Tecnica

A Leader in Point of Sale Solutions...

EMV™ Overview

First Data.
beyond the transaction

What is EMV™?

- EMV – micro-chip payment standard created by **E**uropay®, **M**asterCard®, **V**isa® over 10 years ago and has been implemented globally
- EMVCo – organization owned by the global brands that manages the standard for global inter-operability
- EMV payment cards improve security over magnetic stripe technology through an embedded computer chip
  - Card validation ensures the card is legitimate
  - Cardholder authentication reduces fraud from lost and stolen cards

What Does the Liability Shift Mean to SMBs?

- October 1, 2015 is the effective date for the counterfeit, lost and stolen and non-receipt fraud liability shift from issuers to merchants.
  - Merchants that do not incorporated EMV technology will assume financial responsibility for fraudulent transactions
  - The exception is Automated Fuel Dispensers that have until October 2017
- Late adopters of EMV will be small and micro businesses
- Indications are that around 35% of small merchants do not understand what EMV means to their business
- **Use this unique opportunity to engage with your clients and show genuine concern for their business!!!**

Liability Implications of EMV™

In U.S. today:

- Fraud in card-present environments is absorbed by Bank/Issuer unless merchant fails to meet POS acceptance and dispute resolution requirements
- Losses are offset when dispute resolution requirements allow liability to be shifted through "chargeback process" to Acquirer/Merchant
- Merchant/Acquirer takes liability for merchant data breaches or skimming attacks

In 2015 with EMV:

Visa

Counterfeit fraud losses "shift" to party who does not enable EMV if fraud would have been avoided if EMV had been used

MasterCard Liability Hierarchy

Party that cannot support a lower-risk option holds the liability. Equal capabilities = issuer holds liability.

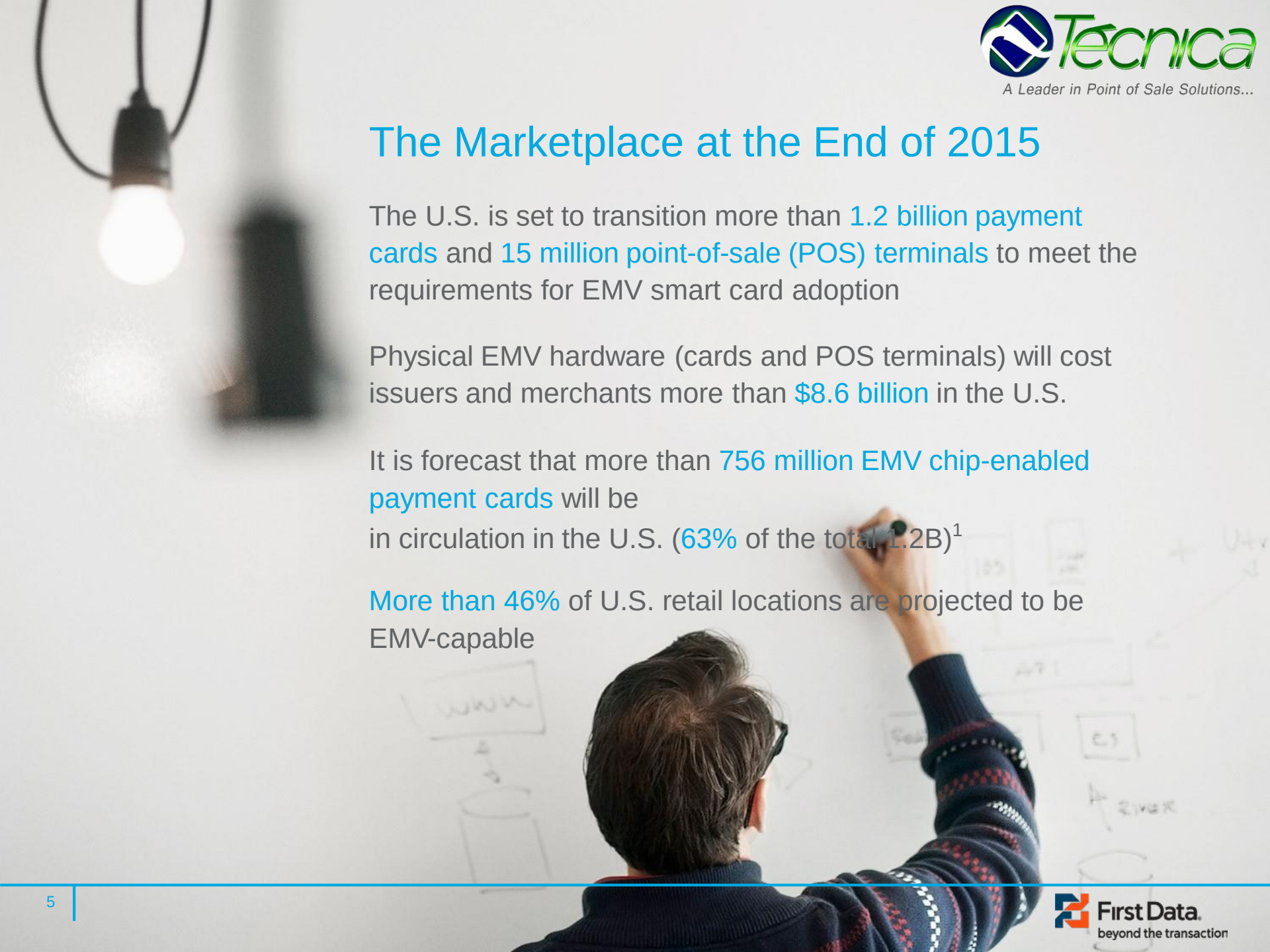
The Marketplace at the End of 2015

The U.S. is set to transition more than 1.2 billion payment cards and 15 million point-of-sale (POS) terminals to meet the requirements for EMV smart card adoption

Physical EMV hardware (cards and POS terminals) will cost issuers and merchants more than $8.6 billion in the U.S.

It is forecast that more than 756 million EMV chip-enabled payment cards will be in circulation in the U.S. (63% of the total 1.2B)[1]

More than 46% of U.S. retail locations are projected to be EMV-capable



Why Implement EMV™?

Tecnica
A Leader in Point of Sale Solutions...

Financial Institutions

Reduce fraud

- Potential to reduce POS counterfeit fraud losses with use of chip
- Shift fraud liability to merchants that do not support EMV

Improve market perception

- Demonstrate to customers and market that cardholder security is important
- Poor brand perception by cardholder if their issuer is last to implement EMV

Avoid increased exposure to cybercriminals

- Late adopters will be the weakest link for cybercriminals – they will find the path of least resistance to identify weakness
- As the market of non-chip card dwindles, the criminals will target non-chip cards

Increase security at the POS

- A primary way cybercriminals use stolen credentials is to create a false card to impersonate the actual card
- Historically, as cybercriminals recognize EMV implementation is underway, they increase activity

Reduce liability costs

- The global card brands have announced a Liability shift for Oct 2015
- In 2015, if the merchant does not support EMV, that liability will shift to the merchant

Avoid increased exposure to cybercriminals

- Criminals will find the path of least resistance through late adopters to identify weakness
- As the population of non-EMV locations dwindles, the criminals will concentrate on non EMV-locations

EMV™ & Data Security – How do they Relate?

Tecnica
A Leader in Point of Sale Solutions...

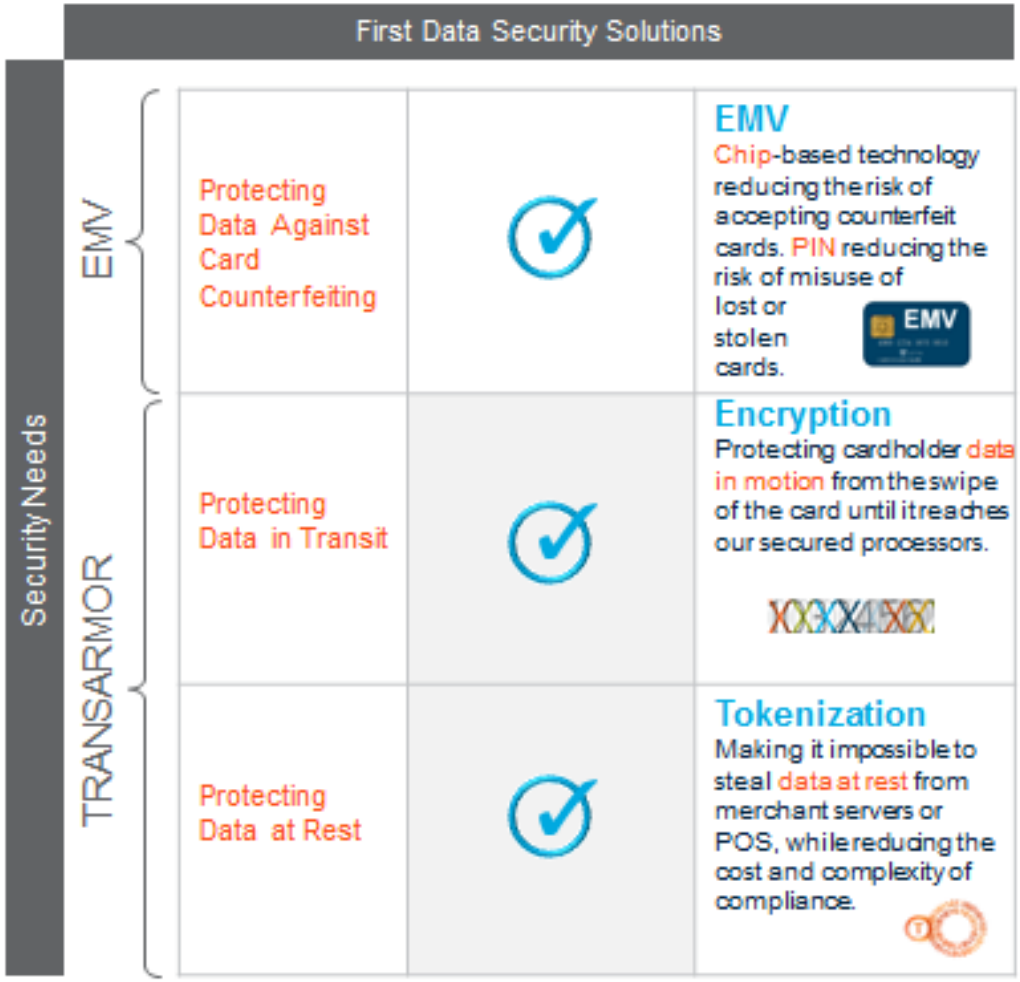
Advances in technology has increased cyber attacks

- Data in motion (e.g., with memory-scrapers)
- Data at rest (e.g., from a database)

Stolen data used to produce

- Counterfeit cards
- Fraudulent online transactions

Focusing on only one or two points of entry can still leave vulnerabilities!



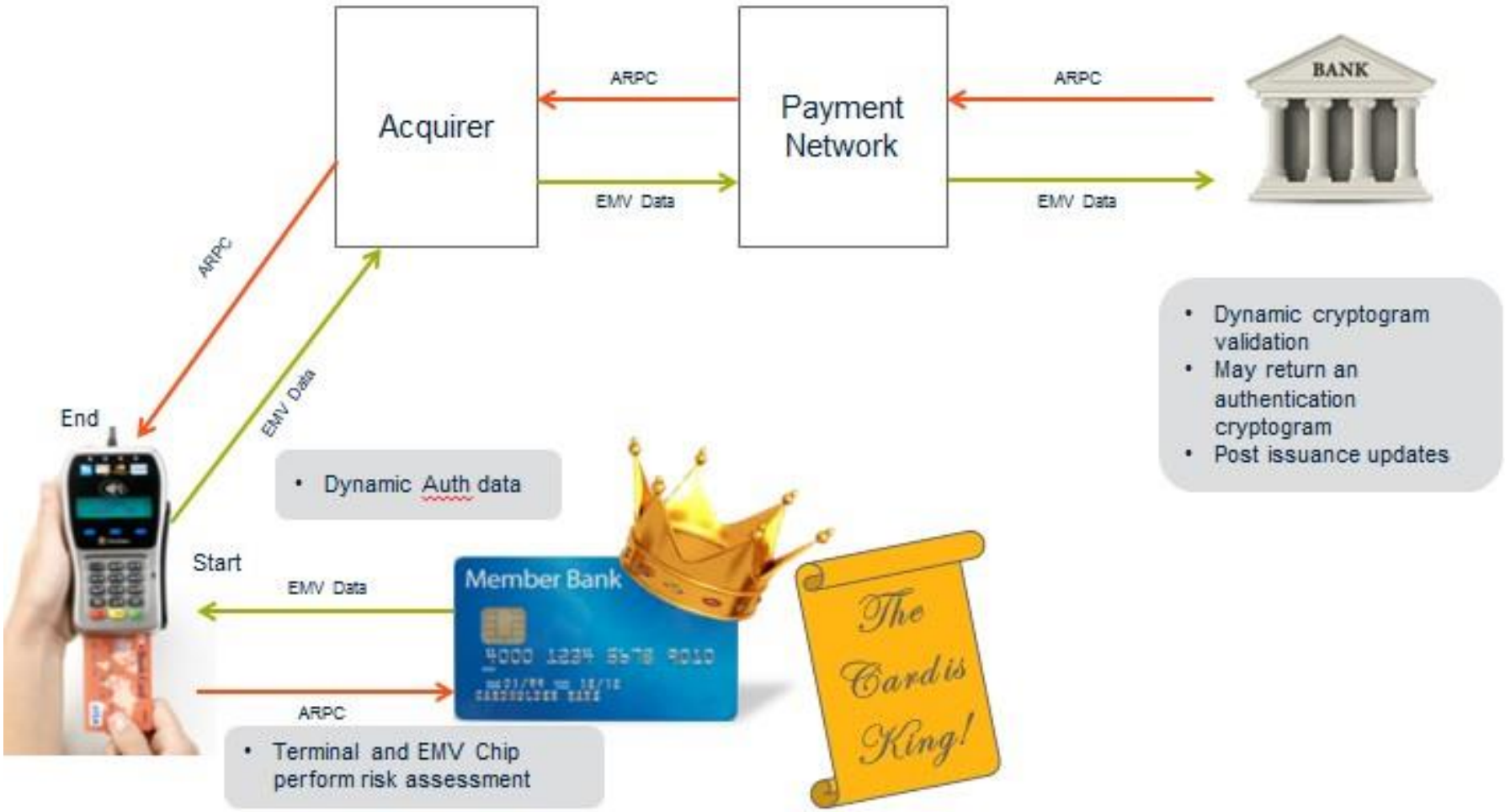
First Data.
beyond the transaction

Tecnica
A Leader in Point of Sale Solutions...

First Data EMV™ Processing

First Data.
beyond the transaction

EMV™ Transaction Processing…the New Normal

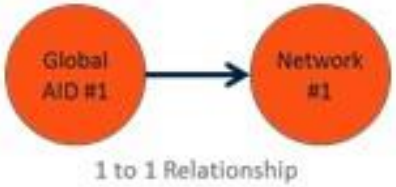


Application Identifiers (AID)

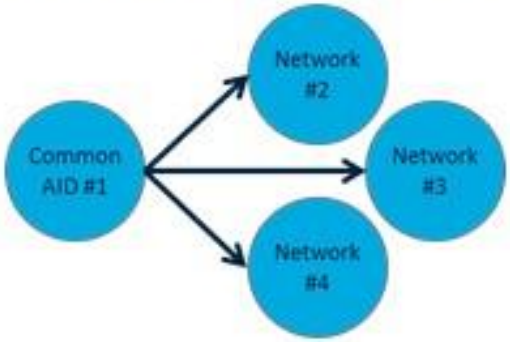
Tecnica
A Leader in Point of Sale Solutions...

Global AID v. U.S. Common Debit AID

- EMV transactions utilize AIDs to determine how or where a transaction should be routed
  - If Global AID is used, transaction must be routed to the one corresponding network only
  - If U.S. Common Debit AID is used, transaction may be routed via unaffiliated networks



1 to 1 Relationship



1 to Many Relationship

- Visa and MasterCard introduced "U.S. Common Debit AIDs" to support Durbin regulations* to route debit/prepaid transactions to unaffiliated networks

First Data.
beyond the transaction

Cardholder Verification Methods (CVM)

- Cardholder Verification Methods indicate the priority order of how the cardholder may be validated in the field – not just one way
  - PIN (online and offline), Signature and No Cardholder Verification Required (No CVM) supported
    - Online PIN is encrypted by the PINpad and sent online to the Issuer host for validation
    - Offline PIN is sent to and validated by the chip; Offline is never sent to the host – only the result is passed
- **The negotiation between the card and terminal determines which CVM to use**

The Different PINs of EMV

Offline Encrypted PIN – only the CAPK keys are required and are used to recover the keys from the card (issuer key & card key which is encrypted with a CA Private Key to which the CA Public Key is used to decrypt it). There are a maximum of six (6) active CAPK keys per card scheme.

***Definition of CAPK**: CAPK (Certificate Authority Public Key) refers to the RSA public key assigned by a card brand and used in EMV to decrypt chip information when paired with a card brand private key. This is used in order to allow the chip card to communicate with the terminal in order to support off-line Card Authentication Methods (CAM) or off-line enciphered PIN. The use of CAPK allows the communication to occur directly between the chip card and the terminal---WITHOUT having to go on-line {NOTE: this is for off-line chip card validation only NOT transaction authorization}. Off-line CAM uses the CAPK to help protect against card counterfeiting and skimming—as it allows the terminal to validate directly with the chip card that the card is from a known issuer. CAPK is also required for off-line enciphered PIN—as this allows the terminal and chip card to communicate directly and validate that the PIN entered by the consumer is indeed valid. CAPK updates are made available via a download from the FD host.*

Online PIN – the DUKPT/3DES keys are required. These keys are used to protect the PIN between the terminal and our host/front-end platform. There may be multiple keys because there may be a DUKPT key between the PINpad and the POS and another DUKPT between the POS and the front-end.

***Definition of DUKPT (Derived Unique Key Per Transaction)/3DES (Triple DES or TDES):** DES, which stands for Data Encryption Standard, is a form of symmetric key cryptography. Symmetric keys are used to ensure confidentiality—meaning the ability to transmit data without anyone being able to see the actual data while in transit. The sending party encrypts the data using the key and the receiving party decrypts the data using the same DES key. 3DES is the DES algorithm performed 3 times. This process scrambles the data making it difficult for an outside party to manipulate. 3DES is an industry standard for encrypting data.*

EMV…..Myth VS Truth

A guide to common myths and the truth about EMV:

MYTH: PIN = Debit, No PIN = Credit.
TRUTH: PIN = Security function for all EMV cards regardless of "Credit" or "Debit" that Issuers are adopting to enhance security around cardholder authentication.

MYTH: Offline PIN only is acceptable therefore no DUKPT/3DES keys (PIN key injection) are required to be injected.
TRUTH: MasterCard has a requirement that as of April 2015 that any device that supports Offline PIN must also support Online PIN and therefore DUKPT/3DES keys are required.

MYTH: Mag Stripe PIN Pads currently deployed will work for EMV (ex. PP1000SE with Vx520).
TRUTH: PIN Pads used for EMV transactions must be EMVCo and Acquirer certified; the use of a specific PIN Pad for EMV will depend on the make/model.

MYTH: An EMV capable PIN Pad already deployed without DUKPT/3DES keys (PIN key injection) will still work for Online PIN transactions.
TRUTH: Online PIN transactions must be protected with DUKPT/3DES keys as they are leaving the device and being transmitted to an external host system for validation. A PIN key injection is required on the PED (PIN entry device—which can be integrated or exist as a separate PIN pad (peripheral)). The same injection will support debit PIN as well as credit PIN for EMV. If devices have been deployed without these keys they should be swapped out with devices that are PIN key injected.

EMV…..Myth VS Truth Continued:

MYTH: The ‘credit’ or ‘debit’ buttons are so the consumer can identify what type of card they are using OR how they wish to pay.
TRUTH: The ‘credit’ and ‘debit’ buttons were asking whether the consumer wanted to use a PIN. The pressing of ‘credit’ or ‘debit’ did not dictate the kind of card. In future application releases the ‘credit or debit’ choice will generally not be available.

MYTH: As long as one device in a store is EMV capable the merchant will not be affected by the Liability Shift.
TRUTH: Any device that accepts a payment card should be updated for EMV. Only updating one device within a store with multiple devices present still leaves vulnerabilities for the merchant as the Liability Shift is on a transactional basis not on a merchant level basis.

MYTH: The October 1st EMV Liability Shift applies to all fraud types.
TRUTH: The October 1st EMV Liability Shift applies to Counterfeit Fraud at the physical point of sale; for MasterCard it also applies to Lost/Stolen/Never Received Issued fraud where a chip PIN preferring card is used in a device that is not PIN capable or where the PIN pad is not present or working.

For more information please contact us Toll Free 800.423.4046
Office 305.477.5617 - Fax 305.591.4255
Email: info@tecnicasystems.com I www.tecnicasystems.com

Tecnica
A Leader in Point of Sale Solutions...