Why You Should Adopt EMV® Chip Card Technology

A perspective on EMV following the liability shift. Get ready now.

EMV chip card technology is here. It is crucial to plan a strategy before implementing EMV.
With EMV chip card technology, the card brands have introduced “liability shifts.” If your payment devices are not EMV enabled, your business could be held liable for counterfeit fraud losses when chip cards are used (card-present transactions only). We can help you understand the cost/benefit of adopting EMV.

**EMV: The Backstory**

EMV is a new technology standard that defines a set of requirements to ensure credit and debit cards can be securely accepted on a common standard worldwide. For this paper, we are focused on those new specifications for cards that have a computer chip embedded in them rather than the more traditional magnetic stripe. This security standard is currently used by credit card issuers and merchants in most countries except the U.S.

In most parts of the world, the retailer is able to take advantage of the security chip by having the cardholder “dip” their card into a card reader, where the card can be authenticated. And when used with PIN codes, EMV chip cards provide retailers and banks greater confidence that a card’s user is its true owner by combining something the card’s real owner would have and something only they would know. Because EMV is not universally deployed, however, even chip cards continue to have magnetic stripes that are used to authenticate the card at a traditional point-of-sale (POS) device. To fully take advantage of all the new chip technology has to offer, U.S. retailers will need to invest in chip readers for each device.

EMV originated as a collaboration among EuroPay (later purchased by MasterCard®), MasterCard and Visa® and was implemented in Europe in the 1990s. By some estimates, almost half of all payment cards issued outside the U.S. have an EMV chip. Although the chip virtually ensures that the card has not been counterfeited, issuers can further customize EMV cards by, for example, requiring cardholders to enter a PIN for each purchase instead of the current standard of signing a receipt.

Given some recent large-scale data security issues, there was a renewed push for EMV adoption in the U.S. Because most other major international markets have adopted EMV, criminal rings had taken to using stolen card numbers predominantly in the U.S. This so-called “fraud migration” was costing banks and merchants. As a result, the major payment networks decided that the U.S. needed to be quickly brought up to the global security standards to ensure the integrity of international commerce.
The Current Plan for EMV in the U.S.

The EMV Directive

In 2011, Visa and MasterCard announced that starting in October 2015, any card-present counterfeit fraud losses would be the responsibility of the party that had the least secure authentication capability, with EMV being the most secure card standard. This is referred to as the “liability shift.” Thus, if a merchant’s POS device is not EMV enabled, the fraud loss would be charged to the merchant. However, if a merchant’s POS device is EMV enabled, but a counterfeit card used for payment had a magnetic stripe only, the issuing bank would be charged for the loss. In the event that neither party adopted EMV standards, the current fraud liability standards would apply. The liability shift does not affect the cardholder’s liability; if they have a fraudulent charge, the issuer still assumes the liability. While the networks have not required whether banks must require “chip and signature” or “chip and PIN,” some are already considering PIN authentication a more secure option. In “chip and signature,” a cardholder presents an EMV card into a POS reader, and otherwise signs the receipt as they would with a magnetic stripe card. With “chip and PIN,” the cardholder keys in a PIN instead of signing the receipt, allowing the retailer to rely on the bank’s authentication rather than having a sales clerk verify the draft signature against the signature on the back of a card. The advantage of “chip and signature” for banks and merchants is that it most closely resembles the checkout process today. But, some experts argue it does not authenticate the cardholder’s identity as well as a PIN does, and lost or stolen cards can still be used. The advantage of “chip and PIN” is that both the card and cardholder are effectively authenticated. PIN initiation, however, is a more onerous process for the banks and cardholders; as a result, there is more complexity and less adoption of implementation.

Issuer Perspectives

Despite being new, EMV is not completely unknown in the U.S. One large retailer with a private label credit card program, for example, launched EMV cards in the early 1990s, but did not continue with the project. Banks are familiar with the technology and have issued some EMV chip cards on a small scale, but have historically been reluctant to issue these cards en masse. In recent years, that reluctance diminishes when a bank knows that a cardholder will be traveling internationally and introduces a hardship that could limit cross-border spending. As a result, some banks, including Bank of America, selectively issued EMV cards to customers in travel-related and other rewards programs. Thus, instead of issuing one billion payment cards, the banks focused only on those customers for whom a magnetic stripe might not allow a completed purchase.
Merchant Perspectives

At the same time that banks are addressing the challenges of issuing a new type of card for customers, merchants are assessing their own implementation costs and efforts. Some estimates to install EMV-enabled terminals and other hardware in the U.S. are as high as $6.75 billion, which includes the costs of hardware for POS chip-reading devices and PIN-pads. Merchant acquirers have already borne additional costs to undertake substantial modifications for ensuring that the chip cards function properly, but are ready to support merchants in this acceptance. Many merchants have integrated POS devices with levels of customization that require effort and time to assess, change and test. That’s why it’s best for merchants to engage in a discussion with their payments processor.

It will likely take a couple years (or more) after the October 1, 2015 liability shift for magnetic stripe cards to be replaced, for consumers to get used to paying with chip cards and for merchants to migrate to equipment that accepts EMV cards.

The overhaul will take immense coordination between merchants, their acquirers and the payment networks. Credit payments are not processed exactly like debit payments, so even though a retailer may have a PIN-pad already, the debit information may be packaged and routed differently depending on a number of bank and network considerations.

Bank of America Merchant Services
The New Rules of Participation

Even though Visa and MasterCard generally do not bear any financial liability for fraud (unlike Discover® and American Express®, who are also issuers), their businesses are predicated on bringing confidence to retailers and banks that, when the rules are followed, payments will be processed. They do not require that you purchase a particular POS device or how issuers authorize a particular transaction, but they can establish rules and standards to encourage migration.

In that spirit, the four major networks in the U.S. (Visa, MasterCard, American Express and Discover) have published rule changes to promote the move to EMV in the U.S.\textsuperscript{7}

The explicit benefits for your business primarily relate to relief from security testing, reporting requirements and data breach fee reductions. Although you must continue to comply with the Payment Card Industry Data Security Standard (PCI DSS), the assessment and audit burdens should be reduced if substantial numbers of transactions are processed using EMV-enabled POS devices. Some card networks also offer a reduction in overall fees associated with a merchant data breach if one occurs.\textsuperscript{8}

Previously, card issuers held most of the burden of fraud losses from lost, stolen, counterfeit and otherwise compromised account numbers. For the same reason EMV cards are more expensive than cards with magnetic stripes, they are more difficult to counterfeit. By migrating to EMV cards, issuers will be more confident that when presented at an EMV-enabled POS device, the card is legitimate and the fraud risk is reduced. And, if the chip card is presented at a magnetic stripe POS device after the liability shift, the issuer would bear no financial responsibility for the resulting fraudulent charge, even if the card is counterfeit.\textsuperscript{9}

The payment networks hope that these changes will reduce, if not eliminate, counterfeit fraud in transactions with physical cards. The EMV conversion experience in the United Kingdom demonstrated that fraud rates dropped by 34%\textsuperscript{1} in the six years following the introduction of the EMV standard, although the fraud that U.K. issuers absorbed from non-EMV markets such as the U.S. and with card-not-present (CNP) merchants remained stubbornly high.\textsuperscript{1}

It is worth noting that based on EMV deployments in Europe, experts anticipate a rise in CNP fraud in the U.S. as a result of EMV rollout here. This is especially significant because online sales are a rapidly growing segment of all consumer transactions. An increased incidence of CNP fraud as a result of EMV deployment in the U.S. will cause online retailers to focus more attention on other fraud prevention, like stronger identity authentication and data protection strategies such as 3D Secure and tokenization.\textsuperscript{10}

Beyond the increased fraud concerns, EMV is effectively a non-issue for eCommerce and other CNP merchants, because they do not have any POS devices. But the potential migration of fraud will still have an impact on U.S. commerce.
Why Switch to EMV?

First, determine whether a case exists for switching to EMV, leaving aside any added expense and implementation effort. In Western Europe, 90% of merchant terminals accept EMV cards, but presumably acquirers will still accept processing for non-EMV merchants. Consider these four determining questions:

1. **Does my business serve international customers?**
   Approximately 75% of all Western European cardholders have EMV cards, and the figure is even higher for Canadian consumers. Before the liability shift, more international banks were declining to authorize transactions, thereby preventing sales. With the liability shift, an effective way to help minimize fraud risk and ensure payment for the sale is to properly accept EMV cards.

2. **Does my business serve the travel and entertainment industry?**
   More travel-oriented cards, including corporate travel and entertainment cards, are being issued with EMV chips in the U.S. to enable their use abroad. To the extent those cards are also used in the U.S., merchants will have a higher risk of fraud in the event the cards are compromised. And as we saw with international customers, the best way to ensure payment for a sale is to properly accept EMV cards.

3. **Do I sell merchandise that is desirable to criminals?**
   Banks have historically analyzed each merchant category for the possibility that a cardholder may later dispute the charge for fraud reasons (so-called “high-risk merchants”). As banks issue EMV cards, the burden of any of these disputes may fall more on merchants. Whereas merchants had come to rely on the bank’s authorization of a transaction, since the EMV liability shift, the bank has a reduced incentive to monitor for potential counterfeit fraud where a chip card is presented to a merchant who is not EMV-enabled. Even if a merchant has scant exposure to fraud today, fraud rings may seek out non-EMV merchants.

4. **Will I be perceived as “less secure” if I don’t accept EMV?**
   In the wake of several high-profile data breaches, some banks reissued cards even in the absence of any detected fraud. Consumer perceptions of what constitutes secure commerce are important, and if consumers grow to accept that reading a chip is more secure than swiping the magnetic stripe, retailers should be prepared to respond to this consumer preference.

So, if the answer to any of these is “Yes,” then we maintain that accepting EMV payments will be a necessary cost of doing business. If the answer to all of them is “No,” then you should review the questions as market or business conditions for the payments landscape change, and consider other facts and circumstances that may be specific to your business.
Choreographing EMV Implementation: What Exactly Changes?

For EMV technology to function properly, it is important to understand the fundamental change the EMV chip brings.

Before, each magnetic stripe card was formatted consistently across issuers and encoded with the same types of information. When swiped, the POS knew how to read the static information, the acquirer knew how to interpret the information and the transaction processing could begin. The POS device was merely an access device to a messaging network where all parties involved exchanged information about the transaction.

With EMV, the POS device will have the ability to interpret dynamic information on the chip, authenticate the card more definitively and (depending on the issuer) determine how a transaction should be processed. With EMV, processing starts with the card, not after a message has been relayed. For example, an issuer can even place logic on the card to perform authentication offline, thereby avoiding sending and receiving messages over the network.

For EMV to improve the integrity of the transactions and for your business to get the full benefit of your investment, it’s important to understand and assess six key functions. It is critical that these functions act in concert with one another to help increase efficiency and reduce your business’ costs for transactions:

1. **Transaction processing**. Transactions are initiated at your business and transmitted to the acquirer and networks for processing. Each payment network has provided implementation standards based on the EMVCo Standard Specification, which means each payment network has slightly different rules. For instance, Visa prefers issuer choice of validation method⁴, while MasterCard prefers PIN as a cardholder validation method.⁸ Furthermore, you have choices as well for the cardholder validation methods you accept. You may prefer PIN to signature. You can choose this preference, but of course, for any situation, only the options provided by the issuer on the card will be available as a choice.

2. **The POS device**. Just like the current marketplace for POS devices, you already have many hardware and software choices with EMV capability. When choosing devices to support EMV, there are additional considerations, such as whether you will support other new technologies like mobile and near field communication (NFC) payments using the EMV contactless specification. Also, because the payment networks require EMV certification for each solution accepting those card types, it is important to consider the timing of changes to minimize how often a product needs re-certification.

With EMV, the POS device will have the ability to interpret dynamic information on the chip, authenticate the card more definitively and (depending on the issuer) determine how a transaction should be processed.
3. **Device management.** The choices do not stop at simply selecting EMV-enabled hardware and ensuring it is certified. Implementing EMV acceptance devices requires ongoing support of both software and hardware. EMV terminals must be able to receive regular remote updates. Also, periodic EMV kernel expiration and POS updates will require your acquirer or payment processor to receive new certifications. Maintenance — to help avoid potential fraud costs or other issues — will be critical for any business adopting new EMV-enabled payment systems.

4. **Cryptographic management.** EMV technology also uses cryptograms offering different levels of security. It is important to coordinate with your acquirer or payments processor on card validation and ensure your security needs are met. There are multiple “approved” solutions, depending on the level of security and whether you choose to accept offline transactions.

5. **Training.** There are changes in how a consumer will interact with payment devices when using EMV cards. For example, with magnetic stripe cards, U.S. consumers typically swipe their credit cards, and then wait for payment details and sign. With a chip card, payment transactions can be processed either by a card reader physically contacting the chip (contact transactions where the card is inserted into the terminal) or by the reader being sufficiently close to the chip to detect it and exchange data (contactless transactions). Your customer-facing personnel will need to be aware of these changes and how to assist customers. Training for these staff on new systems will be crucial.

6. **Integration.** With EMV using enhanced authentication to address counterfeit issues in card-present transactions, it is still critical to transmit consumer data from your business using an encryption and tokenization solution. It is important that you protect cardholder data as well as minimize fraud. While you are upgrading your POS environment to EMV, it may be a good time to consider enhancing the customer experience by adding other services like dynamic currency conversion for international travelers and support for mobile phone-based loyalty and marketing programs.
Additional Migration Considerations

We have covered broad categories to help identify the information and factors you should consider. From a more practical standpoint, it’s important to understand the elements of cost and the customer payment experience.

Costs of Migrating to EMV

The immediate costs of EMV migration relate to the purchase of POS devices and PIN-pads — plus test cards, certification costs, IT resources and more. As with the original POS decision, however, you’ll need to think about more than the investment you are making in hardware. Consider the functionality and flexibility the new terminals can offer. And, be sure to weigh the potential liability of fraudulent transactions if you are not EMV enabled.

We recommend evaluating your POS selection decision on the basis of total cost of payment acceptance over the life of the equipment, and not just on minimizing a 2015 and/or 2016 expenditure. For example, while initial costs may be high in migrating to a new system, the decrease in fraud may more than offset the upfront expense. Or, the increased security of card-present transactions may spur additional business from customers wary of broader card data security issues.

Customer Experience

As a merchant, the customer payment experience should be top of mind when considering an EMV POS device selection. It goes beyond just purchasing the right device for your customers’ needs and your own. Remember to think about the effort to implement EMV in your business, and devote the resources necessary to make it a smooth transition. That means training staff on both purchases and returns, troubleshooting potential problems, and knowing when to escalate payment-handling issues to outside support.

Although the card issuers should educate their customers on the proper use of chip cards, you may find yourself educating your own customers in a more direct fashion. After all, your checkout person probably has a more hands-on payment interaction with your customer than the issuing bank.
Key Takeaways

EMV has arrived in the U.S. Approximately 95%\(^1\) of all POS devices in Western Europe are EMV enabled, and the U.S. is likely to attain a similar level of penetration as U.S. issuers promote EMV credit and debit cards.

This means it is time to make key decisions, if you have not done so yet, about your POS system.

Effective October 1, 2015, your POS must be EMV enabled or you’ll face liability for card-present fraudulent card transactions that occur in your business. You may be inclined to weigh the costs of updating your POS against the risk of fraudulent transactions in your business or market segment. However, the question is larger than that. This may also be an ideal opportunity to modernize your POS systems for improved business performance, through the addition of services such as integrated loyalty programs, tie-ins to eCommerce, business performance dashboards, dynamic currency conversion if your business sees many foreign travelers, and other services.

Perhaps most important of all, this transition to EMV provides an opportunity to evaluate your payment processing service provider. The ideal payments acceptance partner will understand security issues and recommend the right EMV choices for your business, what kind of POS system is best for your business, and what additional POS services are available to enhance the customer experience and help improve overall business performance.

EMV is here. If you haven't done so, now is your opportunity to develop a strategy and roadmap for this change.

To get the most value out of an EMV upgrade, carefully consider how your business and customers will be impacted by the coming transition.
Get Started

EMV chip card technology is here, and we’re ready to help you plan a POS strategy for your business.

We can help guide you through:

• Your decision-making process
• EMV compliance requirements
• Weighing the risks and costs
• Creating the best experience for your customers

We can also help you take a fresh look at modernizing your POS system to maximize what it can do for your business, and evaluate other products and services that can help improve overall business performance.