud reduction benefits won't be realized if the practice/merchant can't accept the cards.

The upcoming liability shift means every podiatrist and his or her practice will have to review their point-of-sale systems, including both hardware and software. The transition could prove easier for small practices, which may be able to move to EMV by simply adding a new external pin pad. But larger practices and businesses will, in all likelihood, have to invest heavily as they look to upgrade thousands of terminals and systems.

The Issue of Fraud

The many countries that have already implemented EMV chip payments have reported a decrease in card fraud. As an example of the impact of EMV, the UK Cards Association has reported a dramatic reduction in fraud since the introduction of EMV cards.

According to the UK Cards group, a trade body for the card payment industry in the UK, "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at U.K. retailers have fallen by 67 percent since 2004; lost and stolen card fraud fell by 58 percent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 percent since 2004."

The national roll-out of EMV chip cards in Canada in 2008 also had a significant impact on fraud. Losses from debit card skimming in Canada fell from CAD$142 million in 2009 to CAD$16.2 million in 2014, according to the Interac Association, a Canadian association specializing in debit card services.

The experiences of the U.K. and other countries that have adopted chip technology have shown a reduction of domestic card-present fraud. Unfortunately, their experiences have also shown a migration to other types of fraud, namely card-not-present (CNP) fraud and cross-border counterfeit fraud (particularly ATM fraud). Admittedly, fraud migration does offset some of the savings from the decrease in domestic card-present fraud, reinforcing the need for a layered approach to security, even with EMV deployment.

The many countries that have already implemented EMV chip payments have reported a decrease in card fraud.

The Bottom-Line

U.S. banks are switching to the new EMV technology, which stands for "Europay, MasterCard, and Visa," making credit cards equipped with a super-small computer chip extremely hard to counterfeit. In all likelihood, most of the cards issued recently have this new technology.

Why the changeover? Surprisingly, almost half of the world's credit card fraud now occurs in the United States—even though only a quarter of all credit card transactions happen here. The banks and financial institutions hope to rein this in by moving away from magnetic-stripe cards, which are much easier to counterfeit to cards using the new EMV technology.

How will this affect a podiatry practice or business? For starters, most will need a new processing device to read the information in the chip cards. While this can get expensive, keep in mind that after October 1, 2015, practices and businesses without an EMV processing device could be on the hook for fraudulent chip card transactions.

There are an estimated 1.24 billion payment cards and 15.4 million point-of-sale (POS) terminals current-

Continued on page 64

EMV Chip (from page 62)

ly in use, most of them in other countries. Making global financial transactions work across many cards and devices are smart chips embedded within new EMV-compliant credit and debit cards. These chips make interfacing with the various POS terminals possible.

Currently, Europe, Canada, Latin America, and the Asia/Pacific region are all well on their way, migrating from the legacy magstripe standard to EMV chip card technology. The world's single largest user of payment cards, the U.S., has just begun the process. However, the potential impact of being the last bastion of magstripe technology is forcing U.S. financial entities to take the idea seriously.

A podiatry practice that is not in compliance by October 2015 will assume liability for any fraudulent purchases—a shift that is poised to drive many to adopt the new standards and avoid the risk.

Although the upcoming deadline should be enough encouragement for all parties involved in the payment processing process to become EMV-compliant, it is increasingly obvious that not everyone will comply by that date. While EMV compliance is required for credit card acquirers and processors, it is not mandated for merchants and processors. Of course, a podiatry practice that is not in compliance by October 2015 will assume liability for any fraudulent purchases—a shift that is poised to drive many to adopt the new standards and avoid the risk.

As the new EMV card strategy was developing, many experts were saying that the only merchants who should think about getting EMV-compatible credit card terminals were those who needed a new terminal. The consensus seemed to be, as with the case for computers, the best time to get a new credit card machine may be tomorrow. The technology will only improve with time, making it less important unless the practice or business is already encountering a large number of chip cards.

But, tomorrow may be today. Expert opinions withstanding, all podiatrists should protect themselves and their podiatry practices from fraud liability. The relatively small price of a new terminal may be worth the peace of mind it brings. Naturally, there is always the chance that no one will ever attempt to use a counterfeit chip card in your practice, but can you afford to gamble? **PM**

James D. Krickett is a well-known tax and financial adviser whose columns are syndicated to more than 65 publications each week. His features routinely appear in the pages of leading trade magazines and professional journals.