A CHIP ON THE

If you accept credit/ debit cards, the world is about to change. Here's what you need to know to stay ahead.

By Tom Wunk, CAPP

OLD CARD

Now what? This seems to be the prevailing response when I bring up the subject of open-standard Europay, MasterCard, and Visa (EMV) credit card processing with parking operations folks. Like many industries, parking is slowly emerging from economic malaise and finally seeing some light at the end of the tunnel. In addition, operations are battle-weary and scarred from last year's payment card industry (PCI) standards saga (see the June 2012 issue of *The Parking Professional*). Between money and time invested and ongoing compliance action items, management and support professionals have had their fill of credit card processing requirements.

Just when you thought it was safe to go outside, along comes EMV.

What is EMV?

Simply stated, EMV is a global open standard for smart card (chip card) payment credentials, acceptance devices (terminals), and the associated transactional processing. In 1994 and 1995, a consortium was formed in Europe to examine the issue of credit card fraud and how technology could help address it in a large-scale manner. This consortium, formed between Europay, MasterCard, and Visa, developed a global standard for the interoperability of credit and debit cards, along with terminals based on chip-card technology. The first formal EMV specification was issued in 1996. Today, EMVCo—jointly owned by American Express, MasterCard, Visa, and JCB (formerly Japan Credit Bureau)—manages EMV specifications, enhancements and associated developments, and most importantly, the associated testing and evaluation protocols.

It is important to note that the while the intent of addressing fraud was primarily focused on credit card payment transaction processes, the entire payments ecosystem, including debit card and ATM transactions, was examined.

How Does it Work?

The initial idea behind EMV was to install some type of intelligent component in a card that could not be copied or transferred and used for unauthorized activity. The advent of paper-thin microchips made card-embedded microprocessors and associated applications possible. This could provide very strong transactional security through dynamic encryption. Traditional magnetic stripes contain static data, which can be stolen or copied and re-used for other transactions. With dynamic authentication, the data exchanged between card and reader changes with every transaction, so even if a transaction was hijacked, it could not be replicated for additional transactions.

An EMV-enabled credit card will include a gold square on the front of the card. This is known as the card's contact. Behind this contact is the card's microprocessor, as illustrated below.

When the card is inserted into a terminal, the gold contact allows a connection between the card and the terminal's reader. This connection to be established enables two processes to occur: the connection provides power to the chip, and once power is applied, data is exchanged between the card and the reader. This type of transaction is a contact transaction. It is important to note that contact readers can be fully manual and require the cardholder to dip and retract his card at the machine, or the reader can be motorized, ingesting and then expelling the card.

Another transaction type, known as a contactless transaction, occurs when a contactless chip-based credit card is held within a couple of inches of the reader. Here, data is exchanged via radio frequency.

Is That All?

Not quite. EMV specifications are very thorough in describing the requirements for proper EMV transactional processes. This overall transaction process addressed by EMV is broken into three primary components:

- Card authorization is the securing and associated protection of the card itself to protect against copying card information and re-creating that information for fraudulent activity. This is primarily handled by the card manufacturers.
- Transaction authorization describes the parameters set to ensure the sanctity of the transaction authorization sent to and returned from the issuer in an online transaction. If offline transaction capability is needed, the actual point of sale (POS) terminal can be configured to accept the transaction based on the card authentication and the associated transaction cryptogram.
- Cardholder verification is used to confirm the actual card ownership component—is this person the rightful owner of the card?—which combats the issue of lost or stolen credit cards. This process is referred to as CVM; EMV supports four types of CVMs:
  - The first method requires the cardholder input a specific PIN (personal identification number). The PIN is verified online by the associated card issuer and the transaction can proceed.
  - The second type of CVM method combines a chip-based credit card with a terminal that's capable of offline transactions. When the cardholder presents a card, he or she is then instructed to input a PIN. Once this is done, the terminal itself will interrogate the card chip to verify if the PIN is correct. It they match, the transaction proceeds.
  - The third type of CVM method is signature verification and signature collection. The terminal itself has signature capture area for the cardholder to enter his or her signature. This uses a manual process of verification as a supplement to card authorization.
  - The fourth type of CVM is no CVM; the card is used as the sole method of transactional identification. This his primarily been identified as the methodology for transactions at unattended POS locations, low-dollar transaction locations, or those transactions with high volume throughput situations.

CVM is of utmost importance to the transportation industry. The determination of CVM will significantly affect the scope of implementing EMV. For example, if your business model incorporates both pay-on-foot machines and exit verifiers that accept credit card payments and you and your bank and processor have determined that CVM will include PIN entry, new terminals will have to be incorporated into those devices. This will be a significant and expensive proposition.

What's the Timeline?

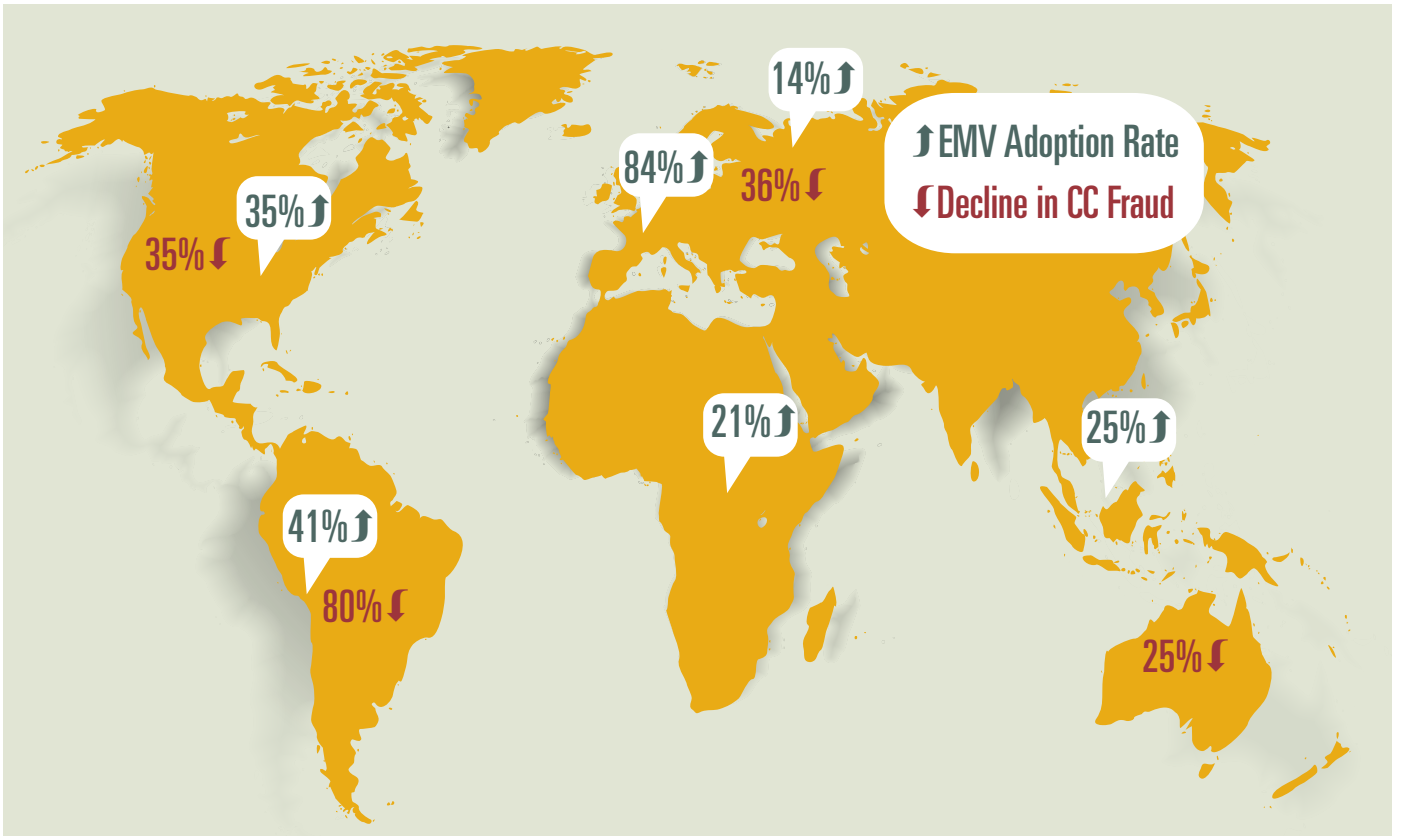
The U.S. is one of the last countries to adopt EMV into its credit card processing infrastructure. But as with PCI, the major card brands are pushing the matter. Visa took the lead by announcing a number of EMV deployment milestones in August 2011. MasterCard followed in January 2012, Discover in March 2012, and American Express in June 2012. The primary milestone categories are as follows:

- PCI audit relief. This is the advertised date by which, if more than 75 percent of transactions originate from EMV-compliant POS terminals, the merchant may apply for relief on the audit requirement for PCI compliance. However, the merchant must maintain all other PCI compliance components.
- PCI account data compromise relief. Driven by MasterCard, merchants are relieved of all or a portion of associated penalties for account data compromise (hacking) if the indicated percentage level of transactions originate from EMV-compliant terminals. If at least 75 percent of transactions originate from EMV-compliant terminals, the merchant is relieved of 50 percent of account data compromise penalties. If at least 95 percent of transactions originate from EMV-compliant terminals, the merchant is relieved of 100 percent of account data compromise penalties.
- Acquirer/sub-processor compliance. This is the advertised date by which acquirers and sub-processors must be able to process full chip data from card transactions for authorizations and for some payment brands, transaction clearing, and settlement.
- Counterfeit liability shift. This is the advertised date by which an associated infrastructure party in the credit card process chain that has invested in EMV deployment is protected from financial liability for card-present counterfeit fraud losses. If none of the process chain parties is EMV compliant, fraud liability will remain as it is today.
- ATM counterfeit liability shift. This is the advertised date that the MasterCard liability hierarchy takes effect for ATM transactions.
- Lost or stolen liability shift. This is the advertised date that the MasterCard liability hierarchy takes effect for lost/stolen cards. The party that has the made the investment in the most secure EMV deployment option is protected for financial liability for card-present fraud losses for lost, stolen, or non-receipt fraud.

EMV Deployment Milestone	Key Dates	Visa	MasterCard	Discover	American Express
PCI Audit Relief	October 2012 October 2013	Y	Y	tba	N Y
PCI Account Data Compromise Relief 75 percent 95 percent	October 2013 October 2015	N N	Y Y	tba tba	N N
Acquirer / sub-processor compliance	April 2012	Y	Y	Y	Y
Counterfeit Liability Shift (except fuel dispensers)	October 2015	Y	Y	tba	Y
ATM Counterfeit liability shift	April 2013 October 2016	N N	Y—Maestro Y—all MasterCard branded products	tba tba	N N
Lost or Stolen Liability Shift	October 2015	N	Y	tba	N
Counterfeit Liability Shift for Automated Fuel Dispensers	October 2017	Y	Y	tba	Y
Lost or Stolen Liability Shift for Automated Fuel Dispensers	October 2017	N	Y	tba	N

Is This Really Happening?

I believe so. While the timing and the actual deployment steps may change, it is hard to dispute the overall results of EMV deployment. There is a distinct association between the implementation and adoption of EMV and the associated reduction in credit card fraud as the following shows:



HOW EMV REDUCES FRAUD

As the number of countries that have not adopted EMV continues to shrink, so the does the associated target-rich environment for potential fraudulent activity. Think about the following information released in November 2011:

CARPENTERIA, Calif.—(BUSINESS WIRE)—The U.S. currently accounts for 47 percent of global credit and debit card fraud even though it generates only 27 percent of the total volume of purchases and cash, according to "Global Card Fraud," from a recent issue of The Nilson Report, a respected trade newsletter on the payments industry.

SOURCE – NILSON REPORT

And from the BBC in January 2013:
U.S. is main source of EU credit card fraud.

SOURCE - EUROPOL

Data breaches in the US account for most of the credit card fraud affecting the EU, a new police report says.
Criminal gangs are making about 1.5 billion euros (£1.2bn; $2bn) annually from such fraud, the EU police agency Europol says, regretting that compliance with new security features remains patchy.

In 2011 nearly all fraud involving EU cards took place outside the EU. Chip-and-PIN security used in the EU is not yet global, Europol notes.

Such fraud cases overseas have risen.
Besides the U.S., the fraud networks are also very active in Brazil, Colombia, the Dominican Republic, Mexico, and Russia, Europol says.

"So far most of the credit card numbers misused in the EU have come from data breaches in the U.S.," Europol says, adding that most illegal face-to-face card transactions with EU-issued cards also happened in the U.S.

Consider the actual cases of credit card fraud and relate that to the areas of the world that have adopted EMV:

The U.S. is one of the last countries to adopt EMV into its credit card processing infrastructure. But as with PCI, the major card brands are pushing the matter.

What About NFC?

When discussions ensue with regard to the evolution of payments, you will hear of EMV and near-field communications (NFC), which are sometimes thought to be synonymous. The truth is, they are distinct in nature but can complement each other. We've discussed EMV as a technological advance in the credit card transactional process. NFC is a set of standards for mobile devices that enables them to establish wireless communication by touching two elements together or being in close proximity. In general, there are three modes of NFC operation:

- Reader to device mode. In this mode, the reader will activate a passive device and then the device will transmit data back to the reader. The device can be in the form of a card, key fob, or other device that does not require batteries.
- Peer to peer mode. This mode allows two NFC devices to communicate with each other when they are touched or are in close proximity.
- Card emulation mode. This by the far the most anticipated deployment of NFC technology. This mode allows an NFC-enabled device to emulate a contactless smartcard, which could be in the form of a credit card, alternative payment credential, access control card, special program card, transit card, or any combination thereof. Both Google Wallet and ISIS wallet avail themselves of this technology.

What Should I Do?

Credit card processing is an integral part of the parking and transportation industry. Usage can run from a low of 30 percent to a high of 95 percent of all payment transactions. Facilities and operations are embracing full-on cashless payment practices. The world is embracing enhanced fraud protection via EMV. Society in general is shifting the payments infrastructure with the rampage of smartphone usage. Consider the following:

- 56 percent of American adults are now smartphone owners. (Source: Pew Internet & American Life Project, 2013)
- Within five years, half of today's smartphone users will be using mobile wallets as their preferred payment method. (Source: Carlisle & Gallagher Consulting Group, 2012)
- Need proof we're addicted? Seventy-five percent of Americans take their phones to the bathroom. (Source: Digiday, 2013)

It is imperative that transportation ecosystems managers remain patiently vigilant with regard to EMV. The deadlines indicated above are real and at this point in time, remain as indicated. Keep appraised of updates relating to EMV. Meet with your operations staff, finance experts, and technical solutions providers. Confirm they are also vigilant and that they are exploring deployable options. Gather potential costs and consider those costs in budget discussions. Contact your bank and processor to determine their position with regard to EMV and how they plan to address the indicated milestones. Become and remain informed. It will enable you to make informed decisions and not be caught off guard. Ultimately it will be to your credit.

TOM WUNK, CAPP, is vice president of PARCS with T2 Systems, Inc. He can be reached at twunk@T2systems.com or 317.524.7425.