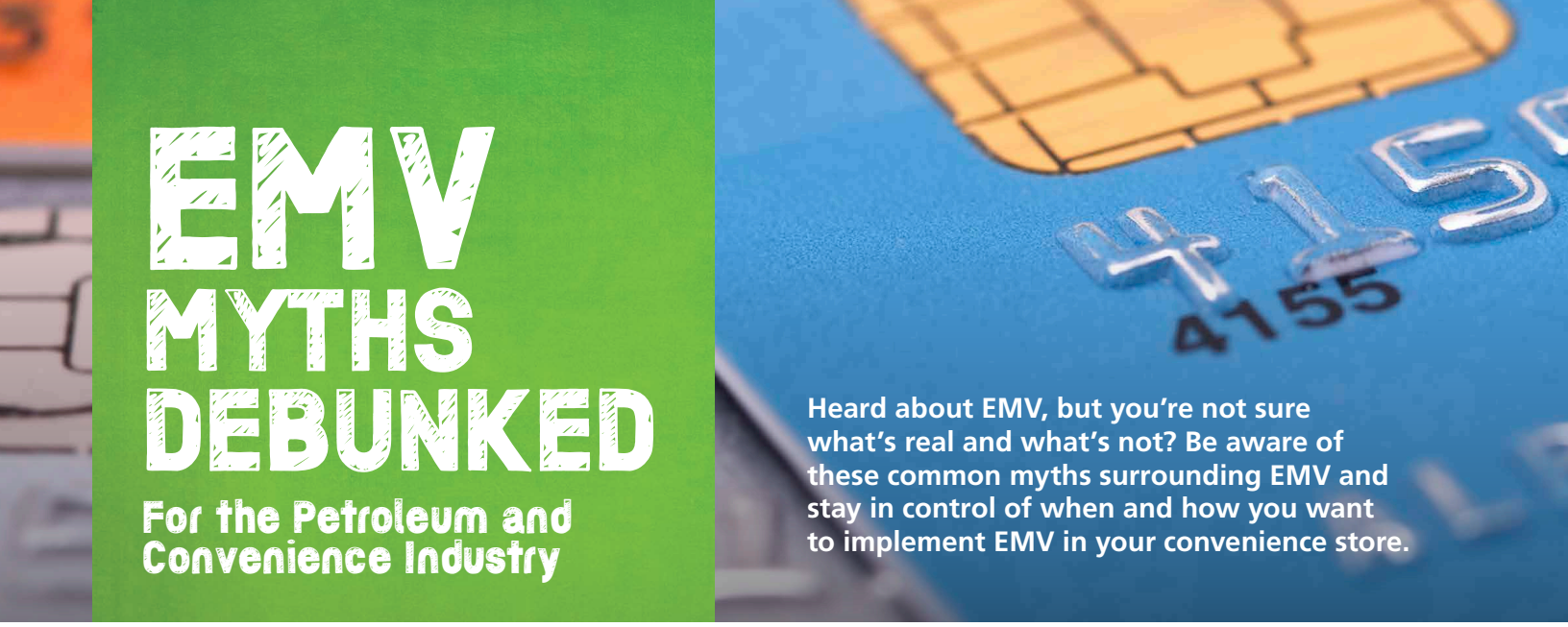
EMV MYTHS DEBUNKED

For the Petroleum and Convenience Industry



Heard about EMV, but you're not sure what's real and what's not? Be aware of these common myths surrounding EMV and stay in control of when and how you want to implement EMV in your convenience store.

On October 1, 2015, a liability shift is occurring as it relates to who is responsible for paying for chargebacks for counterfeit cards that are used at a convenience store. Between the bank that issued the credit card, the convenience store and the payment processor, whoever is least prepared to accept EMV-enabled payment cards will now be responsible to pay for the chargebacks.

Myth #1: Implementing EMV in your convenience store is required and will be enforced by a government regulation or security council.

If you are a U.S. convenience store operator, no government agency or industry association is requiring you to implement EMV. You will not be fined if you do not implement EMV by the often referred to "deadline date" of October 1, 2015. This is not a deadline. It is your decision whether or not you want to implement EMV – there is no requirement.

Myth #2: EMV is a requirement for complying with PCI Data Security Standards.

You don't need to implement EMV in order to be compliant with PCI Data Security Standards. While EMV can be one component of your data security strategy, it is not required nor mandated by PCI Data Security Standards, nor will implementing EMV make you PCI compliant.

Myth #3: Once you implement EMV, you will no longer be able to accept credit cards with magnetic stripes.

Believe it or not, magnetic stripes on credit cards are going to be with us for quite some time. If you're EMV-ready, when a customer pays with an older magnetic stripe credit card you'll simply swipe it through your new payment terminal's card reader. So regardless of whether or not you have implemented EMV, you'll be able to take all credit cards in your convenience store.

Myth #4: EMV protects your convenience store from a data security breach.

Remember – implementing EMV alone will not protect your convenience store from being hacked. While EMV helps protect you from counterfeit card use, it's not the end-all, be-all of convenience store data security. There are measures that you can put into place that are not provided by EMV – such as encrypting credit card data as it passes through your network – that will safeguard your convenience store from a data breach as well as give you greater peace-of-mind.

For more information, visit www.ncr.com, or email sales.pcr@ncr.com.

NCR

Myth #5: EMV will rapidly achieve mass adoption by both credit card issuers and other convenience stores.

Estimates are that only 20 to 30 percent of cardholders in the United States will have new EMV-ready cards by October 1, 2015. Meanwhile, industry experts are saying that it will take at least 3-5 years in order for EMV to reach full acceptance in the U.S., and in Europe the adoption took much longer. So know that it's going to take a while for everyone to finally make the transition to EMV.

Myth #6: If you don't implement EMV, you won't be able to accept credit cards after October 1, 2015.

Even if you don't implement EMV-enabled payment devices by October 1, your business will still run the same as it did on September 30, aside from the liability shift. Both older magnetic stripe cards and newer EMV cards can be accepted by non-EMV merchants, as the new chip cards will also have magnetic stripes available for that very reason.

Myth #7: Transitioning to EMV is as simple as plugging in a new payment terminal.

Making your convenience store EMV-ready can involve lots of discussions, questions and planning about many different things: your POS system, your payment processor and the right kind of payment terminal devices. It's also crucial that you understand the impact that EMV technology will have on your operation; be prepared to train your staff appropriately and assist customers with using their EMV credit cards.

Myth #8: The liability shift for Petroleum Convenience Sites is really in 2017.

Unfortunately, the liability shift for Petroleum and Convenience Retail is split into two dates. Transactions performed at POS terminals, tablets, kiosks or car wash tunnels will incur the liability shift in 2015 while pay-at-pump transactions performed at the dispenser will incur the liability shift in 2017. If you chose to defer your EMV implementation until 2017, you will incur the liability for any fraudulent transactions using an EMV capable card that take place in POS terminals between October 2015 and when your EMV solution is deployed.

Myth #9: EMV provides P2P capabilities.

EMV and Point-to-Point Encryption (P2P) are two separate technologies that address different security concerns and require independent implementations. EMV focuses on securing credit card counterfeit fraud while P2P focuses on securing track and account information in store systems. EMV transactions without P2P will expose track equivalent data and account information in the clear to payment applications. As a merchant you must decide if you want to implement P2P capabilities in addition to EMV and confirm that both your host and pin-pad provider support a common encryption scheme required for implementation.

Myth #10: If you don't implement EMV you are liable for all fraudulent electronic transactions.

If you don't implement EMV, the merchant does not automatically incur liability for all fraudulent electronic transactions. The liability shift applies to whomever is not able to process EMV transactions. If the issuer does not provide EMV capable cards or the acquirer is unable to process EMV transactions the liability will apply to them instead of the merchant. For the liability to shift to the merchant, an EMV card must be processed at the site by an acquirer that supports EMV transactions on a payment terminal that does not support EMV.

Myth #11: Debit cards cannot be processed unless US Common AID (US Debit) is implemented.

To comply with Durban's routing requirements, debit cards for the US market will include two or more AIDs. The cards will include Global AIDs that will enable cards to be processed with the card brand (e.g. Visa, MC, Amex, Discover) and US Common AIDs that will enable cards to be routed to the merchant's debit network or choice. Until support for the US Common AID is implemented, POS systems may process these cards using the Global AID that is specific to a single processor. This will still allow cards to be processed, but will not enable cards to be routed to the merchant's processor of choice. Further, in most cases the Global AID will result in the cards being processed as Credit transactions, which will restrict the ability to offer cash back or fuel using debit specific pricing.

We can help you separate the fact from fiction in order to make the right decisions for your convenience store. Let us know if you have any questions or need further information about EMV at sales.pcr@ncr.com or 1.800.439.6582.

© 2015 NCR Corporation Patents Pending www.ncr.com 15RET2886-0415