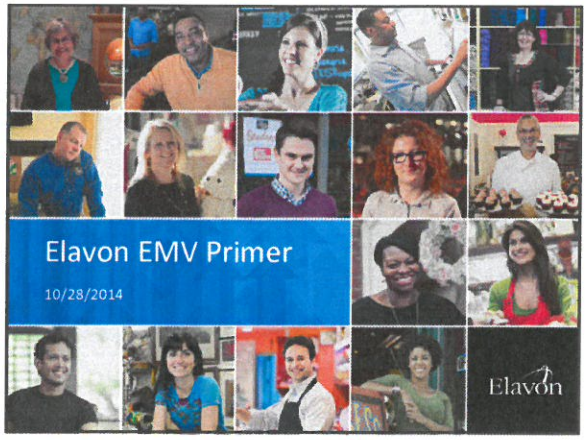
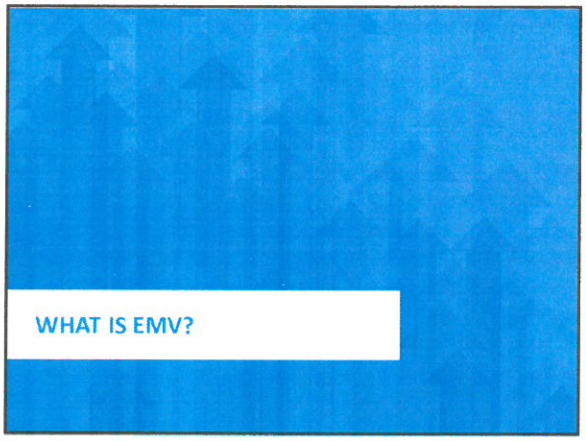




EMV Basics

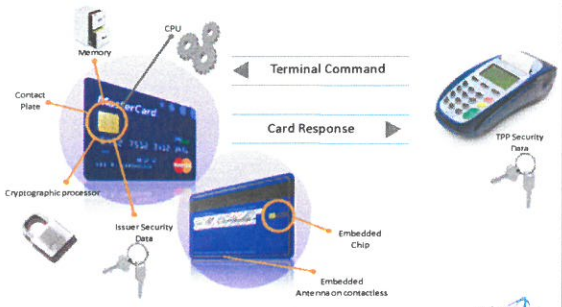
What is EMV?

- EMV is the Global Standard for chip cards to facilitate electronic payment transactions
- EMVCo maintains the EMV specification
- Originally designed to protect against
  - Counterfeit and Fraudulent cards
  - Lost/Stolen cards
  - Delinquent Accounts
- It also provides
  - Transaction integrity
  - End-to-End validation

Elavon

CHIP TECHNOLOGY

What's in the EMV chip?



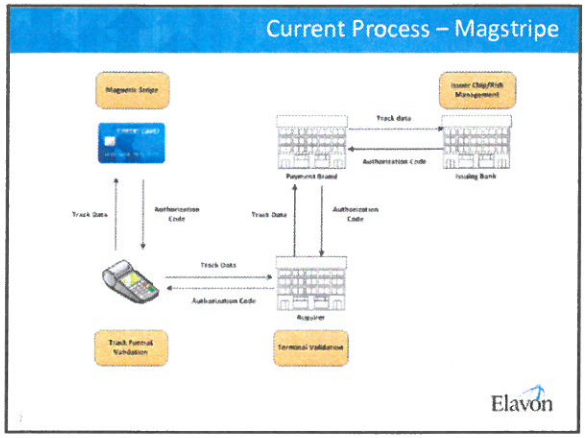
Elavon

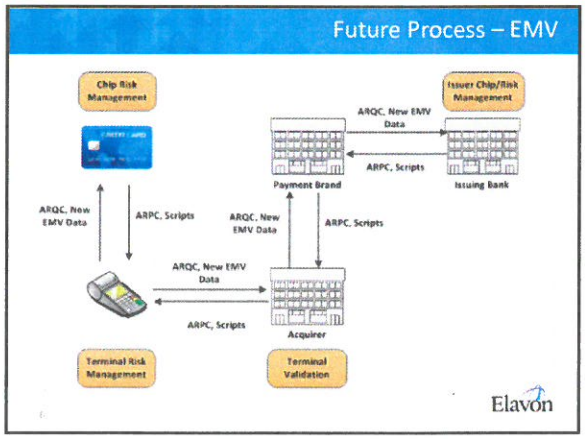
WHY EMV?

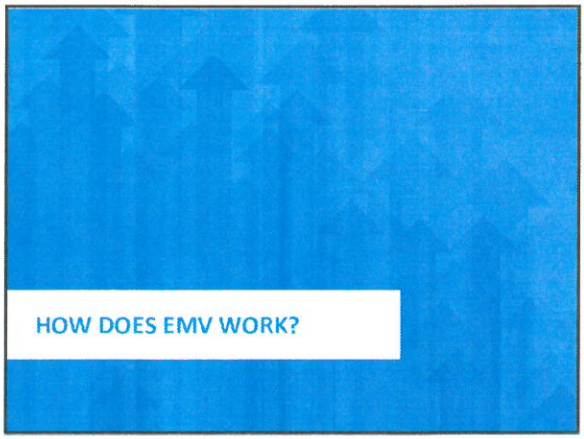
Why EMV in the U.S now?

- EMV is being mandated in the U.S. in 2015 to avoid a liability shift
- EMV protects against fraudulent and counterfeit cards
- EMV provides stronger cardholder verification methods
- EMV provides issuers with a mechanism to manage delinquent cardholders
- EMV protects transactional integrity
- EMV is a global standard
- Supporting contactless is costly on it's own, migrating to EMV provides more benefits to offset the costs
- The payments landscape is changing as new technologies become more prevalent (i.e., mobile, wallets, tokens, ApplePay)

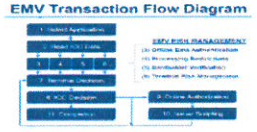
Elavon


Current Process – Magstripe
Magnetic Stripe
Issuer Chip/Risk Management
Track data
Authorization Code
Payment Brand
Issuing Bank
Track Data
Authorization Code
Track Data
Authorization Code
Track Data
Authorization Code
Acquirer
Track Format Validation
Terminal Validation
Elavon


Future Process – EMV
Chip Risk Management
Issuer Chip/Risk Management
ARQC, New EMV Data
ARPC, Scripts
Payment Brand
Issuing Bank
ARQC, New EMV Data
ARPC, Scripts
ARQC, New EMV Data
ARPC, Scripts
ARQC, New EMV Data
ARPC, Scripts
Acquirer
Terminal Risk Management
Terminal Validation
Elavon


HOW DOES EMV WORK?

How EMV Works



- EMV processing steps above is between the chip and the Kernel in the POS hardware
- Processing is accomplished via the hardware reader communicating from the chip (on the card or phone) to the kernel
- The terminal manufacturer's hardware and kernel must be certified – Level 1 & 2 process
- Payment Applications that interface with the EMV Kernel and any components between the PA and the Gateway/Acquirer are jointly certified to the EMV Schemes/Brands – Level 3 process

Elavon

EMV

EMV will act as a catalyst for point-of-sale upgrades throughout the payment ecosystem

- Cardholder data is more secure on a chip-embedded card that utilizes cryptography and dynamic authentication
- Merchants are subject to liability shift for counterfeit cards and lost/stolen if they do not support EMV
- U.S. EMV standards also include support for NFC contactless payments and other emerging payment mechanisms, such as ApplePay
- Four primary features that are defined in EMV:
  1. Authenticate the chip card to protect against counterfeit cards
  2. Cardholder verification to protect against lost/stolen cards
  3. Digitally signing payment data for Transaction Integrity
  4. Transaction Risk Management by the issuer

Elavon

WHERE IS EMV TODAY?

EMV – Adoption

Worldwide EMV Card and Terminal Deployment

The statistics below show worldwide EMV deployment figures as of Q4 2013. The figures represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally.

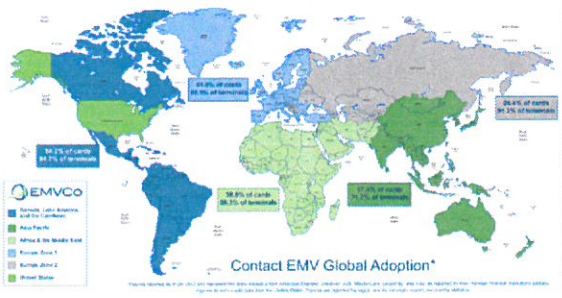
Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Caribbean	47.1M	54.2%	7.1M	84.7%
Asia Pacific	94.0M	17.4%	10.0M	21.7%
Africa & the Middle East	7.7M	38.9%	695K	86.3%
Europe Zone 1	79MM	81.6%	12.2M	99.9%
Europe Zone 2	54M	24.4%	1.4M	91.2%

* Figures reported in Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally

Elavon

EMV – Deployment Map



Elavon

EMV – U.S. Incentive Dates

	PCI Relief	Acquirer Support of EMV	Fraud Liability Shift	AFD Compliance
VISA	Visa • October 2012	Visa • April 2013	Visa • October 2015	Visa • October 2017
MasterCard	MasterCard • October 2012 • October 2013	MasterCard • April 2013	MasterCard • October 2015	MasterCard • October 2017
AMERICAN EXPRESS	AMEX • October 2013	AMEX • April 2013	AMEX • October 2015	AMEX • October 2017
DISCOVER	Discover • October 2013	Discover • April 2013	Discover • October 2015	Discover • October 2017

Elavon

EMV AND SECURITY STRATEGY

EMV Perception vs. Reality

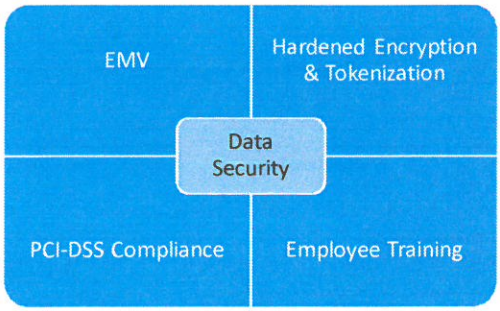
Perception of EMV

Reality of EMV

EMV minimizes, or eliminates, the acceptance of counterfeit payments, it ***does not*** provide transactional data security!

Elavon

EMV - A Piece Of The Puzzle



Elavon

Security Solution Measures Summarized

ENCRYPTION - BREACH PROTECTION

- Card data **encrypted** at swipe head or EMV insertion
- Data only **decrypted** at Elavon's secure data center
- Encryption is the only protection against currently prevalent malware at the Point of Sale
- Simplify eliminates Point-of-Sale card information exposure

TOKENIZATION - DATA AT REST PROTECTION

- **Tokenization** replaces actual card data with a unique ID
- Protects data at rest and in recurring/card on file transactions

EMV - AUTHENTICATION

- EuroPay, MasterCard & Visa (**EMV** aka **CHIP&PIN**)
- Terminals utilize advanced algorithms contained on a CHIP card to authenticate that the card is legitimate.
- **Merchant liability shift date - October 2015**

Encryption + Tokenization + EMV = FULL Security Solution

Elavon

The Reality of Payment Processing

Security Breaches

Market Need

- Retailer – 40 million cards
- Retailer – 50 million cards
- Restaurant – 5 million cards
- Retailer – 3 million cards
- Lodging – Number of exposed cards unknown
- Others ... PCI wide open to breaches

The News Has Escalated POS is Taking the Heat

Major impact:
sliding share prices, CEOs resigning, damaged reputations, financial cost

Customers need payment solutions with a higher-level approach to security

Elavon

Security Breaches - Market Data

Trustwave and Verizon Security Reports*

- Data security is now a global problem.
- A Trustwave survey of security professionals shows that malware has infiltrated 74% of organizations through the web during the past year (2013).
- Primary breach mechanism is malware installed on POS systems, known as POS 'RAM scraping'. 85% of breaches in a 2014 Verizon report incorporated RAM scraping.
- POS RAM scrapers steal payment data - such as credit card track data - from the RAM of POS systems as it is decrypted.

***Recommendation**: Encrypt on the terminal at the card swipe, tokenize all stored payment data, keep sensitive cardholder data away from Point-of-Sale*

Elavon

HOW TO GET THERE?

EMV and Security Implementation Options

Utilize certified stand-alone POS Terminal(s)

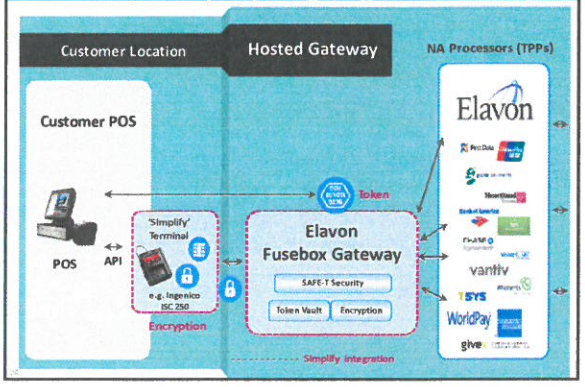
Utilize certified integrated VAR POS Solution

Direct POS Certification:
($30K - $100K certification cost)

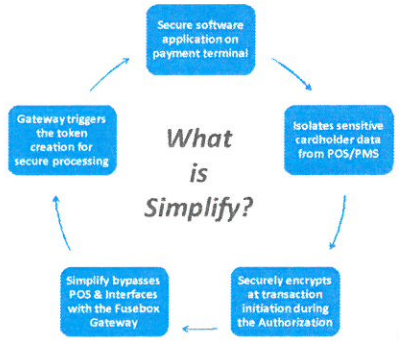
Utilize Semi-Integrated POS Device Delivery (i.e. – Simplify)

Elavon

The Elavon EMV Ready Integration
(Incorporating Encryption + Tokenization)



The Simplify Solution



Elavon

Simplify Benefits

1. **Security**
   - ✓ Eliminates storing cardholder data within your environment.
2. **Reduced PCI Compliance Burdens**
   - ✓ Reduces PCI exposure from Point-of-Sale
   - ✓ Reduces time and effort expended on PCI compliance.
3. **Future Proof and Liability Shift**
   - ✓ Solution is EMV ready including remote device maintenance capability
4. **Flexibility**
   - ✓ Remains compatible with existing Gateway applications
   - ✓ Use variety of terminals without coding to a terminal directly
   - ✓ Support for all payment types (Mag-stripe, EMV, NFC)
5. **Reduced Vendor and Payment Complexity**
   - ✓ Best-of-breed certified payment solution.
   - ✓ Enhanced audit trail + batch settlement.
   - ✓ Tightly integration solution.

EMV SUMMARY

EMV Summary

- EMV is the name of the standards governing ICC (Integrated Circuit Card) transaction processing developed by EuroPay, MasterCard and Visa in 1993
- It's globally accepted as the standard payment acceptance model
- Originally designed for "card present", it has evolved to supports contactless and mobile.
- EMVCo manages, maintains and enhances the EMV specifications to ensure global interoperability and acceptance of chip cards.
- EMV is a specification that was designed to protect against:
  - Counterfeit and skimming – through the use of cryptography, provides dynamic digital signature allows the terminal and issuer to authenticate valid chip and chip to authenticate the issuer
  - Man-in-the-middle – digital signatures and cryptograms based on key elements of the transaction, such as transaction type and amount, provides transactional integrity
  - Lost or stolen – through the use of offline PIN and online PIN
  - Consumer delinquency – through the use of offline risk management and issuer scripts
  - Replay attacks – where a valid transaction is repeated or delayed into the network. EMV has a counter variable that is with the ARQC or TC cryptogram guaranteeing uniqueness, replays are easily identified and

Elavon

Questions?

EMV, mobility, and high profile security breaches are driving the search for more secure, flexible and scalable end-to-end payment solutions.

Elavon can effectively help manage this risk, with a world class end-to-end secure payment integration.

Elavon