Business Circle
brought to you by AT&T

Are you ready for EMV?
A guide to the new credit card standard

How EMV can benefit your business

EMV® chip technology will soon become the standard for in-person card payments in the U.S. It is named for developers Europay, MasterCard®, and Visa®, and centers on new, microchip-enabled credit and debit cards that make transactions more secure. EMV is already in place in much of the world, and in some countries, fraud has dropped by more than 80 percent, according to _Wells Fargo Merchant Services_.

Businesses that accept in-person card payments have incentive well beyond fraud prevention to support EMV. Starting **October 1**, any business unable to process EMV chip cards will be held responsible for certain fraudulent transactions that are currently covered by card issuers.

This guide was developed to help prepare your business for EMV. It provides information on EMV, a timeline for meeting the October deadline, and tools to support you through the process. Sections include:

What will EMV mean for your business?

The transition to EMV is already underway. Banks and other card issuers are now sending chip-enabled cards to customers; by the end of this year, 70 percent of credit cards and 41 percent of debit cards are expected to support EMV, according to research and advisory firm Aite Group.

Following these steps can help ensure you are ready for the October deadline:

Check your current payment hardware

If you purchased your point-of-sale (POS) hardware within the past five years, it may already be "EMV-capable," meaning it has a slot at the bottom of the terminal for accepting chip cards. If this is the case, you may be able to keep the terminal, but it will likely need a system upgrade so that it can begin reading the chips. Your merchant services or POS system

provider can confirm this and help you upgrade. They can also suggest replacement options if you will need a new terminal. Keep in mind that mobile card readers, such as Square® or Intuit® GoPayment, will also need to be replaced.

Consider POS software

If you use a more robust POS system—for example, one with advanced payment features or inventory management capabilities—ask about new software that might be required along with replacement hardware. If your system is heavily customized—i.e., programmed to meet your business's specific requirements—you may need to work with your vendor to arrange for testing and certification as part of upgrading the system. This process may take up to a few months, so it is best to start early.

Explore system replacements, if needed

Chip cards require customers to either sign a receipt (known as "chip-and-signature") or enter a personal identification number (known as "chip-and-PIN") to confirm purchases. The hardware you choose should support both transaction types. (If you plan to upgrade your current system and it does not have PIN functionality, consider buying an external PIN pad that can be attached to your terminal.) Though "chip-and-PIN" cards and transactions will be less common than "chip-and-signature" in the beginning, some experts believe they will become more popular in the future because they are considered more secure.

As you explore new hardware, consider features that might benefit your business long term. For example, investing in a terminal that reads both standard chip cards and "contactless" cards (which are waved in front of the card reader rather than inserted) can allow you to support mobile payments such as Apple Pay™. Using this type of terminal may also enable you to waive certain PCI-DSS assessment requirements. (See *"5 reasons EMV is good for your business"* on **pg. 11.**)

Train your staff

Your customer-facing employees will need to be comfortable using new hardware and helping customers through EMV transactions. Though these transactions are not difficult to complete, they differ from magnetic-stripe transactions in a few key ways. For one, customers will need to insert their chip cards face up into the terminal, rather than swiping them. They will also need to keep their cards in the terminal for the entire transaction. (The first generation of EMV terminals will include a slot for swiping magnetic-stripe cards, so you will still be able to service customers who have not yet received their chip cards.)

Protect card-not-present transactions

Because the EMV shift applies only to in-person transactions, businesses that sell solely online or by phone or mail order will not be affected. As in-person card fraud becomes much harder to commit, thanks to the security of EMV technology, experts expect

spikes in so-called "card-not-present" fraud. Companies that sell through these channels, particularly through the Internet, should take steps to strengthen their security.

Explore fraud protection services that credit card companies offer. For example, _Verified by Visa_ and _MasterCard_® _SecureCode_™ require customers to confirm their identity by entering a previously chosen password or code before making online purchases, which helps ensure that no one else can use the card. Also be sure to take advantage of shopping cart features such as address verification, which compares order addresses with those on file with customers' credit card companies, and card code verification, which uses a card's three- or four-digit number to validate customer information on file with the card issuer. Stay alert for unusual activity, such as orders in which the cardholder and recipient names are different, or multiple large orders being shipped to the same address.

Timeline for U.S. EMV rollout

Now-2017: Banks and credit card companies issuing EMV chip credit and debit cards. The first generation of chip cards includes a magnetic stripe so that they can be processed at non-EMV machines.

October 2015: "Liability shift" goes into effect for in-person American Express, Discover, MasterCard, and Visa transactions.

October 2016: Liability deadline for MasterCard ATM transactions.

October 2017: Liability deadline for Visa ATM transactions and automated fuel dispenser terminals.

Why chip-card transactions are more secure

The security of EMV transactions comes in large part from the microchip embedded in each card. When a card is read, the chip generates unique data that can never be used again. If criminals were to capture information from one sale, it would be useless later on. Magnetic-stripe cards, by comparison, save and transmit payment information in unchanging form that is easy for experienced fraudsters to replicate.

Security is also built into each step of the transaction process:

Card authentication. Once a customer inserts a chip card face up into the terminal (or waves the card in front of it, if a contactless card), the card and the terminal jointly authenticate the card based on technology that has been programmed into each. The terminal then goes online, and the card then generates a "dynamic cryptogram"—the data unique to that transaction—which the card issuer validates. Because the terminal plays an important role in verifying chip cards, the cards must stay inserted for the duration of the transaction.

Cardholder verification. Once the card is authenticated, the terminal prompts customers to either sign a receipt or enter a PIN to confirm their identities and verify their purchases. PIN verification offers particularly strong protection against using lost or stolen cards, since the number is required to complete transactions. The card will allow a certain number of PIN attempts (determined by the card issuer) before declining a transaction.

Transaction authorization. The issuer decides to authorize the transaction based on a host of information, such as whether or not it recognizes the cryptogram, the cardholder verification, and the transaction amount. If the terminal is offline—as it might be, for example, if at a ticket kiosk or if it simply loses connectivity—the terminal authorizes or denies a transaction based on "rules" the issuer has pre-programmed into the chip, such as how many transactions have been made on the card and the number of PIN attempts made versus the number allowed before a transaction is declined.

5 reasons EMV is good for your business

Transitioning to EMV will require time, money, and patience as customers and staff adjust. Yet the long-term benefits to your business and customers may far exceed the costs. More secure card transactions means fewer fraud-related hassles and more confidence in making card purchases.

Consider these benefits of making the switch:

1 Reduced risk of fraud on your own card purchases

Just as EMV can significantly reduce the risk of fraud for customer transactions, it can also protect card purchases you make for your business. Because chip cards are nearly impossible to counterfeit, there is little incentive for fraudsters to steal card data. That makes everything from business-supply purchases to travel reservations more secure.

2 Fewer chargebacks

Though card issuers are now liable for in-store transactions that customers flag as fraudulent, these costs may be shifted back to merchants if they cannot provide adequate documentation of these transactions. The fraud protection that chip cards provide will likely mean fewer of these chargebacks. This will be especially important once the shift in liability takes effect October 1. Some experts believe fraudsters will target magnetic-stripe cards more aggressively, meaning chargebacks could spike for businesses that do not support EMV.

3 Ease of use abroad

Using chip cards will potentially simplify many aspects of business travel. The EMV payment standard is already used in much of the world, and many merchants abroad prefer not to process less secure magnetic-stripe cards. In Europe, some self-service terminals (at train stations, for instance) do not even read magnetic-stripe cards. From an acceptance standpoint, supporting chip-card payments may help international customers who are already accustomed to EMV payments feel more comfortable buying from your business.

4 Potential to expand POS capabilities

Purchasing new hardware for EMV compliance can give you an opportunity to gain functionality that could improve your return on investment long term. For example, if you have basic POS equipment now, but have been considering a system with inventory management or loyalty program features, preparing for EMV may be a good opportunity to add these capabilities.

Purchasing EMV-enabled hardware can also help you prepare for future payment methods. Most EMV terminals also support near field communications (NFC) technology, which makes it possible to accept Apple Pay™ and other contactless payments. The cost of basic EMV/NFC terminals starts at under $200.

5 Reduced PCI-compliance requirements

Visa, MasterCard, American Express, and Discover have announced that they will waive businesses' annual PCI Data Security Standard reporting requirements if they conduct at least 75 percent of their card-present transactions through terminals supporting both contact and contactless EMV payments. This reporting requirement, which verifies that businesses are protecting customer data, is typically met by completing a self-assessment questionnaire. Businesses will still need to maintain PCI compliance, but they will not need to validate compliance with the payment brands.

How to keep your customers happy during the EMV switch

Though EMV chip technology will ultimately improve the security of in-person card payments, there may be some snags in the beginning. Businesses in Canada and overseas that have already integrated chip cards experienced some snags at checkout initially. Review the following to learn about these customer service hiccups and how to avoid them:

1. **Card leave-behinds.** Because chip cards remain in the terminal for the duration of transactions, it can be easy to forget to remove them. In Canada, which adopted EMV in 2007, the problem was so widespread that terminals were reprogrammed to include prompts for card removal, the publication *Digital Transactions reported*. Train your staff to remind customers to take their cards with them and post a sign by your terminal. Be sure to have procedures in place for customers to retrieve forgotten cards such as a locked drawer for storing cards and a photo ID requirement for card pick up.

2. **Card sliding issues.** Customers may think that they should insert and remove their cards quickly, similar to how they use ATMs. Doing this will lead to a transaction being denied. Worse, inserting and removing a card repeatedly may lead to multiple

charges appearing temporarily on a customer's account. Tell customers to leave their cards in until after they have signed a receipt or entered their PIN.

3. **Terminal malfunctions.** Terminal providers typically offer guides that include solutions to common problems or error codes. If your terminal loses connectivity, transactions may be able to proceed offline using the rules that the card issuer has programmed into the chip. In cases in which a card's chip or the chip reader malfunctions, transactions may be completed using the magnetic-stripe reader, though you will be liable for losses associated with any fraudulent transactions. Guidelines vary among payment processors, so know what yours requires.

4. **PIN issues.** Using PINs for credit card sales will be new to many customers. In places where chip cards have already been rolled out, some people have had trouble remembering their PINs to complete credit card transactions. In most cases, customers will need to contact their card issuer or log into their account to reset their PIN.

How prepared is your business for EMV?

With the EMV liability deadline fast approaching, taking steps now to accept chip cards can help you avoid fraud-related costs and make shopping safer for you and your customers. Use this checklist to identify the steps you need to take to achieve EMV compliance and to track your progress. Because the timeline to compliance varies among businesses, start now to help ensure you are ready by **October 1, 2015**.

○ **Check POS hardware.** Determine if your current POS terminal(s) include a slot for chip cards. If they do, they may need only a simple upgrade to support EMV transactions; your merchant services or POS system provider can confirm. If your terminals do not have a chip-card slot, talk with your provider

about EMV-compliant hardware that can meet your business's needs.

○ **Consider software.** If you have a more complex POS system that includes advanced payment functions, inventory management or other capabilities, ask your provider about any necessary software upgrades you may need, along with new hardware. If your system is heavily customized, talk with your vendor now about testing and certification requirements you may need to meet, as these can take months to complete.

○ **Explore new POS equipment, if necessary.** Look for hardware that supports chip-and-PIN as well as chip-and-signature transactions. If you've considered adding new features, such as inventory management or support for digital wallet technologies (e.g., Apple Pay), explore systems that include these features.

○ **Upgrade mobile hardware.** If you use a mobile card reader, such as Square or Intuit GoPayment, you will need a new reader that processes chip cards. You may be able to order these on the provider's website or by contacting the company.

○ **Prepare for different chip-card transaction types.** Be sure you and your staff know how to handle chip-and-signature and chip-and-PIN transactions.

Role-play through different scenarios so that everyone knows how to spot chip cards, help customers insert them properly, and keep them in the reader throughout transactions.

○ **Implement chargeback prevention procedures.** Instruct employees to keep receipts and other records of customer card transactions, including transaction dates, amounts, and authorization information. Be sure all purchases requiring signatures are signed for and that receipts for PIN purchases state the transaction is PIN-verified. Your card processor may have additional rules for accepting cards, so be sure you are familiar with these.

○ **Protect card-not-present transactions.** If you sell online, consider improving the security of these transactions by using a fraud-protection service offered by the credit card brands, such as _Verified by Visa_ or _MasterCard SecureCode_. Stay alert to unusual activity, such as orders in which the cardholder and recipient names are different, or multiple large orders being shipped to the same address.

Frequently asked questions

Having answers to your questions about EMV will help you quickly and smoothly make this important transition. Use these FAQs to find information not covered elsewhere in this guide. Have more questions? Join the EMV conversation on [Business Circle](#).

Q **Why is the U.S. adopting EMV now?**

A As other countries adopted EMV, more in-person card fraud began to shift to the U.S. Although 23.5 percent of card transactions worldwide are processed in the U.S., the country accounts for nearly half of all incidents of card fraud, according to the *The Nilson Report*, an industry newsletter. High-profile data breaches at Target, Home Depot, and other retailers have also spurred demand for more secure payment methods.

Q Will the transition to EMV be complete on October 1, 2015?

A No. Because the U.S. is a large and fragmented market, and because POS specifications for EMV compliance were just released late last year, the changeover will likely span the next couple of years. Still, businesses should migrate to EMV as soon as possible to reap security benefits and minimize fraud liability costs.

Q How much do EMV terminals cost?

A This depends on the complexity of the terminal. A basic countertop terminal can cost anywhere from $100 to $500, depending on screen size, memory, connectivity, and other features. More robust POS systems with advanced payment features, analytics, inventory management capabilities, and loyalty program support may cost upwards of $1,500.

Q If my volume of in-person card sales is very low, do I still need to support EMV?

A No business is required to support EMV. However, those that do not could face significant fraud-related costs following the liability shift. Even

if you process relatively few card sales or have experienced little card-present fraud in the past, not accepting chip cards may place you at risk, since fraudsters will likely begin targeting less secure technologies (i.e., magnetic-stripe cards).

Q **If chip-and-PIN transactions are more secure than chip-and-signature, why are most of the cards being issued in the U.S. chip-and-signature?**

A Card issuers believe that requiring a signature rather than a PIN, particularly for credit card transactions, will help the rollout proceed more smoothly, since the process is familiar. Some experts predict chip-and-PIN cards to be more widely used in the future.

Q **Do POS systems that include inventory management features or customer management capabilities need certification and testing?**

A Unless your system is heavily customized with functionality specific to your business, you most likely will not need to go through certification and testing. If you use a non-customized or minimally customized system with features such as inventory management, customer loyalty, and/or analytics, the vendor will complete this process in most

cases. Talk with your vendor if you have any doubts.

Q Will EMV prevent data breaches?

A No, but it can help reduce their frequency.
Encryption, fraud-protection tools (such as
those offered by the major payment brands),
and vigilance can also help protect transactions
and customer data, particularly for online and
other card-not-present sales.

EMV by the numbers

1986
Year that EMV payments were launched, in France

130
Number of countries in which EMV is used

59
Percentage of U.S. POS locations that will be chip-capable by the end of 2015, according to _Aite Group_ research

47
Percentage of fraudulent card transactions worldwide that occur in the U.S., according to _The Nilson Report_

600 mil
Number of chip cards expected to be in circulation in the U.S. by the end of 2015, according to the _EMV Migration Forum_

$3.50
Average cost for issuing a new chip card

EMV resources

As you prepare your business for EMV, information from banks, card issuers, and other organizations can help you find the hardware you need and ensure there is nothing you have overlooked. Here is a partial list of resources:

American Express Knowledge Center

https://knowledgecenter.americanexpress.com/american-express-chip-technology-video

Resource center including a video on chip card technology and stories of business owners who have migrated to EMV.

Bank of America® EMV Resource Center

https://merch.bankofamerica.com/emv-resource-center

Merchant-focused web page with links to an EMV migration guide and information on the liability shift.

Chase Paymentech™ EMV FAQ

https://www.chasepaymentech.com/faq_emv_chip_card_technology.html

Extensive list of questions and answers for merchants, including links to a whitepaper and video.

Citibank® Chip-and-PIN FAQ

http://www.citibank.com/transactionservices/home/email/a2/misc/102349_chip_and_pin/cardholder_faq.pdf

List of common questions and answers about using chip-and-PIN cards.

Discover EMV Resource Center

http://www.discovernetwork.com/chip-card/merchants

Website including articles, archived webinars, and other resources to help merchants transition to EMV, with an emphasis on Discover chip cards.

EMV Connection

http://www.emv-connection.com/emv-resources

Website featuring comprehensive EMV-related information for business owners, consumers, card issuers, and others. Includes archived webcasts on a wide range of EMV-related topics.

First Data™ EMV Resource Center

https://www.firstdata.com/en_us/all-features/emv.html

Website by the payment technology company that includes EMV tutorials, articles, and more.

GoChipCard

http://www.gochipcard.com/merchant

Online resource developed by the *EMV® Migration Forum* and the *Payments Security Task Force* with basic chip card information for business owners and consumers.

MasterCard EMV Resources

https://www.mastercard.us/en-us/issuers/products-and-solutions/grow-manage-your-business/payment-innovations/chip-emv.html

Web page that explains the EMV standard, chip technology, and their potential to reduce fraud. Also includes links to other EMV resources.

Visa U.S. Merchant Chip Acceptance Readiness Guide

https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/resources/merchant-toolkit/index.jsp?page=toc

10-step guide to help business owners plan EMV chip implementation for contact and contactless transactions.