


PARKING & TRAFFIC
CONSULTANTS



EMV Credit Card Parking Technology for 2012.

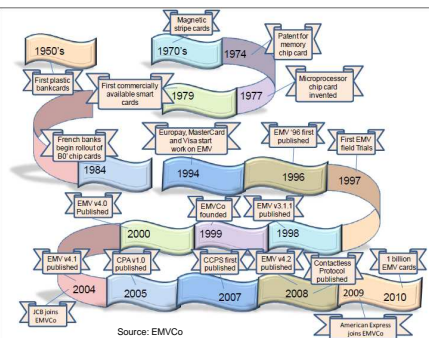
What are the various stakeholder obligations to ensure its proper implementation?

Glenn Caldwell

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC
CONSULTANTS

In the beginning there was the card
.....next there was fraud (its not just about fraud)



Source: EMVCo *Driving success through valuable advice*

PARKING & TRAFFIC
CONSULTANTS

Fraud History 1980 – present

- Around the world, bank card fraud losses to Visa and MasterCard alone have increased from \$110 million in 1980 to an estimated \$1.63 billion in 1995
- The Australian Institute of Criminology has revealed that fraud accounted for 57.15 cents of every \$1,000 transacted using credit and charge cards in 2009.
 - This is an increase of 55 percent since 2006
- The Australian Crime Commission 2011 report found that in 2010, 593,819 fraudulent credit card transactions occurred, scamming Aussies out of a whopping \$145,854,208
- 10% of Australians says they have been a victim of credit card fraud over the past 5 years, which is relatively low compared to some other countries.
 - America and UK - 27%
 - China and Singapore – 15%
 - Germany – 8%
 - Dubai - 7%

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC
CONSULTANTS

Who are the people we can thank for EMV

- Albert Gonzalez – one of 11 men charged with the largest credit card security breach recorded in 2008. 46 million customers were affected
- Database driven fraud (rather than skimming) via "Wardriving"
- 3 massive attacks
 - TJX Retailers
 - 7 eleven
 - Heartland payment systems



© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*


PARKING & TRAFFIC
CONSULTANTS

Recent Changes in fraud behaviour

- Most common form of identity theft
- Petrol Pump fraud on the increase as criminals continue to find new areas of weakness. Internet security and PCI are making it increasingly harder for criminals and they are now moving into new territoryUnattended credit card.!

New Credit Card Skimming Scam Hits RB, PQ Gas Stations
November 10, 2011

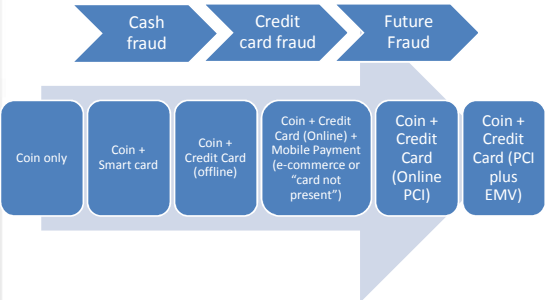
New generation of card skimmers sold online, hit Colorado
November 8, 2011



© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC
CONSULTANTS

The Parking Journey –
Managing cash fraud a priority



© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

What is EMV?

- EMV® is a global standard for credit and debit payment cards based on chip card technology. As of end-2010, there were more than 1.24 billion EMV compliant chip-based payment cards in use worldwide.

EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.

- EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications.

Source - EMVCo

Driving success through valuable advice

Key advantages of EMV

- More secure than encoded magnetic stripe.
- A unique digital signature of each new transaction is produced in the chip proving authenticity in an offline mode and prevents use of fraudulent cards?
- Can be used to secure online transactions through cryptograms
- Supports enhanced cardholder verification methods
- Configuration of the card can be changed AFTER it has been issued
- Contactless (Tap & Go) – upgradeable
- Offline transactions

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

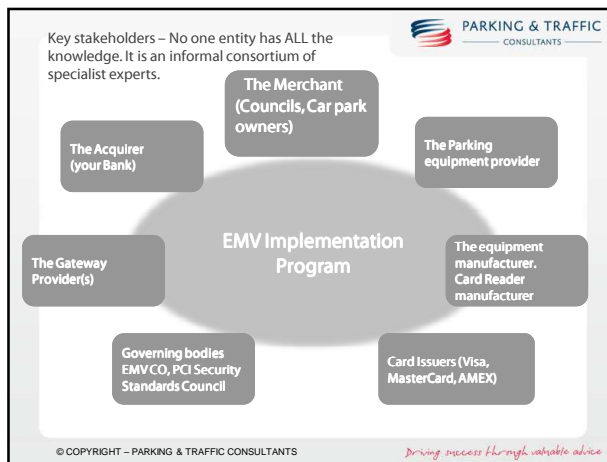
Driving success through valuable advice

We have a General Direction – But no real “Directive”

Proliferation of EMV POS terminals for attended – yet little progress for unattended

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

Driving success through valuable advice



EMV - An Overview

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

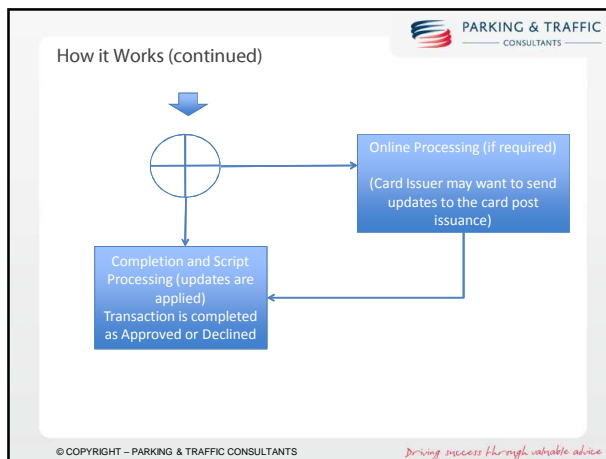
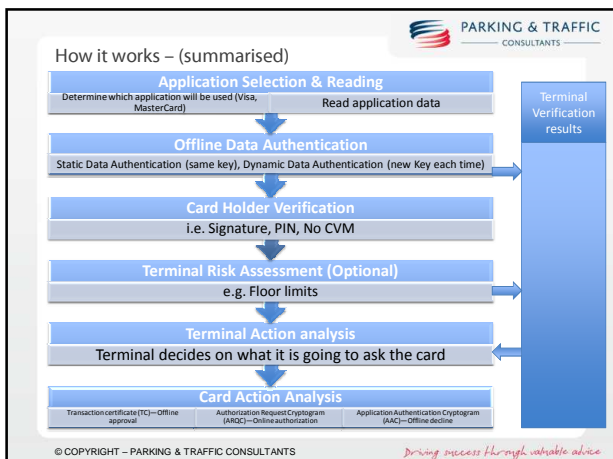
Driving success through valuable advice

The EMV Credit Card

- EMV “SMART CARD” is personalised by the card issuer and certifying authority
- Superior levels of security is achieved by employing Public Key Cryptography
 - Asymmetric rather than “shared”

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

Driving success through valuable advice



- Key Terms**
- CAT/ UPT - Cardholder Activated Terminal/Unattended Payment Terminal
 - Unattended**
 - Card not present**
 - PAN – Primary Account Number
 - No CVM – No Customer Verification Method**
 - EMV level 1**
 - EMV level 2**
 - 2 key triple des encryption-** K1 != K2; K1=K3. Data Encryption standard.
 - Cryptograms – AAC, TC, ARQC, ARPC
 - Digital Signature
 - PCI-DSS
 - PA-DSS
 - PCI – PTS (3.1)**
 - Chip & PIN
 - RSA Public Key Cryptography
- © COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

Liability Shift

The Liability Shift applies to the party (Issuer/Acquirer) for all losses related to fraud incurred by card payment transactions, that are non-EMV compliant.
E.g. **Mastercard** "An acquirer operating a magstripe-only terminal will be liable for any counterfeit fraud that is conducted at that terminal using a counterfeit card that was originally issued with a chip. The principle is that the fraud would have been prevented if the terminal had been chip-capable" *

Possible E.g. Floor limits A terminal has a floor limit set to \$20, Yet decides to go online for a \$19 transaction despite the card having an offline limit of \$10.

- Floor limits, Lost & Stolen cards, Counterfeit cards, Online/offline, Insufficient funds (offline restrictions applied to each card to reduce this), \$100 (greater or lesser than)


- The liability parameters must be verified by your Acquirer**

*Mastercard – An introduction to chip



© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

- Liability Shift**
- The Liability shift is already in place – We are just waiting on deadlines until the penalties start applying
 - Penalties?.....PER TRANSACTION, PER TERMINAL?
 - What's in it for the card schemes?
 - What's in it for the merchant?
- © COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*






The Complex Dialogue that is EMV & PCI

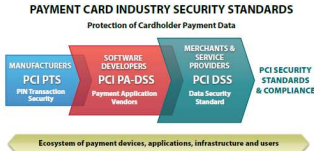
Driving success through valuable advice



PCI –DSS


- PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions.

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data



Source: PCI Security Standards Council

Driving success through valuable advice




PCI - Terms

- The PCI DSS** applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS. (the organisation)
- The PA-DSS** is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties.
- The PCIPTS** (formerly PCI PED) is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Most relevant is the new standard – PCI-PTS (3.1) for payment terminals with no PIN entry (October 2011).
PTS= PIN Transaction Security.

Source: PCI Security Standards Council

Driving success through valuable advice




PCI and EMV

- However, EMV by itself does not protect the confidentiality of, or inappropriate access to sensitive cardholder data.** Current EMV acceptance and processing environments may process both EMV and non-EMV transactions, (such as magnetic stripe, or primary account numbers (PAN)).These non-EMV transactions do not have the same fraud-reduction capabilities of EMV transactions and, consequently, require additional protection.
- In addition, it is important to note that in EMV environments the PAN is not kept confidential at any point in the transaction, indeed, it is necessary for the PAN to be processed by the point-of-sale terminal in the clear in order to complete critical steps in the EMV transaction process. The expiry date and other cardholder data are also transmitted in clear-text.
- The potential for these transaction types and/or data elements to be exposed and used fraudulently within both the face-to-face channel and the card-not-present channel are the reasons why it is necessary to implement PCI DSS in today's EMV acceptance environment(s)
- By design, PCI DSS does not distinguish between underlying transaction security mechanisms, but instead seeks to protect the PAN and other sensitive authentication data. Both PCI and EMV are essential elements in the fight against fraud and data exposure. Together they provide the greatest level of security for cardholder data throughout the entire transaction process

Source: PCI Security Standards Council

Driving success through valuable advice



Deadlines

VISA timeline

- All new unattended payment terminals must be EMV from April 2012
- All existing unattended transactions must change over to EMV by January 2014

MasterCard Timeline

- All Unattended payment terminals must be EMV by April 2013

What if your bank is not ready to process EMV transactions in time for Visa mandate April 2012?

What if the Merchant is not ready?

- Do you have budget deadlines that need to be submitted for 2012 – 2013
- Need to get estimates for credit card upgrades including full scope of works

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

Driving success through valuable advice



Upgrades of current equipment

Off street

- New EMV card readers installed (separate to a coding unit)
- No PIN - Good News!!!

On-street

- New card readers?
- New CPU?
- New software

Other Changes

- Gateway configuration

Only the equipment provider can provide a definitive answer!!


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS

Driving success through valuable advice

EMV Terminals – local options

All in one card reader – Level 1 & 2
e.g. Hypercom

Open architecture solution – level 1
e.g. Magtek I-65



What is the difference and does it really matter?

- Answer: speak to your bank. Check for PCI Certification

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

Key issues

- Parking Equipment Upgrade Costs
- What are the penalties for non-compliance
- Does the bank have a say in regards to the merchants choice of equipment supplier
- In light of the announcements recently from Visa and MC, if a merchant has recently bought equipment that is not EMV enabled – but the upgrade costs are high – what can they do?
- What are the equipment providers obliged to sell in the current environment?
- For all new equipment – if it is “EMV compliant” but not “EMV enabled” then what is involved in complete the process. Is there any additional costs to the customer?
- Contactless...when is it going to roll out?

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

What is the business case for Shifting to EMV

Considerations

- What is the true value of the liability shift?
- What is the real financial incentive?
- Capital upgrades – cost
- Risk management factors (reduced fraud)
- Compliance to current standards
- Future proof
- *How old is the current equipment?*

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

Stakeholder Collaboration & Consultation

- Suppliers to work with Third Party Certifiers + Banks + Acquirers
- Merchants to determine what PCI obligations they may have
- Gateway providers to assist as required
- Organisations (e.g. Witham Labs) are available to assist with PCI compliance.
- Acquirers must demonstrate leadership and direction!

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

Implementation

What are the responsibilities for each stakeholder in regards to the roll out of EMV?

Driving success through valuable advice

Stakeholders

1. COUNCILS & CAR PARK OWNERS (THE MERCHANT)
2. BANKS (THE ACQUIRER)
3. PARKING EQUIPMENT PROVIDERS (SUPPLIERS)
4. GATEWAY PROVIDERS

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

The Merchant

- Councils
- Car park operators
- Car park owners and managers
- Universities
- Hospitals

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

The Merchant

Who can you trust for the best advice?

- Your team – internal stakeholders
- Must be your preferred bank.
 - Get technical advice
 - Ensure they are “part of the team”

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

Your bank – how they can help

- Provide written advice regarding the changes to unattended transactions
 - Timeframes
 - Fines
 - Liability shifts
 - How does this apply to transactions above and below \$100
 - In what way does it include lost, stolen and counterfeit cards
 - Technical direction
- Provide advice on PCI and EMV standards
- Review current credit card payment solutions
- Assist with the assessment of future upgrades and capital purchases (can you get them to sit on the panel?)
- Project manage the EMV certification process with the gateway providers, suppliers and independent certification agencies (e.g. Witham Labs and FIME)

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

The Supplier

- Understand EMV technical requirements
- Develop a technical roadmap that includes contactless
- Organise gateway partners and major banks
- Develop or acquire EMV terminal hardware + software
- Futureproof to include Contactless.

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

EMV Certification Process

```

    graph TD
        Bank((The Bank)) --- Agency((Certifying agency  
e.g. FIME))
        Supplier((The Supplier)) --- Agency
        Gateway((The Gateway provider)) --- Agency
    
```

- Supplier develops technical product
- Supplier manages EMV certification and PCI for applicable payment solutions
- Supplier – gateway provider – Acquiring bank establishes a working group
- EMV testing commences – data logs are created
- All data and logs are submitted to an EMV certifying body for verification
- Card Scheme issues letter of approval


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

PARKING & TRAFFIC CONSULTANTS

Put IT in writing

- EMV status of current equipment
 - Are the reader EMV level 1 compliant at least
- What is the end-to-end upgrade to EMV
 - What will it cost
 - When will it be ready
 - Which banks and gateway providers is this compatible with
- Overseas EMV certification (e.g. Europe)next steps.....
 - Local gateway and banking partners (SPECIFIC DATA FIELDS MUST BE ACCOMMODATED BY THE BANK)
 - Local testing for MasterCard and Visa
 - Letters of Approval for local solutions
 - Relevant PCI compliance

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



Gateway Providers


- There are a variety of gateway providers that have varying depths of platforms. They are the link between the merchant and the acquirer
- The banks do not have the capacity to develop a new interface every time a new merchant comes along with a new device OR there are new banking requirements that affect interface architecture.
- The gateway provider becomes a partner to the bank in that they take on board the banking mandates on their behalf

Key Roles

- 1 – An Aggregator and interface provider that develops the technology to facilitate merchant transactions.
- 2 – And when required – educate merchants

- The gateway provider may decide to become involved in technology and develop a plug and play terminal for the unattended (or attended) market.


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



The Acquirer (The Bank)

- Likely to NOT be EMV ready for unattended transactions
- Currently handling EMV for ATTENDED transactions...however.....
- Need to update system (in some instances) to handle the extra data elements relating to unattended transactions
- Please do not send out the relationship manager to “relay” questions and answers..... Get one of the technical people to be included in client meetings!

© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



The Merchant (Part 2) – Do’s and Don’ts

- Establish a **working group** that includes internal staff (operations, finance, contracts etc..) plus representatives from the bank
- **DO NOT GET INTO THE BUSINESS OF STORING CREDIT CARD DATA** – outsource this to your providers
- Ensure you have contracts in place to cover parking equipment maintenance, banking, gateway processes. These contracts must stipulate:
 - PCI certification is current and relevant to the applications being used and covers the process end-to-end
 - Relevant technology has EMV certification (Levels 1 & 2)
 - Card Scheme approval of the solution.
 - Liability shifts are clear
 - Upgrade costs are well defined
 - No increases in merchant fees!!
 - Any current EMV architecture is relevant and will contribute to a future upgrade
 - Back of office management systems and reporting will continue with minimal disruption to transaction history. Credit Card History can be tracked on back office systems (with the permission of the card holder only)
- **YOU MUST WORK WITH YOUR BANK AS THE PRIMARY PARTNER IN THE PROCESS. THEY MUST UNDERSTAND THE ENTIRE SITUATION ON A TECHNICAL AND RISK MANAGEMENT LEVEL.**


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



Budget Implications

- Forecasting cost to upgrade in 2012 – 2013
- Local Councils – procurement guidelines and “exceptional circumstances”
- Do your current contracts with your suppliers cover EMV retrofitting and maintenance?


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



Conclusion

- EMV solutions must be “end to end” for it work. EMV “compliant” solutions do not necessarily stack up.
- Unattended – No CVM – No PIN – Online (Floor limit = 0)
- The Acquirer is ultimately responsible for verifying the EMV and PCI compliance for the merchants facilities. Merchant cannot be expected to know if a transaction is EMV or not and is securely transmitted.
- Acquirers must assist with project management of the EMV certification process
- Any claims made by suppliers must be put in writing with technical diagrams and specifications and verified by the bank.
- Your bank is expected to have a clear vision and roadmap for EMV and contactless in the unattended space – including liability rules, fines and technical aspects of EMV for both MasterCard and Visa
- A Working group is essential to ensure a united position on various issues and that the journey is a lot smoother
- The merchant (Council, car park owners) must be given a chance to upgrade their current facilities with sufficient time to allow for budgeting, procurement and implementation.


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*



Contactless – how does it fit into the picture?

- AMEX – latest developments – commence rolling out chip cards before XMAS
- Mag stripe for HOW LONG? Currently used as a fall back
- Contact – THEN – Contactless. How and EMV solution easily bridges the gap to introduce contactless
- Benefits of contactless. Transit systems – reduce read errors and maintenance. Near Field communication. Faster transactions.


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

 PARKING & TRAFFIC
CONSULTANTS


Next Steps

- Other options in the meantime.....
 - Pay by phone
 - Coin only? For some meters with low revenue
- Expected increases in "Card not present" fraud due to EMV
- Develop a consistent message on what
 - Parking Association role? PAA steering group?
 - Regular updates on changes to PCI and EMV for unattended
 - Councils to work together


© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*

 PARKING & TRAFFIC
CONSULTANTS

for more information
visit us at: parkingconsultants.com

subscribe to  WAYFINDING
CONSULTANTS

for the latest in parking industry
news



© COPYRIGHT – PARKING & TRAFFIC CONSULTANTS *Driving success through valuable advice*