The State of EMV:
Pushing Towards EMV Implementation in the U.S.

HARLAND CLARKE® | PAYMENT SOLUTIONS

As Europay®, Mastercard® and Visa® specifications were adopted in many global markets, fraud became less of a problem and paved the way for emerging technologies. Despite all the improvements that EMV offers, why hasn't it been fully embraced in the U.S.?

The Push Towards EMV Implementation in the U.S.

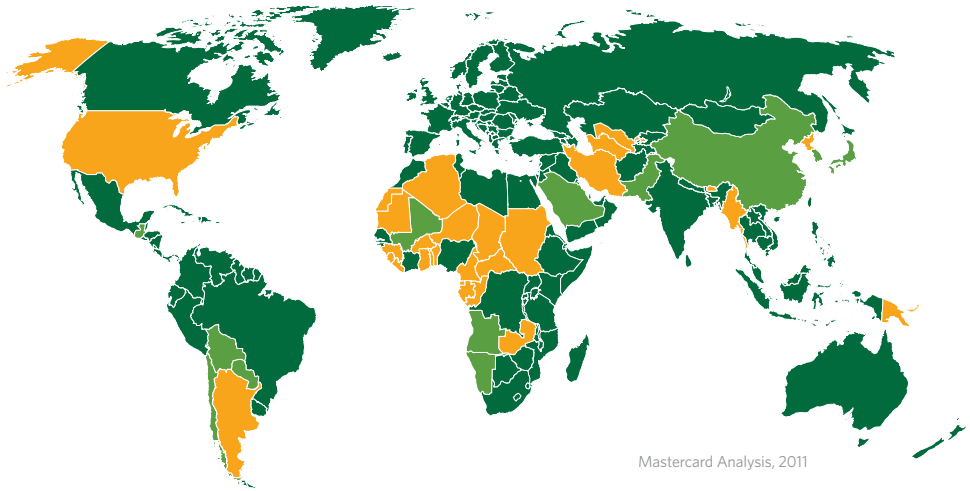
EMV is a global, open-standard set of specifications for smart cards and compatible acceptance devices (ATMs, merchant terminals, etc.). Originally developed by Europay, MasterCard and Visa (hence the acronym EMV), the EMV specifications define requirements to ensure interoperability between chip-based payment cards and terminals that authenticate credit and debit card transactions. EMV chip cards contain embedded microprocessors that offer greater transaction security — and other capabilities — than the magnetic stripe card technology used in the U.S. Other benefits of EMV include 1) guaranteed payment interoperability between countries and; 2) payment innovation – EMV is seen as a gateway to emerging technologies like mobile payments. So, despite all the improvements that EMV offers, why hasn't the U.S. fully embraced the technology?

Why the U.S. Has Been Slow to Adopt EMV

The U.S. is one of the last major markets to adopt EMV technology. EMV has already been deployed in Europe, Asia and Canada. More than 1.3 billion EMV cards and 20.7 million EMV acceptance terminals have been deployed worldwide as of September 2011[1]. There are several reasons why the U.S. has not yet adopted the technology.

The most important reason has to do with payment infrastructures. Chip cards were first tested in the mid-1980s and were fully deployed by French banks by 1994. When markets outside the U.S. developed their payments infrastructures, chip technology was already available. Chip technology works for both the smart cards of the past and today's EMV chips, so the infrastructures were ready for and easily accommodative of EMV chips. In contrast, the U.S. payment infrastructure was developed around magnetic stripe technology – which has served the industry well, being both reliable and inexpensive to operate.

EMV adoption rates, 2011



Mastercard Analysis, 2011

- Countries with no preparation to migrate
- Countries where one or more banks are migrating/have migrated to EMV chip
- Countries where MasterCard-branded EMV, POS or EMV ATMs penetration exceeds 50%

Canada
- 67% of cards, 75% of POS and 40%+ of ATMs EMV chip enabled as of 2011
- Introduced domestic liability shift in 2011

Europe
- 70% of cards EMV chip enabled
- 90% of POS EMV chip enabled
- 90% of ATMS EMV chip enabled
- January 2011 EU regulators migration mandate for SEPA countries

Asia-Pacific
- 30% penetration of cards
- Almost 50%+ penetration of POS devices
- As of 2011, ATM migration to EMV chip underway; domestic migration mandates in Malaysia, Korea and Indonesia; dual interface (PayPass M/Chip across key markets)

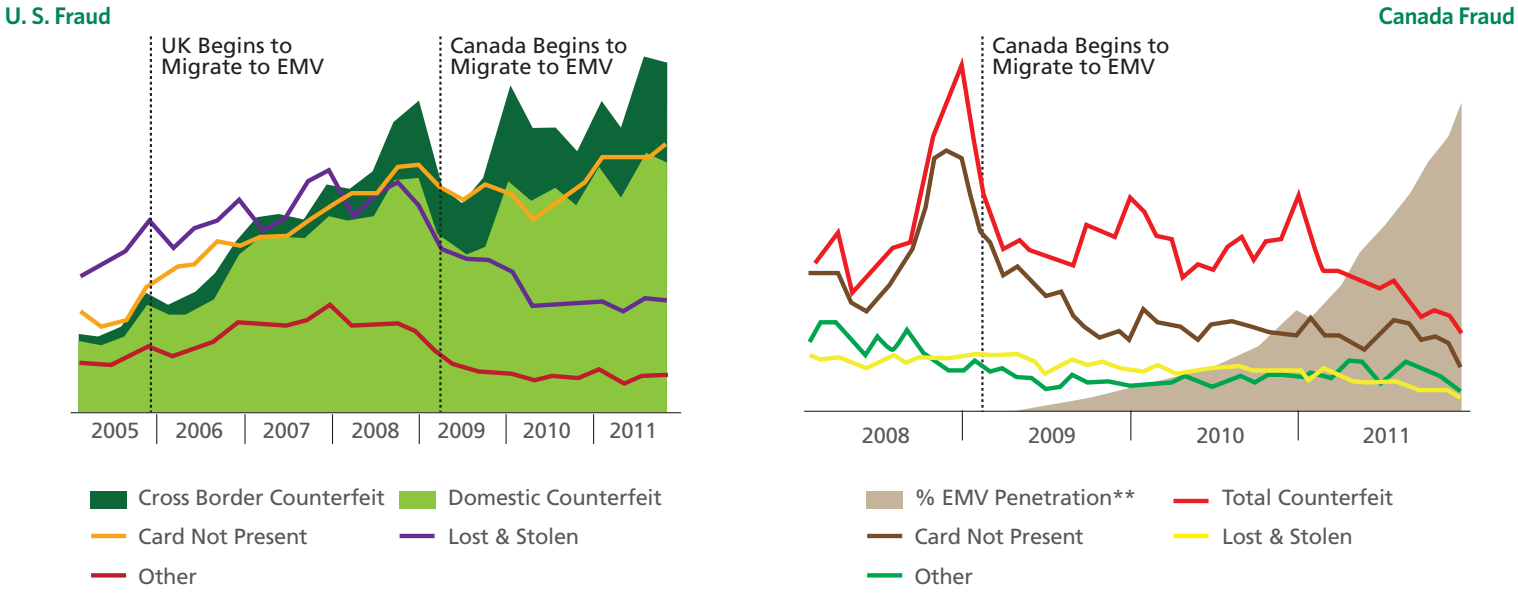
Latin America/Caribbean
- 80%+ acceptance EMV chip enabled
- Brazil, Mexico, Peru, Venezuela and Columbia most advanced
- Heavy regional EMV chip migration (Venezuela, Central America and Caribbean)

Middle East & Africa
- Twelve key markets with EMV chip penetration on POS above 80%; 75%+ penetration across region
- Sharp rises in EMV chip card issuance in key markets (e.g. South Africa)
- Domestic migration in Qatar and Bahrain

[1]EMVCo, Q3 2011

Now, fraud considerations are the impetus for change. As global markets adopted EMV technology, fraud became less of a problem in those markets.

Card Fraud Declines in Canada after EMV Implementation



Mastercard Analysis, 2012
** % face-to-face EMV penetration

Card fraud usually migrates to the weakest points in the payments chain, which leaves U.S. merchants, issuers and financial institutions that have not implemented EMV vulnerable.

The U.S.-based card associations, Mastercard, American Express, Discover and Visa weighed the low cost of processing magnetic stripe card transactions against the high costs of increased fraud. They couldn't mandate a change in payments systems, but they could establish incentives to change. One of the incentives is a shift of liability away from adopters of EMV technology and towards non-adopters. The liability shift means that the entity not supporting an EMV transaction (be it the merchant or issuer/financial institution) becomes liable for fraud incurred on a transaction.

"For many institutions, the liability shift is driving the timeframe."
Nicole Machado, Harland Clarke, Director of Card Services

Key Dates for Liability Shifts

In the U.S., there are several key dates related to the liability shift. For 2013, processors should be able to support American Express EMV transactions, while both processors and merchants should be EMV-certified for Discover. In 2014, merchant acquirers and processors should be EMV-certified for Mastercard. By October 2015, all financial brands (Mastercard, Visa, American Express and Discover) will enforce a liability shift to issuers. In October 2017, the liability shift will be enforced for automated fuel dispensers (AFD). Financial institutions are busily preparing for the October 2015 deadline.

Financial Institutions Vary in EMV Knowledge

A May 2013 Harland Clarke survey shows that 74 percent of clients have begun researching EMV. Financial institution respondents had consulted their card associations, EFT processors and card issuers as primary information sources. Card association questionnaires, which help determine an institution's fraud risk and technology needs, were a useful starting point for many respondents. Most remain hungry for information – 30 percent say they are "somewhat unknowledgeable" of EMV and another 17 percent indicated they "don't know where to begin."[2]

Nicole Machado, director of card services for Harland Clarke, encourages institutions to engage their card associations, EFT processors, card issuers and card manufacturers so they can understand their software platforms, their chip options and the programming necessary for EMV implementation. "This is the homework to do now. Once financial institutions have scoped out the requirements, they will be positioned to implement," she said.

How EMV Works

EMV uses a secure chip embedded in the plastic payment card issued to a consumer. The chip provides three key elements related to secure payments:

- Storing cardholder account information
- Processing a transaction
- Performing cryptographic processing of stored account holder information

To execute a transaction, the chip connects to a chip reader at an ATM or merchant terminal. The physical connection can be made on either a contact or contactless basis.[3]

Chip options include "EMV-only," meaning each card has a chip used for terminals with contact interfaces, but the card cannot be used for contactless transactions. Another option is "dual interface," which means the card contains both a microchip for contact interfaces and an RFID (radio frequency identification) contact list antenna for contactless transactions. Dual interface requires a more expensive card, but establishes the gateway to emerging technologies, including mobile.

Greg Kuyava, senior product manager of card services at Harland Clarke, said different chips run on different platforms. After choosing a chip that meets its needs, an institution should work closely with its card association to outline program parameters – specific instructions about how payment transactions will be processed across a range of scenarios. "Once these requirements have been met, an institution can begin to identify its conversion and programming costs for moving from a magnetic stripe-only card portfolio to an EMV card portfolio," said Kuyava.

[2] *Harland Clarke, Financial Institutions Grapple with Costs and Look for Guidance, 2013*
[3] EMVCo, A Guide to EMV (May 2011)

Timely Employee and Card Holder Communication Important

Last but not least, institutions need to develop multi-channel communications strategies to explain to employees and customers the benefits of EMV conversion. Institutions should plan to educate employees in the six months leading to EMV conversion. "Electronic communications are ideal for introducing what EMV is, how the transition will work and over what time frame," said Kuyava. Early training prepares employees to help explain details of the conversion process to customers. Cardholder communications should begin several months ahead of an institution's EMV conversion and continue throughout the conversion process. A strong communications effort should include all customer touch points — including online and contact center support — and help spur card usage.

"Electronic communications are ideal for introducing what EMV is, how the transition will work and over what timeframe,"
Greg Kuyava, Harland Clarke,
Product Manager of Card Services

For more information on how Harland Clarke can assist with your card services needs, including expertise on making a smooth transition to EMV, please contact us at **1.800.277.7637** or visit **harlandclarke.com/Cards**