



To EMV or not to EMV?

That's the question ALL restaurants are asking.

Deciding whether to invest in card-processing systems that accept credit and debit cards embedded with microchips – also known as EMV, or “chip” cards -- is the hottest topic in the restaurant world these days. Here's why: Starting Oct. 1, 2015, merchants who haven't invested in EMV-enabled equipment will be liable for fraudulent purchases made with a counterfeit credit or debit card.

If you're like many restaurateurs, you may be having a hard time building a business case to take action to meet the EMV “liability shift.” Often, the numbers just can't justify the time and cost it takes to implement the technology. Here are a few tips to consider when purchasing and installing EMV-enabled terminals

What's EMV?

EMV® is a global standard for credit and debit payment cards based on chip card technology taking its name from the card schemes Europay, MasterCard, and Visa - the original card schemes that developed it. Long used in Europe, makes it harder for criminals to produce counterfeit credit and debit cards.

Criminals known as “carders” take card numbers, often from hacked businesses, and make counterfeit cards using real account numbers. Counterfeiting remains easier in the United States because of outdated magnetic-stripe technology. EMV technology helps end this kind of fraud because retailers presented with an EMV card can run it through their readers to know it's genuine.

Banks and card companies have begun rolling out EMV Enabled “Chip” cards in the United States. Estimates for how quickly they'll roll out vary widely. One research group estimated that 70 percent of credit cards and 41 percent of debit cards in use in the United States will be EMV-Enabled by the end of this year, yet another predicts 29 percent of credit cards and 17 percent of debit and prepaid cards will be EMV-enabled by the end of 2015.

Unlike in Europe and Canada, the card brands in the United States are only issuing EMV cards that require “chip and signature” authorization. It's not clear when “chip and PIN” will arrive in the United States for EMV cards. Also, for the foreseeable future, the EMV cards that are being rolled out in the United States continue to carry the magnetic stripe. So even if you haven't installed an EMV reader, you can still continue to take and process card payments just as you always have.

Know the facts:

It's important for restaurateurs to know the facts as the Oct. 1 liability-shift deadline approaches. Among the top things to remember:

- **This is a choice.** There's no legal or regulatory requirement for merchants to install EMV readers or take action by Oct. 1. The card brands have simply modified their contracts to penalize those merchants that chose not to implement the technology – and the penalties happen only if a merchant is defrauded through the use of counterfeit or stolen cards. It is a business decision that each company must make.
- **EMV may be a fix for a problem you don't have.** Counterfeit cards have primarily been a problem for high-end retailers, electronic stores and other retailers. Criminals use counterfeit cards to buy high-end goods and resell them on the black market for a quick and easy profit. Typically, carders and other criminals haven't targeted restaurants. If you haven't had a big problem, you may not need to make a change. If you see a growing problem after the October 2015 liability shift, you may want to reevaluate.
- **Weigh the costs.** To evaluate your potential liability, look at how many, if any, of your charge-backs are due to the use of counterfeit or stolen cards. If the numbers are low, it may be hard to justify the cost of EMV-enabled terminals. Even if you experience fraud, the cost of the chargeback may be far less than the cost of installing a new EMV reader(s). As you look at the expense of buying and installing EMV readers, consider whether you're better off investing in new technology that offers stronger protections and more features, such as point to point encryption, NFC, and Pay at the Table features.
- **Ask the right questions as you upgrade.** Is it time to upgrade your POS system to Digital Dining version 7.4.3? This will be the only version that will allow you to incorporate not only EMV technology, but also point to point encryption and use features like Mobile Payment (Apple/Google Wallets) and Pay at the Table technologies. Point to Point Encryption is the highest level of security and immediately encrypts card data as it's entered into the POS system, so it's unintelligible even if it gets stolen. The NRA considers these technologies far more important for restaurants than EMV alone. Your credit card processor and your POS software will determine the available solutions as the features and equipment can vary, both vendors have to work together to have an "integrated" solution. You need to plan on upgrading your software to help you accommodate all the technologies coming along.

In summary: EMV helps you deal with counterfeit cards, but point to point encryption will protect a restaurant from hacking and data breaches – and that's a bigger threat to a restaurants' bottom line because it could subject you to huge fines from card companies, customer lawsuits and damage to your restaurant brand. There are many technologies evolving for operators over the next 6-12 months please contact your dealer to evaluate options available for your operation now and moving forward.

Visit <http://www.restaurant.org/paymentsHQ> for more information.