

# Assessing the impact of EMV migration: A pragmatic delivery approach

**Ian C. Povey**

*Received (in revised form): 24th June, 2008*

CardsConsult Pty Ltd, PO Box 4069, Croydon Hills Victoria 3136, Australia.  
Tel: +61 407 042 885; e-mail: Ian.Povey@CardsConsult.com

*Ian Povey is the Managing Director of CardsConsult, a specialist international business adviser focusing on innovation of cards and payments programmes. Ian has directed cards and payments initiatives for more than 12 years in senior positions at PwC Consulting, at EDS, as the Director of Cards Strategy for the EMEA region, as Senior Vice President at MBNA Europe Bank as Head of Product Development and, recently, as an Executive Manager at ANZ Bank in Australia, heading up Emerging Payments. Ian's EMV experience dates back to 1996 working in Asia and culminated in directing the ten million card portfolio conversion to chip and PIN (EMV) for the European operations of MBNA in 2002–2004. At CardsConsult, Ian and his associates currently support card issuers and retailers in Canada, Australia and New Zealand drawing on the lessons of earlier implementations. The development of coherent strategies for chip best to leverage the investment remains a core focus. Beyond EMV, Ian was appointed Program Director at the National Registration Department for the Malaysian National ID, provided expertise in the development of the Bonus Card in Turkey with YKM, who initiated the programme and its award to Garanti Bank, and Ian was seconded as the Smart Cards Policy Adviser to the UK Government at the Office of the e-Envoy. Today, Ian continues to provide strategic business and technical advisory services internationally on chip and PIN, de-coupled debit, remote mobile payments and government payment services, looking for both disruptive and innovative approaches.*

## **ABSTRACT**

*This paper assesses the impact of the global migration of card-based payments to move away from magnetic-stripe-based transactions to EMV (Europay, MasterCard, Visa) or chip-based transactions. It is imperative that all aspects of the card payments model are considered when assessing the impacts of changes to technology, business processes and the end customer experience. The key driver for chip-based card payments over 12 years of standardisation and deployments globally has centred on fraud. Market migrations range from nationally coordinated efforts through to individual organisational programmes. Today, markets grapple with business cases, market or industry mandates, regulatory intervention and identifying marketing opportunities. The growing strength of the retail sector to challenge the banking industry as the traditional custodians of the international payment schemes (Visa and MasterCard in particular) has required the engagement model between stakeholders to become more inclusive. Strong engagement between the retail and financial services sectors is a critical aspect of a successful migration to EMV. The payments schemes (including American Express and JCB) play an increasing role in supporting all stakeholders in the payments model. This paper provides insight into the impacts of an EMV migration and best practices to manage market migration effectively.*

**Keywords:** *EMV, chip and PIN,*

*card issuing, card acquiring, payment processing*

## **INTRODUCTION**

A glance at a payment card shows that there has been relatively little change in its design and utility. In fact, the combination of security features has continued to grow without the removal of older features. Most payment cards continue to have raised embossing details to denote card number, expiry and name. The signature panel, hologram and magnetic stripe also continue to reign, together with the EMV chip.

### **What is EMV and why chip?**

Smart cards or chip cards have a long history, patented initially in 1968. They are only now coming of age across a plethora of industry sectors and technology platforms. Mobile telecoms, National ID programmes, banking, mass transit systems and defence facilities are just some of the user groups of smart cards today.

A smart card chip is most often embedded into a credit or debit card-style plastic card body. The SIM card used in GSM network mobile phones is 'popped' out of a card with similar qualities. The chip has greater durability and is a more secure alternative to magnetic stripe. Additionally, the chip card supports enhanced data storage capabilities and new user interfaces such as contactless or radio frequency.

In 1994, the payments industry delivered the first version of a chip-based payment specification and, in 1999, a governing body EMVCo LLC<sup>1</sup> was established to oversee the ongoing development, maintenance of and compliance with the EMV Specifications. The primary role of EMVCo remains to ensure ongoing interoperability and acceptance of chip-based payments globally.

### **Market maturity of EMV migrations**

Three mature Chip and PIN markets worth noting are France, the UK and Malaysia. During the 1990s, France and the UK, in particular, started to deploy chip-based cards. France developed a domestic specification known as 'B Zero Prime', to be deployed nationally as chip and PIN, while the UK developed the UK Implementation Specification (UKIS) in line with developments on the EMV specification at that time, but as chip and signature. In the six years from 1992 to 1997, the French industry experienced a 4.5-fold decline in fraud from 0.087 per cent to 0.019 per cent,<sup>2</sup> resulting from their migration to chip and PIN. The UK at the time, struggled to move forward, as many aspects of the migration had not been resolved — in particular, the method to verify the cardholder.

There is now a growing body of evidence to suggest that markets without EMV merchant terminals are being targeted for cross-border counterfeit fraud. A Visa presentation<sup>3</sup> notes that fraud on UK cards in Canada grew 250 per cent between 2006 and 2007. Additionally, the evident migration of fraud activity between Malaysia and Thailand is telling with the Visa data shown in Table 1.<sup>4</sup> Visa further records that EMV cards have been issued in more than 92 countries across all global regions as of March 2007.<sup>5</sup>

### **WHY MIGRATE TO EMV?**

With progress for smart cards in payments during the 1990s, it became apparent that a number of business issues could be overcome. Today, many of these benefits are overshadowed by tensions between the banking and retail sectors over the cost and impacts to upgrade to chip versus the savings to be achieved from such a migration. The evidence of cross-border fraud and fraud migration should not

**Table 1: Visa fraud statistics**

<i>Year</i>	<i>Malaysia fraud figures (US\$m)</i>	<i>Thailand fraud figures (US\$m)</i>
2003	5.9	0.25
2005	0.3	3.40

be ignored, however, when deciding to migrate to EMV.

Yet, a lack of business case has now emerged as a prominent point for debate. Arguably, it is not this black and white. While markets do grapple with business cases, market mandates and regulatory intervention, many payments stakeholders choose to adopt EMV, despite others deferring their migration activity. Even today, acceptance of chip and PIN in the UK has not reached 100 per cent.

Fundamentally, the integrity of the payments systems must be protected. Migrating to chip supports this objective and can provide a foundation on which to build additional enhancements for card-not-present fraud. The current drivers to migrate to EMV do ultimately fall back to either fraud or marketing-related drivers.

Both Visa and MasterCard have communicated regional dates for EMV compliance. These were communicated via a strategy known as a 'liability shift' in relation to disputed transactions or chargebacks. The traditional chargeback processing rights have been modified to reward the party who has adopted chip as their preferred method of payment. Table 2 indicates that the merchant acquirer would be accountable for certain categories of fraud where a regionally issued chip card was used at a non-chip-enabled point of sale (POS) within that region.

The regional nature of the liability shift means that issuers and acquirers are only exposed to transactions that originate between a card and POS within the speci-

**Table 2: Liability shift chargeback overview**

<i>Card (issuer)</i>	<i>POS (merchant acquirer)</i>
Magnetic stripe	Magnetic stripe
Chip	Magnetic stripe
Magnetic stripe	Chip
Chip	Chip

fied region. As an example, an EU chip card used in an Australian non-chip POS would not fall under the liability shift arrangements, as this is an inter-regional transaction. A Malaysian issued chip card used in an Australian non-chip POS, however, would qualify.

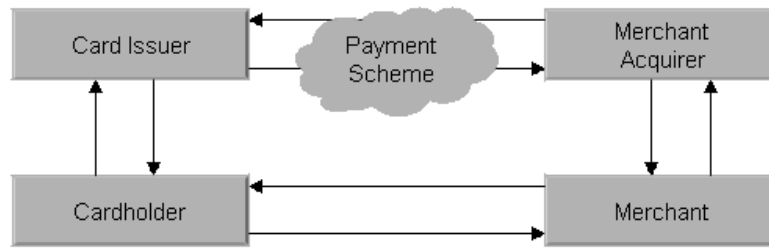
Most liability shift dates are now historical. Some countries within a region agreed domestic variants, whereby domestic transactions were exempt from the liability shift until a future agreed date. The European liability shift started on 1st January, 2005, which included domestic and regional cross-border transactions. Spain, for example, sought to delay its domestic transactions falling under the liability shift until 2008.

### **ASSESSING THE IMPACT OF AN EMV MIGRATION?**

It is important to consider EMV migration as a significant and complex change project. It is definitely not a standalone technology project; it incorporates business re-engineering and places a high burden on training and communications. Figure 1 reflects each of the stakeholders in the standard 'four party' Visa and MasterCard payments model.

This paper pragmatically discusses the impacts of the migration on each of the stakeholder groups, and highlights points of focus to deliver a successful programme.

Figure 1 Standard four-party payment model



**Chip payment cards change processes**

The change management effort relating to the customer and merchant experience at the POS with an EMV card should not be underestimated. There are a number of chip-based actions that can deliver different procedural outcomes compared with magnetic stripe transactions.

Explicitly, chip-based transactions require the card to be ‘docked’ in the device for the duration of the transaction. This apparently simple process change requires issuers and merchant acquirers to consider a number of policy, training and procedural impacts. Examples include POS service offerings such as pre-swipe in multi-lane supermarkets, tipping and the management of cardholder verification — PIN or signature.

**Stakeholder impacts**

Each stakeholder aims to obtain a tangible benefit from their investment in EMV; to what extent benefits are delivered comes down to market adoption, commitment and an agreement to engage at an industry level to manage issues and solve for common approaches at the point of transaction. Alongside the explicit impacts outlined in this paper, stakeholders are exposed to impacts both within and outside their control.

*Issuers*

The impact at the moment of payment for the cardholder is the greatest risk to an

issuer. Transaction behaviours remain an ongoing discussion point in the industry, particularly where a transaction is declined offline between the card and the device. Under the Scheme requirements, there are no formal requirements for an issuer to be advised as to the reason for this type of decline. An exception is an offline decline that follows an online approval by the issuer. This would be notified in the reversal transaction and may have resulted from an issuer authentication failure.

Many of the transactional impacts will be derived from the configuration of the chip risk profile set by the issuer and signed off by the payment scheme. It is generally advisable not to deviate too far from recommended payment scheme risk profile templates.

The impact on brand reputation can be positive for an early adopter; an issuer may be perceived by the consumer to be innovative and providing for their future security. This may result in increased acquisition activity where first mover advantage is available. On the negative side, an issuer who is seen to be at the tail end of delivering chip may see a decline in acquisition rates and even net attrition.

Positive impacts are also derived from cardholders who are frequent travellers to markets with mature chip environments in place. While a magnetic stripe card is a valid payment token, they have been known to be rejected by some retailers in mature chip markets.

Yet, while an issuer’s risk profile settings

on the chip are important, it is equally important for an issuer to understand the impacts of risk settings on the payment terminal. A number of suitable test tools are available to simulate transaction outcomes with different terminal and card configurations. The relevant EMV settings on the chip and terminal that should be reviewed include Issuer and Terminal Action Codes (IACs and TACs).

Issuers should pay careful consideration in providing permissions to the chip card to transact offline to the issuer host. The outcome of transactions that are unable to go online from the merchant may be configured to support offline approvals or to indicate that the issuer supports voice authorisations.

Issuers continue to have system development options (Early or Full Data) that can support a faster issuance of cards, with minimal host impacts. While this is an initial benefit, the longer-term impact of an Early Data implementation needs to be addressed if support of card risk management is to be a requirement in a mature market.

### *Acquirers*

While acquirers and their merchants have the greatest technical impact (they must implement a Full Data host environment), they are also affected operationally.

While some markets provide for domestic transaction interchange benefits, many markets see this as a 'penalty' model to encourage migration to EMV. With an increasing degree of cross-border card-present fraud, acquirers who move to chip are better positioned to address and mitigate their exposure to chargebacks under the various regional liability shift arrangements.

Acquirers who are part of a single organisation with an issuing business are well placed to deploy new initiatives leveraging chip or alternatively to partner

with a suitable issuing partner for rewards, contactless or other related propositions.

Acquirers are the conduit between the retail POS and the payment schemes. It is important that acquirers are actively engaging and supporting major merchant groups, in particular those who own their POS devices. This dialogue is also important in managing timing and resource expectations for testing and certification dependences through to the payment schemes.

### *Merchants*

It is arguable that this stakeholder group has the greatest impact, as they are the frontline of card-present transactions with cardholders. Here, they will either create or receive card acceptance issues, there will be challenges with cardholder communications, and there are significant overheads in retail staff training and conformance.

As in the issuer community, it is critical that merchants understand the impact at the POS of the combined issuer risk and terminal risk settings (IACs and TACs). As the chip card and terminal undertake a number of interactions leading to a decision, these together with other chip-related parameters (floor limits, velocity counters, etc.) can lead to outcomes that require additional processing or unhappy customers. It is recommended that merchants simulate transactions with a variety of different card profiles.

While some merchant communities have succeeded in obtaining significant interchange discounts for compliance to chip and other payment system requirements, this stakeholder group is often cited for not always seeing the benefit of moving to chip alone. Merchant groups such as Tesco have positively supported chip and PIN because of the savings attributable to stationery, transaction times and merchant fee discounts predominantly

delivered by the introduction of PIN and POS in the UK and Ireland. Nick Mourant, Group Treasurer of Tesco, notes a payback in less than 12 months.<sup>6</sup>

### *Cardholders*

What is in this for me? Aside from the chip on the front of the card, I see no real benefit. In fact, I now have to leave the card in the device and I don't get the benefit of pre-swiping in the supermarket queue as I have done before. Why am I more protected now? I wasn't at risk if the transactions were fraudulent before!

In reality, few customers actually seek answers to these questions. If they see a transaction work, that is often sufficient. Yet the issuer and merchant community should consider these questions and the responses that they will make.

Unknown to the consumer, a magnetic stripe card with online PIN may have been blocked overnight owing to failed PIN entries, but now the chip card is blocked until he/she can get to an ATM, if the card has offline PIN in place. How does one communicate the difference between online and offline PIN to a cardholder? One does not.

The deployment strategy of issuers can be a major impact on cardholders. Many are not expecting their card in a forced re-issue model, and some issuers may have changed the PIN in parallel with the chip card issuance, further inconveniencing the cardholder.

Best practice remains with keeping customers well informed and, above all, not creating actions that they were not expecting. Success relies on looking after the customer. The customer experience is where the media will focus. The UK witnessed several misinformed journalists going to print — resulting in the industry having to pick up the pieces with confused

customers and managing call centre loads.

Consequently, clear and concise customer messages and cooperative industry engagement on common practices for the POS will provide for a smoother transition and one that supports a more rapid adoption of any new procedures by both customers and merchants.

### *Payment schemes*

It is arguable that, without payment schemes, EMV would not exist. Yet, in undertaking an EMV migration, it is very important to remain actively engaged with the payment schemes as an issuer, acquirer and as a major merchant group. Their early support throughout testing and certification will benefit the initiative and provide insight into other market developments.

At the same time, it is important to validate requirements and to engage broadly with the vendor community to ensure that one is delivering what is right for the organisation and that it is not over-engineered.

Some existing market practices may be outside the standard recommendations of the payment schemes. In situations where PIN bypass is available on all transactions or the ability to link cards to multiple bank accounts is supported, some of the risk settings on both card and terminal may need to be altered to avoid negative impacts at the POS. Stakeholders should be always willing to challenge each other in ensuring the best solution is delivered that supports international interoperability, yet can address domestic requirements.

### **A consideration for offline processing**

In a number of markets and for stakeholder groups, the idea of allowing offline decisions between the chip card and the POS device is foreign and certainly concerning. Yet, offline transac-

tion authorisations are a benefit of EMV. The full benefit is not achieved unless all aspects of the transaction that can be undertaken offline. Three fundamental aspects of a chip card interaction with the payment terminal include

- card authentication method or CAM
- cardholder verification method or CVM
- payment authorisation.

Each of these three aspects of card to terminal interaction could require an on-line connection. Herein lies a point of challenge for issuers. While EMV positions the issuer as the dominant party in what should happen at the POS, they are still not able to dictate that a transaction should stay offline. The Terminal Risk Parameters set by the merchant acquirer will also come into action. Further, the ability to support an offline CVM requires either signature or an offline PIN stored on the chip card.

#### *Practical offline PIN*

There is a lot of market debate about offline PIN and the impact on cardholders who do not have offline PIN on their card when travelling overseas. Much of this emerged from the migration in the UK, where PIN was not used at the POS prior to the migration to chip. The introduction of offline PIN only at UK POS allowed the industry to introduce PIN to its cardholders for POS transactions without the need for investment in the passing of PIN blocks in online authorisation messages.

Offline PIN also receives media attention around security which is dependent on the chip capability selected by the issuer. At issue is the manner in which the PIN is stored on the card chip, ie plain text or encrypted. Fundamentally, offline PIN is a great attribute for EMV, but it

comes at a cost to the issuer and the consumer.

If offline PIN is offered, it must always remain synchronised with the host-based online PIN used at automatic teller machines (ATMs) or, potentially, where offline PIN is not available at the POS. If the cardholder is able to change the PIN, this must occur at a secure, card-present device, namely an ATM or in-branch terminal. In both cases, this is a major investment for the issuer, where they have control of either or both of these channels. For mono-line card issuers, it is often more problematic unless there is a market-wide PIN reciprocity agreement in place. This would allow any cardholder to use any nominated device for PIN maintenance. This was delivered in the UK.

The last impact of offline PIN relates to exceeded PIN tries at the POS. Often with online PINs, the card will be blocked for up to 24 hours and, so long as the cardholder is able to recall their PIN, would be available for use from that moment. In the case of offline PIN, once the chip is blocked, external intervention is required using an EMV script and PIN maintenance services at an ATM or branch or the alternative card re-issue.

Offline EMV transactions provide for significant operational and financial benefits; however, they require thorough consideration by an issuer before executing this type of payment authorisation strategy.

#### **RECOGNISING THE IMPACTS: ESTABLISHING MIGRATION**

While each market may have a different driver for migrating to EMV, the impacts and benefits to each stakeholder are similar. Payment card fraud is a global issue, and recognising the cross-border nature of this in both card-present and card-not-present transactions is essential.

### Obtaining project approvals

Fraud migration is real, and engagement with scheme risk management will highlight the trends in this area on targeted retailers who continue to make floor limits available for magnetic stripe transactions. While the magnetic stripe of a chip card can be counterfeited, its abuse is restricted to markets that potentially ignore certain Track 2 data elements (Extended Service Codes) and who may process transactions offline.

Reputation impacts tend to be towards the end of a market migration. The New Zealand market witnessed some activity in the press prior to Christmas 2007, and it is anticipated that this may resurface during late 2008. The UK Chip and PIN Programme had provided for the naming and shaming of organisations that were failing in their support for EMV — including vendors — yet this has not been a widely adopted strategy.

Markets that have ignored the payment scheme liability shift trigger provide a challenge and an opportunity to stakeholders who have chosen to absorb the risk associated with these liability shifts. The US remains extremely visible in its view against EMV adoption, yet is positioned between two emerging EMV markets in Canada and Central and South America.

If incentives are available, they are valuable if there are limited active chip participants at play in a market and the company holds strong market share. This may be worth pursuing; it is worth investigating any scheme's expiry plans for their incentive programmes. It is often the early adopters who gain most from the interchange-based incentives, as the value is dependent on low EMV adoption by the opposing stakeholder group; that is, issuer versus acquirer.

Using EMV as a foundation for innovation in payments has been evident

in some migrations. These opportunities should be considered, if only at the early planning and strategic direction phase of the initiative. The incremental cost to implement all or parts of a value-adding proposition at the same time as EMV may provide the point of differentiation and return a business is seeking. As an example, securing a positive business case and approval for a standalone contactless EMV project may be difficult, so it may be more effective to integrate development into the overall EMV programme.

While a strong business case for EMV is not always evident, measurable benefits are available. EMV does not have to be viewed as a compliance project — especially as it falls outside the scheme compliance release schedules. With the current pressures on the payments systems, including declining interchange fees, Payment Card Industry Data Security Standards (PCI DSS), increasing cross-border and card-not-present fraud levels; the industry seeks tangible benefits from new technology and processes.

While many markets do not have fraud levels like those witnessed in the UK, this should not be the sole reason for deferring a migration to EMV. Fraud mitigation is a fundamental aspect of any EMV business case. National statistics for many countries are readily available. For international scheme-based payments (Visa/MasterCard), the introduction of chip has also seen a shift to PIN as the preferred cardholder verification method at the POS, adding lost and stolen fraud benefits to a business case.

Calculation of the fraud benefit should account for domestic and cross-border fraud for both card issuers and merchant acquirers. While there are recognisable fraud benefits, however, other types of fraud may increase as a result, namely card-not-present, card-not-received fraud and even other payment products, in-

cluding cheques on credit card accounts. The latter two were evident during the mass market migration in the UK over 2004 and 2005, in particular where issuer strategies for card activation may have addressed some of this fraud volume.

Where there is an appetite to combine additional functionality into the core EMV migration project, consideration of MasterCard's Chip Authentication Programme (CAP) or Visa's Dynamic Passcode Authentication programme (DPA) to target card-not-present fraud may be a timely option.

The success of card-not-present fraud propositions is now very much dependent on the adoption of mobile phone-based alternatives that disintermediate the card-based models for two-factor authentication of online and Mail Order Telephone Order (MOTO) transactions.

With a focus on timing, infrastructure investment cycles and the appetite for risk, an organisation may be able to address a number of strategic imperatives on the back of the EMV infrastructure development. In seeking to benefit from EMV, stakeholders who have seen an opportunity to invest incrementally have recognised the effort to migrate and seek to minimise future development efforts. While adding risk to the core project, a considered and timely chip marketing strategy may pay dividends in the future through market differentiation and an ability to respond to market dynamics rapidly.

Revenue opportunities may arise for early adopters in particular. Some first-to-market stakeholders have used chip as a strong marketing tool for enhanced acquisition rates of cardholders or merchants. As the market matures in its adoption of EMV, the laggards have in the past been targeted by the media and consumer groups, leading to a potential impact on market reputation. Clear

customer communications are important throughout for all parties.

Like fraud benefits, additional chip functionality may drive incremental revenue towards an organisation. It is recommended that an individual assessment of cost/benefit for each proposition is carried out accounting for deployment within the EMV migration or at a future time.

In making this decision, organisations should be cognisant of the numerous failed initiatives that detracted from a core deliverable or could not agree a suitable commercial framework for engaging with third parties. Past examples include chip-based rewards, stored value, authentication services and ticketing. The demand for chip-based loyalty is low, yet it is ideally suited to markets with poor or expensive telecommunications and deserves a strategic review under these conditions.

### **Delivery considerations**

EMV migrations are, by their nature, a significant investment on technology and resources. Card issuing projects have timelines stretching from as short as four months to longer than a year, while merchant acquiring initiatives are often longer owing to their complexity and need to support many variants of card on issue.

In markets where the business case is seen as difficult to achieve, issuers will often follow a phased and light investment strategy in an effort to issue chip cards as a minimum. To this end, both Visa and MasterCard continue to support issuers with an 'Early Data' host development option that minimises project cost, timelines and development impacts, while still delivering chip cards to market.

Acquirers, however, must now implement 'Full Data' support for EMV transactions which places the burden of

investment on this side of the payments model. Early or Full Data refers to the ability to manage partial or all incremental chip data in a transaction message including cryptogram validations.

Careful planning, strategic thinking and sourcing strategy can substantially change the look of a business case and the success of EMV migration. There is a strong case for inclusion of subject matter experts in an initiative, to avoid the pitfalls of earlier deployments and to ensure that the agreed strategy fits with an organisation's technical and operational framework.

The business of issuing a chip card has operational impacts that could 'blow' the budget if implemented in an uninformed way. Equally, merchant acquiring initiatives could have grave impacts on customer transactions if exception handling has not been considered.

The opportunity to over-engineer the solution based on available products and solutions is high. A major factor is an uninformed stakeholder who has not been advised of the alternatives available for compliance to EMV. It is often difficult to see through the interests of vendors and the payment schemes as they seek to protect their margins and continue to seek market share and visibility. Remember, EMV is no longer new.

There are four key delivery areas for an EMV migration: cards, host systems, payment terminals and the deployment itself. Each area requires consideration of a number of factors as a company plans its migration to EMV.

The interdependences of one decision on another are complex and can mean the difference between a future proof deployment and one that requires reinvestment. The objective in looking at cost considerations pragmatically is to minimise the exposure to an over-engineered deployment and to recognise the status of competitors and the market as a whole.

### *Chip cards*

The card is often the critical path for an issuer. While the finished product looks innocent enough, the impacts to the issuer when changing to chip are far more complex. One task that often brings an initiative unstuck is the card design. Many incumbent designs require a change to become chip compliant. This may mean moving a company logo or modifying an image that would otherwise be covered by the chip. Issuers with third-party card agreements will be largely affected by this area. In each case, the project timeline and cost base is affected as each card design is submitted to the payment schemes for approval and old stock is written down as obsolete.

A subtle yet relevant consideration is the colour of the chip contact plate to suit the card design. Issuers are not limited to gold coloured chips alone. Palladium is often better suited to card artwork outside gold cards. Vendors may seek additional charges for palladium over gold contact plates.

The card plastic will also need to be altered in thickness to support the process of milling a hole in the front to embed the chip. The international standards organisation specifies these requirements under ISO 7810 as  $760 \pm 80$  microns. For chip cards, it is advisable to ensure that the base plastic card is in the upper regions of this specification.

Inevitably, it is the chip that will drive the cost of the card, and this is from three attributes: memory, security and operating system. Much like buying a laptop computer, there are several options and configurations available to select from.

Figure 2 provides a simplified view of the issues a project is faced with when selecting a chip solution. The industry referenced EEPROM (Electrically Erasable Programmable Read-only Memory also known as 'E-squared') will

EEPROM
ROM
Operating system

*Figure 2 Simple view of a chip*

drive the cost of the chip. A smaller EEPROM memory should be the goal. Unless a bank card issuer is seeking to add significant value added services to their card, it is unlikely that there would be a need for anything greater than a four kilobyte memory.

Higher memory chips have been used in banking. In some cases, these have not been driven by any additional functionality for the cardholder, only to accommodate the minimum capabilities of the operating system, such as Java card, or the minimum security domain to be supported by the issuer or the domestic industry.

While some issuers selected highly specified chips to support adding or deleting services from the chip while in the customer's hand, the infrastructure to support this often prohibits such a strategy becoming reality outside a very few exceptions in banking.

It is now a choice of operating system which fall into two categories — Open (Java card and MultOS) or Proprietary operating systems from independent card vendors. The choice of operating system at this time is arguably a reasonably moot point for most traditionally conservative bank card issuers. Off the shelf solutions generally include pre-loaded applications for Visa or MasterCard payments and often with both in the memory. This allows an issuer to source a single chip that may be embedded into either Visa or MasterCard plastic, further reducing the

operational and financial burden for dual card scheme issuers.

Other applications are also available alongside payment, including rewards, data storage or authentication. This equates to a static multiple application product, which provides for a wide choice of chip solutions compared with dynamic multiple application referenced above that could support post-issuance downloads of applications (add/delete).

Security debates surround Static Data Authentication (SDA) versus Dynamic Data Authentication (DDA) capable chips. The distinction is the additional processing capability of a DDA chip owing to the inclusion of a 'crypto-coprocessor'. While DDA is more secure, it comes at a higher cost and higher memory requirement compared with SDA chips. Both SDA and DDA support multiple applications, but only DDA allows for the dynamic add/delete of applications in a post-issuance environment. The objective of this paper circumvents the ability to provide more detail on this area, other than to inform the reader that this can be a significant area for over-investment.

An issuer is not likely to derive additional benefit by issuing a DDA chip card during their first issuance cycle if the payment terminal rollout remains low. The value of DDA is apparent where a mature chip POS environment exists. The reality during a migration is an initially low volume of chip-on-chip transactions, resulting in the ongoing experience of

magnetic stripe transactions, making the DDA investment expensive at this stage.

To add complexity to the mix, a new Common Payment Application (CPA) has been specified by EMVCo to support dual scheme issuers. This latter offering is in line with a new initiative sponsored by EMVCo called Common Core Definition. The vendor community has responded with a single chip solution with both VSDC and M/Chip as noted earlier, continuing to disintermediate the deployment of CPA-based chip cards at this time.

In concluding with the laptop analogy, the chip can be preloaded with applications to support the requirements for payment or other functions. The best solution is to ensure that these are stored in the ROM area of the chip (Figure 2), again reducing the need for a large EEPROM memory. The standard applications are VSDC for Visa or M/Chip for MasterCard.

#### *Payment terminals*

Retailers and acquirers must be able to support most combinations of cards on issue. To this end, the development effort, testing and certification of their solution is a significant exercise. Some hardware solutions are not suitable for compliance to EMV owing to the lack of a chip reader, their slow processing capabilities (less than 32 bit, which is a significant issue when processing DDA-based EMV cards) or lack of memory or security requirements. Where a full hardware upgrade is triggered by EMV, it will significantly affect the business case unless the normal business operations of amortisation and hardware upgrades can be used to disburse this cost.

In either case, the software impact is similar. POS devices sourced from the key industry suppliers will have off-the-shelf solutions for EMV. The challenge comes for multi-lane retail environments and

integrated POS solutions. With a focus on speed and the introduction of PIN for Visa and MasterCard transactions, sourcing of new hardware solutions may also need to factor in portability of devices, for example in restaurant environments where patrons will also include tips as part of the transaction.

Incremental cost decisions on POS solutions will include the capability for contactless transactions now or in the future. With a number of plug and play contactless reader solutions available and new fully integrated devices, one strategy is to ensure that the software upgrade for any legacy terminal infrastructure and message formats includes requirements for contactless payments.

In deploying the payment terminal infrastructure for chip, the degree of testing required ahead of payment scheme certification should not be underestimated. Equally, a sound understanding of the TAC settings and their impact on transaction behaviour is critical in identifying where exceptions are likely to be derived and how to respond to them, particularly when the device is unable to go online when requested.

For completeness, the ATM should not be immediately ignored from scope. This channel can be an important part of any PIN management strategy for chip card issuers where they decide to issue offline PIN. Importantly, ATMs do remain a target for counterfeit fraud rings globally, and chip compliance may need to be a consideration. The owners of ATM network should also consider the revenue opportunity in offering PIN maintenance services in a reciprocal environment rather than using this as an exclusionary tactic to support related card issuing business.

#### *Host systems*

This is an area that distinguishes the impacts on the issuers versus the acquirers.

In most regions (there remain some exceptions), both Visa and MasterCard ask that acquirers and merchants who self-acquire implement for full EMV data on their hosts and network links. This is known as Full Data mode or Full Option mode acquiring.

With no real options available to this side of the payments model, it is essential that they are able to align their developments when supporting multiple card schemes. Can a project support upgrades for Visa, MasterCard, American Express, JCB and any dependent domestic debit scheme arrangements in one initiative? Unfortunately, in some markets, such as Australia, there will be a need to revisit development to support future chip rollouts for payment schemes outside Visa and MasterCard.

Acquirers should also consider data storage for future disputed transactions and the need to respond to advice requests from issuers. Acquirers are additionally required to support 'scripts' sent from compliant issuers to their cards that may change the risk settings on the chip in a retail terminal. The reporting and customer servicing needs of the business should be given priority, as they will underpin the success of the initiative at deployment.

Issuers, however, continue to have the ability to implement only Partial or Early Data mode on their host systems and, consequently, rely on arrangements with Visa or MasterCard to provide services that convert a chip transaction to almost magnetic stripe-like data formats.

For an issuing organisation keen to have cards issued, the partial option is very attractive. It provides a low-cost speed to market, but with some areas of compromise.

In this model, by arrangement with the appropriate payment scheme, the scheme will see the transaction authorisation tar-

geted for the issuer and will remove the additional chip information and pass through a magnetic stripe looking request.

The impact of this model at the moment of transaction will be dependent on the chip settings and ensuring that approvals are accepted from the issuer even though expected chip data is not returned to the card.

A further consideration for Early data issuers is the inability effectively to send 'scripts' to the chip during an authorisation to change risk parameter settings or to block the chip.

It is important to note that the card itself is agnostic of the host's capability. Hence, an issuer could choose to upgrade their host fully for EMV in the future without affecting existing cards on issue.

Third-party solutions are also available for issuers to consider, which in essence leaves an issuer's legacy magnetic stripe authorisation platforms untouched. This model also alleviates the requirement to engage the schemes to provide on-behalf-of services to remove incremental chip data.

Ultimately, an organisation derives most value in a mature chip environment from full EMV data. While issuers may be able to defer major effort on authorisation and risk systems, the card management system generating embossing files to the card vendor cannot.

It is recommended that the decisions for the scope of host system changes are set against a concise marketing and risk management strategy that identifies areas that would be affected as a result of limiting the upfront investment on EMV.

### *The deployment*

The UK witnessed a 'big bang' approach to deployment, with millions of cards and PIN mailers in the post on a monthly

basis. While, on the one hand, it accelerated the maturity of the market for chip-on-chip transactions, it significantly exposed the consumer to card intercept fraud and account takeover.

Operationally, the forced re-issue of a card portfolio can be difficult to coordinate where the card vendor has limited capacity together with the overhead of card expiry levelling to smooth out re-issue bubbles in the future. While there may be financial benefits achievable with a higher chip card volume on issue, the impact on the customer must be foremost. Are they expecting a new card and PIN? Has the company changed their PIN? If yes, will they be able to conveniently change it if they wish to?

The deployment of POS devices and upgrades is limited to the availability of resources to install, train and support the vast array of retailer communities that exist as the end customer. The timing of this deployment may also be affected by vendor challenges where a significant market share is held by one or two suppliers.

It is important during the deployment phase that regular and detailed reporting is generated to identify rapidly any acceptance issues or failures. Look for trends in transactions for faulty devices and significant levels of fallback to magnetic stripe at chip-enabled devices as only some examples.

A recommended strategy prior to and during the deployment is to establish a central reporting/help desk email account (eg SmartLine), which allows customer service staff to report customer issues and feedback to the project team. During these phases, the project team should respond as the subject matter experts and use the data for future testing and training material development.

Driving towards a common market ap-

proach for media and communications is strongly recommended to the extent that consumers are able to establish consistency at the transaction moment. Linked to this is the ability to move all market participants to EMV over an agreed, yet relatively short period. Failure to do so will only retain inconsistent POS experiences for cardholders and retail staff and delay the full benefits of EMV.

## CONCLUSION

Delivering an EMV migration with positive impacts on customers and retail staff should be an essential pillar of a project's objectives. Notwithstanding this goal, the migration to EMV will deliver impacts on all stakeholders owing to procedural changes, the vast array of configurations for risk parameters on the chip or device and the constrained scope of the EMV specifications at the point of transaction.

Consequently, it is incumbent on all organisations moving to EMV to be aware of the impacts and to address these through industry collaboration, testing and effective communications. As noted at the start of this paper, EMV is not a standalone technology project; it has the capacity to be a complete change management exercise.

## REFERENCES

- (1) [www.emvco.com](http://www.emvco.com)
- (2) (April 2007) 'Security A Strategic Advantage for CB', *Expertise CB. The Newsletter of Groupement des Cartes Bancaires CB*, p. 3.
- (3) 'The Migration to Chip & PIN', Visa Canada, Financial Services Technology Forum presentation, 24th October, 2007.
- (4) *Ibid.*
- (5) *Ibid.*
- (6) Arnfield, B. (2006) 'Selling Smart Cards to Canada's Merchants', *Card Technology*, June.