

## **EMV: How might the investment be reaped**

### **EMV: Chip Level 1**

Those in the industry who went through the cost and effort of EMV migration during 2004/2005 and those who are either still in the thick of it, or preparing to embark on it, will know how it impacts the whole transaction lifecycle. EMV stands for Europay/Mastercard Worldwide/Visa International standard for chip and PIN implementation. This standard came into effect formally across the EU region on 1 January 2005 although many countries are still way behind in terms of the percentage of credit cards migrated (Spain 0.8% Italy 2%, Portugal 2%, Germany 10%). Other regions have implementation dates ranging from January 1<sup>st</sup> 2006 to January 1<sup>st</sup> 2010.

### **Acquirers**

For an acquirer, quite simply everything, from message protocols to terminal download processes and from interchange qualification routines to scheme file generation is affected. All POS and ATM terminals in the field have to be either upgraded (in many case both hardware and software) or replaced. Authorisation host systems have to be enhanced, retested and recertified with the schemes. Batch processing systems have to be modified to handle new data elements and to ensure that clearing transactions are properly processed to avoid interchange downgrades or worse still, rejects.

### **Issuers**

For issuers, the changes are also very far reaching. In most cases, a total overhaul of card issuance technology and security practices has to be undertaken, then there is the mammoth logistical task of card re-issuance, and enhancements similar to those needed on the acquiring side have to be performed on authorisation and clearing host systems.

In the lead into all the activities described above there is the task of sourcing appropriate test tools and preparing test environments in which all this new functionality has to be thoroughly exercised before certification with the card schemes.

### **Benefits**

All of this was done in the EU region in an effort to tackle the growing fraud losses associated with the counterfeiting of magnetic stripe cards. By all accounts; where EMV has been implemented, it has worked. Taking the UK as an example, which along with Belgium, Ireland and Luxembourg had by mid 2006 converted in excess of 95% of its credit cards to EMV, the results are impressive. Fraud losses on lost and stolen cards 2005 v 2004 had fallen by over 30%!

## **So, is that it then?**

There is a popular misconception abroad that once all non EMV cards and terminals are decommissioned the job is done! The truth is that in terms of Chip and PIN accomplishing its full potential, nothing could be further from the truth.

## **The Economics of EMV**

As mentioned earlier, the core objective of EMV was to address a serious and growing fraud problem. Historically, the bulk of financial losses sustained through cardholder fraud were borne by issuers so clearly they had the most to gain from the introduction of chip and PIN. On the other hand, the cost and effort of delivering on EMV referred to earlier does n't come cheap and it does n't end there. Some sources estimate that it costs at least 30 % more to produce and deliver a chip card to a cardholder as compared to a magnetic stripe card. Others put the cost of producing a chip card at somewhere between \$1 and \$3 dollars compared to 13 cents for its magnetic stripe counterpart. Whichever you believe, the incremental cost is considerable.

On the acquiring side, early adopters insulated themselves from what is called the "liability shift" – a principle whereby a non-EMV compliant acquirer would be automatically liable if the issuer party to the transaction is EMV compliant. As adoption of EMV among issuers and acquirers grows both domestically and regionally, the "liability shift" benefit is diminished and ultimately eliminated. Beyond this, the other benefit to the acquirer is the reduction in interchange pay away on EMV transactions versus non-EMV transactions. On this point however, due to merchant funded EMV investment (among large merchants owning their own POS systems), the increased awareness by merchants of scheme interchange and the consequent demand for transparent and unbundled pricing, the acquirer has ended up sharing up to 50% of this interchange reduction with the merchant. On the cost side, acquirers have had to shoulder the cost burden of the systems changes referred to earlier and the terminal and ATM upgrades/replacements.

So how might returns be achieved on this rather large investment which for some (particularly acquirers), will take a very long time and may not be very significant?

## **Benefits waiting to be leveraged**

One of the expected benefits of embedding data and intelligence securely into the chip and placing it on the card was that transactions could be carried out off-line without incurring the time and telecoms cost of going on-line. The principle here was that the card and the cardholder could be authenticated totally off line through the use of

public/private key technology. Whilst this solution addressed the fraud (counterfeit, lost and stolen) issue it did not address the credit risk issue i.e. does the cardholder have enough available credit.

### **Issuer Scripts on the Chip**

Conceptually, the credit risk concern can be addressed easily, using a core capability of the chip to store multiple applications. One of these is the ability to receive and store scripts or pieces of data which can be referenced to make the credit risk decision. These credit risk parameters are basically transaction counts and amounts, generated by the issuing banks credit risk systems which when stored on the card can instruct the terminal to complete the transaction offline. When the transaction counter is decremented to zero the terminal knows that it now must go on-line for authorisation. During this process, the issuer can refresh the credit risk parameters on the card such that the card can continue to be used offline for transactions up to a certain value.

So why, since this would deliver tangible cost savings for issuers and acquirers on their telecoms bills and in reduced demand for CPU resources, is this not happening? The truth is that given the challenges presented by the introduction of chip and PIN for card and cardholder authentication, the industry simply could not accommodate the added complexity, cost and time of supporting issuer scripts. Of the 3 factors mentioned – complexity, cost and time, the writer suspects that the later was the key impediment.

The wider impact of supporting the risk management scripts beyond simply sending the data to the terminal should not be underestimated either. Card and risk management back office systems need to be analysed to ensure they can interface to the terminal management systems to provide the data in an accurate, timely and reliable fashion. While most card issuers now possess sophisticated on-line risk management and behavioural scoring systems, not very many have looked at this area in any depth.

### **Value add applications**

There appears to be a growing view in the industry that if tangible and appreciable returns are to be obtained from the investment in EMV they will be reaped from the capability of the chip to house many applications. In the same manner in which a risk management application can reside on the chip, so too can prepaid products, loyalty schemes, tolls systems, parking and transportation applications, medical records ..... the list is endless. Up to now these areas have not been core competencies of banks charged with the task of embracing chip and PIN, but this may change.



## Conclusion

**If ROI beyond the immediate gain outlined above is to be achieved, issuers will have to utilise the huge potential of the Chip to host multiple applications. This may be achieved through alliances forged in some of the industries/industry segments mentioned above (transportation, loyalty, medicare). In the short run however, there is an immediate need to implement risk management scripts to benefit from savings accrued from off-line processing of cardholder authorisations.**

**If you would like to comment on this article or find out more about O-C Group please contact us at [info@o-cgroup.com](mailto:info@o-cgroup.com) or visit our website: [www.o-cgroup.com](http://www.o-cgroup.com)**