EMV Talking Points

EMV stands for Europay, Mastercard and Visa and is the global standard for credit cards with encrypted chips rather than magnetic stripes.

What is EMVCo, and what is its role?

EMVCo, LLC, was formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV™ Specifications for Payment Systems.

EMVCo's primary role is to manage, maintain and enhance the EMV Specifications with the objective of ensuring interoperability and acceptance of EMV based payments on a worldwide basis. EMVCo has expended it's scope from EMV Chip specifications to include EMV tokenisation specifications as of January 2014.

EMVCo is also responsible for type approval processes, which presently include EMV Chip terminal compliance testing, as well as Common Core Definitions (CCD) and Common Payment Application (CPA) card compliance testing. These EMV Chip testing processes ensure a single terminal and card approval at a level that will allow cross payment system interoperability through compliance with the EMV Chip specifications.

EMVco is owned and operated by VISA, MC, Discover, JCB, American Express, and Union Pay

EMV is NOT mandated or required - it is the merchant's choice to implement.

EMV is just a liability shift - effective October 2015. **Liability Shift = Potential Chargebacks**

EMV does NOT protect against all chargebacks - the liability shift is for counterfeit and lost/stolen cards only.

EMV does not protect or encrypt credit cards.

EMV is not PCI DSS compliance - EMV protects against fraud, PCI focuses on data security.

Chip and PIN? or Chip and Signature - there is no industry standard yet. If a restaurant wants Chip and PIN for table service, each server will need access to an EMV payment device that they can leave with the customer - a Pay at the Table application that will accept most payment types.

Investments for Businesses to move to EMV
Software upgrades
Hardware upgrade
Testing and certification by software developers - there is currently a very long waiting period for software/hardware vendors to get certified.
Time, resources, and training
Benefits of moving to EMV
Fewer disputes for fraud
Data becomes less attractive for hackers
Path to innovation
Consumer confidence

Counterfeit Card Fraud Liability Shift - American Express, Discover, MasterCard & Visa

Current	October 2015
Card Issuer is liable	For chip cards, **merchant** liable if non-chip terminal

Lost/Stolen Card Fraud Liability Shift - American Express, Discover & MasterCard

Current	October 2015
Card Issuer is liable	For chip & PIN cards, **merchant** liable if terminal is less secure

Visa rules on lost and stolen fraud are different than the other card brands:

Lost/Stolen Card Fraud Liability Shift - Visa

Current	October 2015
Card Issuer is liable	No change

Supported Cardholder Verification Method (CVM)

•PIN

•Signature

•No Signature (such as implemented at a QSR; also called no CVM)

EMV and Cardholder Security

•Implementing the EMVco and Card Brand EMV specifications still leaves a customer's primary account number (PAN) and discretionary data exposed

•In the event that crimeware has found its way into the retailer's POS system or network, the cardholder data still could be stolen and used fraudulently

•Every EMV card being issued in the US includes a magstripe

•Visa has provided no "sunset" date on magstripe support

More Examples and talking points:

To switch or not to switch?

October marks the start of the EMV card liability shift, but accepting the chip cards won't be mandatory for businesses. Most EMV cards still have magnetic stripes, so businesses can swipe those cards if they're willing to risk fraud. When it comes to deciding whether to update to EMV technology, the advice to small business owners is, "Don't run blindly forward."

Businesses should consider both the cost of switching to EMV technology and the likelihood of fraud. For example, a dry cleaning business with a relatively new credit card terminal doesn't necessarily need to rush to purchase a new EMV terminal. But if a business has to replace its credit card terminal anyway or has a history of customer credit card fraud, it makes sense to invest in EMV technology, he says. He cites a jeweler as a business that might be more susceptible to fraud.

Beyond updating the credit card terminal hardware and software, businesses need to train employees to use the new EMV technology. For example, employees should get into the habit of reminding customers to take their cards out of the EMV reader. (Unlike with magnetic stripe cards that customers use with a simple swipe, EMV-chip cards require customers insert the card in the reader and leave it there until the transaction is complete.)

But EMV-chip cards won't eliminate fraud altogether, says Richard Crone, founder of Crone Consulting LLC, a mobile payments consulting firm.

"You cannot get rid of the risk until you get rid of the card," Crone says.