The Ultimate Guide to Understanding EMV

bematech

Intelligence for business.

Today, electronic payments represent a significant percentage of transactions for even the smallest retail and restaurant operations. However, along with the convenience and expanded customer options associated with accepting credit and debit cards come a range of security responsibilities for merchants, highlighted by several recent high-profile data breaches.

The U.S payment industry is preparing for one of the biggest changes in the past forty years – the advent of EMV. EMV (Europay, MasterCard, and Visa) is a set of global standards for electronic payments, including specifications for Point of Sale hardware, software, and systems, as well as the payment cards themselves.

> *Every EMV enabled card contains an embedded chip or "smart chip." The smart chip uses a dynamic authentication process or "digital handshake" between the chip and the payment terminal that is unique to each transaction. If a hacker stole chip card information from a point of sale terminal, typical data replication would be useless because the transaction code created for that one instance would not be usable again and the card would be declined. In contrast, a magstripe card's data is static or unchanging, meaning if it's stolen once, the data can be replicated over and over again.*

The EMV standards and technology aren't new, but they are less well-known in the U.S. than in other parts of the world. In fact, they are a global success story: EMVCo, which manages EMV specifications and testing processes, reported that the number of EMV payment cards in circulation jumped by one billion in 2014, hitting a total of 3.4 billion by the end of last year. Globally, just under one-third of card-present transactions (i.e. those not conducted over the phone or online) are now EMV.

The U.S. is one of the last major markets to adopt EMV, but payment card issuers have been aggressively playing "catch-up" in anticipation of the shift to these standards. Aite Group estimates that by the end of 2015, 70% of U.S. credit cards and 41% of U.S. debit cards will be EMV-enabled. (Many of the cards already in consumers' wallets are dual-enabled, meaning they feature both the traditional magstripe and an embedded smart chip.)

Understanding the EMV Liability Shift

What's behind the EMV shift? In addition to bringing U.S. payment systems into alignment with an increasingly globalized economy, the greater security offered by EMV is highly likely to lower fraud rates. Criminals are attracted to U.S. consumers and merchants not just because of the size of this market but because current U.S. payment systems are a "weak link" compared to other countries. The numbers are significant: a report from Javelin Research found that more than $11 billion was reported due to credit and debit card fraud in 2013, up from $8 billion in 2012.

As a way to motivate merchants to upgrade their payment systems for EMV acceptance, the major card issuers (Visa, MasterCard, American Express, and Discover) will institute a liability shift beginning October 1, 2015. (There will be similar shifts for ATMs in October 2016 and for fuel dispensers in October 2017.) Traditionally, liability for fraudulent transactions was absorbed by card issuers or financial institutions. The shift puts the responsibility on the weakest link in the payment security chain for certain transactions. In this case, that would be a merchant that has not upgraded its POS to handle EMV transactions.

Specifically, if a retailer or restaurant is presented with a fraudulent dual (EMV and magstripe) card, and processes that card using magstripe technology, the merchant will be liable for losses that are incurred. Given that data thieves tend to seek out the least secure targets, merchants who delay their POS upgrade efforts may find they are the object of increased fraud attempts compared to their counterparts who have upgraded their POS to accept EMV cards.

Along with the threat of financial losses, several major card companies are offering incentives to move to EMV, such as audit relief from PCI-DSS (Payment Card Industry Data Security Standards), or reduced chargeback fees.

STEP 1: ASSESS YOUR CURRENT POS SYSTEM

In preparing to accept and process EMV-enabled card payments, retailers and restaurants will need to audit the capabilities of their current Point of Sale solutions – everything from the devices used to read customers' cards to how transaction data is communicated, authenticated, and processed. It's also important to carefully document exactly where your POS system is now, so that you can monitor and measure the cost and impact of the changes you'll be making.

The major components of a POS system include:

> **POS software:** Check with your software provider, VAR, or ISV to determine if your latest software upgrade or patch brings software in line with EMV specifications.
>
> **POS hardware:** Because chip cards are "dipped" rather than "swiped" as magstripe cards are, hardware and peripheral upgrades may be necessary. Find out whether your current hardware is already EMV-capable, or has sufficient communication ports to support EMV-compatible PIN pads, payment terminals, and other hardware.
>
> **Electronic cash registers:** To accept card transactions the electronic cash register systems often rely on 3rd party systems for credit card acceptance. Merchants can check with these 3rd party software, hardware, and services providers to learn about the products for EMV conversion.
>
> **Credit card terminals and PIN pads:** In many cases you will be able to keep elements of the existing POS system, by updating to EMV-capable credit card terminals and PIN pads at your primary POS location as well as at other cash wrap stations.
>
> **Integrated elements:** If you have deployed a mobile POS, incorporated gift card sales or redemptions, or operate a loyalty program through which customers accrue points based on purchases, impact on these integrated elements need to be considered during any major system upgrade.

STEP 2: BEGIN WORKING WITH YOUR POS PARTNERS

It's important to remember that while the October 2015 liability shift represents a strong motivator, it's not a mandate for EMV readiness. (In contrast, PCI compliance is a mandate that merchants need to meet, at the risk of incurring significant penalties.) So while there's certainly no time to lose, retail and restaurant owners can establish a workable timetable for their EMV upgrade efforts that's in tune with their budget and bandwidth.

Consult with your POS software and hardware provider, ISV, VAR, credit card processor, and financial institutions to set up a timeline for action. Make sure the key players know your goals and where they fit into the overall picture and use your leverage to keep the various elements of the project on schedule. Remember, more communication is better than less when there are multiple "moving parts" to be coordinated.

In establishing your project budget, remember that net costs will include more than simply replacing or upgrading technology. There will be installation costs, as well as time and money spent integrating new applications with existing solutions. You may want to upgrade your data connection at various stores to support faster, more reliable transactions. Deployment, testing, and training will also need to be accounted for.

Many forward-thinking merchants are taking this opportunity to future-proof their POS solutions. EMV cards equipped with embedded antennas will work with contactless payment terminals, and the specifications also cover mobile payments, such as those leveraging Near Field Communication (NFC) integrated into many smartphones.

These options offer faster transaction speeds, along with more opportunities to provide coupons and integrate with loyalty programs, so EMV-capable systems equipped with these options can prepare your business for the future of payments.

In addition, if you've been considering alternate payment methods (e.g. gift cards or private label credit cards), these capabilities can be easily included in your upgrade plans. Offering more payment options and building customer loyalty can help grow your business, defraying some of the costs of EMV compliance for retailers and restaurant owners.

STEP 3: IMPLEMENT AND DEPLOY YOUR NEW SOLUTION

As you move into the implementation phase of your EMV upgrade, pay close attention to how the customer-facing aspects of transactions will change. Part of the increased security associated with chip cards is that they can require an additional form of user identification, such as a PIN or signature. As noted, these cards are "dipped" into a reader rather than "swiped" as magstripe cards are, so you may need to invest in more PIN/signature capture devices. Another option is to invest in mobile devices, such as those that allow for tableside transactions at restaurants or perform "line-busting" operations at retail stores.

Payment terminals offering all-in-one support for EMV-compatible hardware and peripherals are also a strong option, providing flexibility as payment technologies and processes continue to change. Key considerations include:

> Transaction times: How long does a credit card transaction currently take versus a debit transaction? Credit requires a pen for the customer and for some merchants, a stapler, both of which tend to slow down payment processes. When credit becomes PIN-based, as debit is, will this increase throughput? Will it change cashier requirements during peak times?
>
> Transactions not affected by EMV, e.g. refunds
>
> Processing transactions during power outages or other "POS down" scenarios

The next step is to test your decisions and certify the results. Work closely with your POS technology and financial partners to ensure your systems are in compliance and will all work together. Remember that in addition to EMV capability, all systems must also pass PCI certification as well. If you operate a chain, conduct a pilot in one location (or at one POS station within your store/restaurant) to field test how EMV acceptance will work in real-world conditions.

You should already have been developing new training materials prior to your field test, but use the results to refine them further. Make sure to document all aspects of handling an EMV transaction (i.e., what to do when a customer doesn't remember his/her PIN). Remember that with staff turnover, these new processes and customer interactions will need to become an integrated part of cashier and manager training going forward. Take this opportunity to review all your POS-related training materials to ensure they are up to date and easy to understand.

Conclusion

EMV is a fast-approaching reality for U.S. retailers and restaurant owners. The security protections built into chip cards and the payment infrastructure that supports them should have a significant impact on reducing fraud levels and deterring cybercriminals – a benefit for both merchants and consumers. Investments in bringing your POS solutions into alignment with EMV standards also present an opportunity to future-proof your payment offerings, preparing for advanced options such as mobile payments and business-building tools such as loyalty programs.

Finally, with the October 2015 liability shift, merchants have a vested interest in ensuring their payment systems are at least as secure as their competitors'. Being the "weakest link" puts both your business and your customers at risk – risks that can be avoided with careful planning, deployment and testing, in close cooperation of your POS partners.

Additional Resources

EMVCo: http://www.emvco.com

PCI Security Standards Council: http://www.pcisecuritystandards.org

That's EMV: http://www.thatsemv.com

American Express: https://www209.americanexpress.com/merchant/services/en_US/data-security

Discover Financial Services: http://www.discovernetwork.com/merchants/fraud-protection

JCB International: http://partner.jcbcard.com/security/jcbprogram/index.html

MasterCard: http://www.mastercard.com/sdp

Visa Inc: http://www.visa.com/cisp

Visa Europe: http://www.visaeurope.com/ais

About Bematech

For three decades Bematech has been a leader in producing solutions that redefine consumer experience at the Point-of-Sale, enhancing restaurateurs and retailers' businesses. The company offers a broad portfolio of integrated solutions – equipment, management systems, services and training – and specializes in serving small and mid-sized businesses through a wide distribution network that covers over 415,000 points of sale in 37 countries. The company operates four R&D excellence centers, with over 1,500 professionals in Brazil, China, Taiwan, USA and Argentina. For additional information, visit www.bematechus.com.

Contact Us

Bematech
999 S. Oyster Bay Road
Building 104
Bethpage, NY 11714

Phone: 1.516.248.0400
Email: sales@bematechus.com
Facebook: /bematechintl
Twitter: @bematechintl

bematech
Intelligence for business.

www.bematechus.com