TSYS® People-Centered Payments

White Paper

EMV: Preparing for Changes to the Retail Payment Process

A forthcoming shift in the liability for card-present fraud—and changes to the customer-facing payment process—require the attention of merchants and acquirers.

Executive Summary

The U.S. is the lone major commercial holdout in the global migration to the EMV (Europay, MasterCard, and Visa) standard for secure payments. As a direct result, card present fraud has migrated here en masse. Thus, on the heels of successful EMV rollouts and the resulting documented fraud mitigation in Europe, Canada and several other countries, the major card brands have provided an impetus for U.S. merchants and merchant acquirers to migrate to EMV. That impetus comes in the form of a shift in liability from issuers to acquirers and merchants beginning in 2015. As of October 1 of 2015, merchants and acquirers—not card issuers—will bear the financial burden resulting from fraudulent use of counterfeit, lost and stolen cards. It's a risk that's only mitigated by demonstration and documentation of EMV compliance.

Beyond the liability shift, EMV holds promise as an enabler of secure mobile and e-commerce payments, with attractive PCI (Payment Card Industry) Security Standards-related benefits for merchants. Those who implement EMV contact- and contactless-enabled POS devices may be excused from PCI audits and the costs associated with them, creating further incentive to adopt EMV. In this paper, we'll discuss the details behind the migration to EMV, how the technology works, and the changes merchants must prepare for at the point-of-sale (POS).

What Is EMV?

EMV is a globally accepted approach to payment security based on smart card technology. The contact/contactless EMV interface can be deployed in a card format that's not at all unlike the roughly 1.5 billion credit cards in U.S. circulation today, as well as in mobile electronic devices such as smartphones. For perspective on the global deployment of EMV cards, consider that worldwide deployment of the cards nearly equals the circulation of traditional credit cards in the U.S.

Where EMV cards differ from the standard magnetic stripe cards in service since the 1950s is in the mechanics of payment data transmission. The EMV standard calls for the adoption of smart cards, which contain a microprocessor that enables transactions to contain a cryptogram that is unique on every transaction. The cryptogram is validated by the issuer, making counterfeit cards virtually obsolete. In effect, the technology makes it extremely difficult, time-consuming, expensive—and therefore unprofitable—for fraudsters to attempt to break transaction cryptography and copy card information. In countries where card issuers have widely deployed EMV, the rampant counterfeiting of credit cards has been all but eliminated due to the near impossibility for criminal card counterfeiting and duplication of payment data. Countries that have not deployed EMV widely, such as the U.S., have become hotbeds of opportunity for credit card counterfeiters and fraudsters.

The EMV standards deployed around the globe were developed by EMVCo (www.emvco.com), a group that's jointly owned by American Express, JCB, MasterCard, Visa, and more recently, China Union Pay. These card brands have chosen EMV as the standard technology to help end credit card counterfeiting and improve cardholder security.

EMV technology also supports the mitigation of merchant risk via offline data authentication, which enables validation of the card for offline transactions. In this scenario, the personal identification number (PIN) entered by the consumer is compared to an encrypted, but matching PIN on the application stored within the card. Merchant acquirers and card issuers can set parameters around the number of transactions or purchase totals acceptable for offline transactions. The ability to securely accept cards when online communication is not possible amounts to a financial benefit to merchants and integrators.

Here in the U.S., the first major initiative toward EMV—stimulated by the migration of fraud to our inadequately protected card payments infrastructure—was announced by Visa in August 2011. That announcement outlined the high-level requirements for EMV card deployment and acceptance as follows:

- **Expand the Technology Innovation Program to Merchants in the U.S.**
  Effective October 1, 2012, Visa expanded its Technology Innovation Program (TIP) to the U.S. TIP eliminates the requirement for eligible merchants to annually validate their compliance with the PCI Data Security Standard for any year in which at least 75% of the merchant's Visa transactions originate from EMV chip-enabled terminals. To qualify, terminals must support both contact and contactless chip acceptance, including mobile contactless payments based on near field communication (NFC) technology. Contact chip-only or contactless-only terminals do not qualify for the U.S. program. Qualifying merchants must continue to protect sensitive data in their care by ensuring their systems do not store sensitive cardholder data and that they continue to adhere to the PCI DSS standards as applicable.

- **Build Processing Infrastructure for Chip Acceptance**
  Visa required U.S. acquirer processors and sub-processor service providers to be able to support merchant acceptance of chip transactions as of April 1, 2013. Chip acceptance requires service providers to carry and process additional data that is included in chip transactions, including the cryptographic message that makes each transaction unique.

- **Establish a Counterfeit Fraud Liability Shift**
  Visa intends to institute a U.S. liability shift for domestic and cross-border counterfeit card-present POS transactions, effective October 1, 2015. Fuel-selling merchants will have an additional two years, until October 1, 2017, before a liability shift takes effect for transactions generated from automated fuel dispensers. Currently, POS counterfeit fraud is absorbed by card issuers. With the liability shift, if a contact chip card is presented to a merchant who has not adopted contact chip terminals (at a minimum), liability for counterfeit fraud may shift to the merchant's acquirer. The liability shift encourages chip adoption, since any chip-on-chip transaction (chip card read by a chip terminal) provides the dynamic authentication data that protects all parties.

In January 2012, MasterCard followed suit with an endorsement of EMV (www.mastercard.us/mchip-emv.html) and a multiple-layer benefit plan for merchants who adopt the technology. Among other benefits, MasterCard's acquirer mandate for EMV includes breach and lost-stolen card protection for EMV-enabled merchants who are able to use PIN cardholder verification methods. The acquirer mandates adopted by Visa, American Express and Discover also include various levels of protection for EMV-equipped merchants.

Preparing for EMV in the Store

For merchants, preparation for the transition to EMV begins with hardware infrastructure and physical card payment processes. EMV cards feature magnetic stripes and can indeed be swiped through traditional non-EMV terminals. However, when a consumer swipes an EMV card at an EMV-enabled payment terminal, the terminal will prompt the consumer to insert the card into a slot, where a metal contact on the face of the cards facilitates data communication with the reader. In contactless environments, the internal chip in the card (or mobile device) communicates with the reader via NFC.

This change requires multiple levels of device and software compliance testing with each card brand on the part of the acquirer or acquirer processor to ensure that the chip on the card and the terminal application interact as expected under card brand regulations and requirements. Because EMV card acceptance requires a different interface than

legacy card reader equipment, merchants outfitting or retrofitting locations with EMV terminals should seek assurance from their hardware providers that the terminals they're implementing have passed EMV Level 1, Level 2 and application certification. Currently, nearly all European payment devices and more than 70% of global payment devices in service are EMV-enabled, but U.S. penetration remains well below those figures.

The EMV combination of chip and PIN technology is widely preferred for security purposes, but it creates another deployment consideration for acquirers and plays into the purchase decision for merchants. Chip-and-PIN terminals with integrated PIN pads must usually be injected with keys to process online PIN-authenticated transactions. If the merchant's PIN pad terminals lack these keys and a consumer presents a card that requires a PIN, acceptance of the card requires the POS associate to manually key in the card's information.

These are among several important considerations that require thorough testing and systemic analysis in advance of rollout to ensure the migration to EMV doesn't encumber the transaction process, or burden the POS associate with the task of coaching consumers through new payment procedures.

Changes to the POS Configuration and Payment Process

Other key considerations in the assessment of hardware infrastructure are the physical space consumed by the payment device at the POS and the process by which consumers will engage the device. In high-volume environments, a consumer-facing EMV-enabled peripheral device—in addition to the associate-side payment terminal—might be the merchant's best choice. In lower-volume environments where transaction speed is of less concern, a single, pivoting payment terminal manipulated by customers and/or associates might prove effective.

In either case, the aforementioned EMV terminal software configuration and change management initiatives will go a long way toward a smooth rollout. Because the EMV payment process requires the consumer to insert the card after the merchant enters the transaction amount or when prompted—and leave the card in the terminal until prompted to remove it—a fair degree of coaching can be expected as necessary. The more automated the process via device prompts, the less likely the need for associate intervention.

E-Commerce and Mobile Transactions: Where Does EMV Fit In?

As retail e-commerce and mobile transaction volumes grow, some merchants have taken the position that holding out on new payment processing investments—in hopes of a single, secure acceptance technology that meets the card processing requirements of every channel or transaction scenario—is the prudent decision. Allen Friedman, Associate Director at TSYS Acquiring Solutions, disagrees. "The incredible financial toll that fraudulent card-present transactions exact on all parties in U.S. commerce, from consumers to merchants to card issuers, is one of the biggest problems the industry faces. It requires an immediate solution," he says. Friedman says that solution is the EMV standard, which is poised for adoption in the U.S. But, how will EMV technology affect mobile and e-commerce payments, if at all? Here's his take.

- **Friedman on EMV in a mobile payments environment:** "There are millions of mobile transactions taking place daily, but many of them are not what we consider retail card present transactions. Of the mobile payment solutions that are in the retail space, many are cumbersome, and many others can't be sustained because they aren't widely supported or applicable to multiple merchant environments. Large-scale adoption of many of the mobile payment solutions on the market today would require an even bigger change at the POS than EMV, with some solutions adding seconds to transaction and wait times. EMV comes into play because it works well with NFC contactless technology initiated from a phone or a card."
- **Friedman on EMV in e-commerce:** "Visa and MasterCard have developed methods for EMV to support e-commerce transactions, (MasterCard's Chip Authentication Program (CAP), and Visa's Dynamic Passcode Authentication (DPA)). While not yet widely in use, leading-edge adopters of EMV in Europe are already exploring the use of these EMV technologies for e-commerce transactions. With that said, we should not defer using existing technology to address one source of fraud until we can address them all. For the U.S. in the near term, payment security begins with cutting card present fraud as much as possible using the tools at our disposal, and EMV is the best tool we have to do so. Then we can address variants of EMV, or other secure technologies, for mobile contactless and e-commerce transactions."

Conclusion: Collaboration is Required Among Merchants, Acquirers and Integrators

Merchants should work closely with their payment acceptance and technology integration partners to determine the most effective and cost-efficient approach to the new configuration and to develop a systemic approach to the actual rollout. Because EMV cards are able to support so many payment variables and configurations, integrators will play a pivotal role in the merchant's ability to customize an EMV environment that streamlines consumer interaction with the card's expanded and more secure credit and debit functionality.

TO LEARN MORE

+1.480.333.7799 or acq-sales@tsys.com. You can also visit us at www.tsysacquiring.com.

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTH ASIA	JAPAN	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+81 3 6418 3420	+971 (4) 391 2823	+1.706.649.2307	+55.11.3504 6600