READY FOR EMV?

> Credit card fraud in the United States is rampant. In 2014, credit fraud costs totaled $32 billion, 38 percent more than 2013, according to the 2014 LexisNexis True Cost of Fraud Study. That's why US banks have been issuing new credit cards featuring an embedded computer chip designed to combat credit fraud called EMV — it stands for Europay, MasterCard and Visa.

As the name implies, EMV has been the standard in Europe (and most of the world) for about 10 years and has proven effective in stemming fraud. This month, we explore EMV, discuss equipment considerations in order to accept EMV and other types of secure payments and provide insight on how this impacts your business.

Chipping Away at Fraud

So why is EMV a better, more secure solution than traditional credit cards with the magnetic stripe? Magnetic-stripe cards contain unchanging data. So, all it takes is an inexpensive fake swiper to copy that data, make replicas of the card and go on a shopping spree.

EMV features a functionality called "dynamic authentication" and it protects against a very specific type of fraud: card-present transactions with a counterfeit card. It does not protect against stolen numbers being used on your website or given to you over the phone or any other kind of credit card fraud.

Getting Equipped

Accepting EMV requires new equipment that lets customers insert the card into a machine that reads the chip. Customers then type in a PIN (or provide a signature, which is less secure) to complete the sale. This is known as a **"contact" type EMV terminal reader.**

Another payment alternative leveraging the EMV process is **"contactless" payment** using a mobile phone, such as Apple Pay and Google Pay. Both the smartphone and terminal are equipped with a Near Field Communications (NFC) transmitter and receiver. As the name implies, customers hold the smartphone near the reader to initiate the transaction. To complete the transaction, you can input a signature or, if your smartphone features a fingerprint reader or PIN input, you verify the payment using these secure methods.

Apple is determined to make mobile payment a de facto standard, so they are pressing banks and the nation's largest retailers to use this system. Given the push by Apple, you may want to consider equipment that can handle both EMV and mobile payment.

But before you buy all new equipment, determine whether your POS vendor can accommodate EMV payment. Since many florists use POS systems provided by the wire services, we reached out to them regarding their EMV status. FTD reports their POS systems will be able to accept EMV early next year. Bloomnet and Teleflora report they should have EMV solutions this year.

Are you a new or small florist without a POS? Square has two separate readers, one for EMV and one for Apple Pay. (But don't judge POS providers on whether they integrate with Square; as one put, "It's like trying to integrate a skateboard with a car.")

Time for Panic Mode?

Maybe you've heard about an October 2015 deadline and liability shift. It sounds scary, but you can continue to process credit cards (including EMV cards) just as you do now with your existing equipment and software. In fact, Javelin Strategy & Research estimates only 23 percent of debit and credit cards will be replaced with EMV cards by the end of 2015.

The change is a shift in liability for sales charged to counterfeit cards. If you process a counterfeit card through a standard swiper before the deadline you are not liable. When the holder of the cloned credit card number disputes charges the credit card company will protect you by making sure that you get paid.

After the deadline the liability for charges to counterfeit cards shifts to you – you won't get paid for sales charged to counterfeit cards. You will only be protected on such charges if they were processed through an EMV terminal.

So as it stands, EMV protects only a fraction of potential, card-present orders. Let's break it down. Orders conducted over the phone or web probably represent 80 percent (if not more) of your transactions so therefore, EMV does not come into play. Of the walk-ins, not all customers will have — or know how to use — EMV cards, and counterfeit card-present fraud EMV protects against is something most florists have not or will not likely experience.

Renato Cruz Sogueco is SAF's chief information officer and the floral industry's go-to tech guy. **rsogueco@safnow.org**

WHAT NOW?

Best practice for now? Stay in touch with your POS vendor and stay up to date on EMV developments. Here are a few links:

- **emv-connection.com/emv-faq/**
- **usa.visa.com** (search "visa merchant chip acceptance readiness guide")
- **mastercard.us** (search "chip-emv")
- **smartcardalliance.org** (search "emv faq")