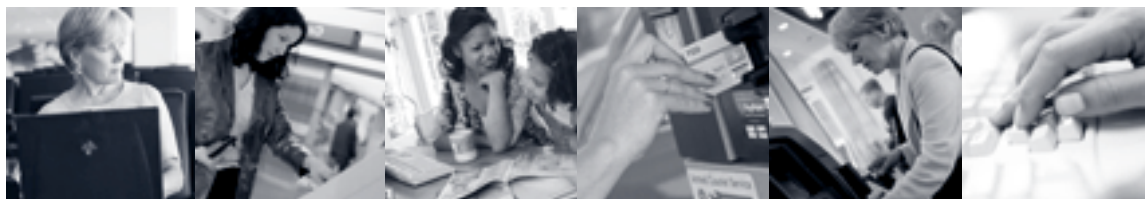


Dynamic Risk Management with EMV Data

Researched and authored by Jane Adams, freelance journalist, on behalf of ACI Worldwide

July 2006



In 2005, the first full year of chip and PIN use in the UK, British card fraud fell 13 percent. As the British retail banking sector based their investment in EMV on a fraud reduction business case, they could rightly be pleased. Nonetheless banks could be missing out on a big opportunity because EMV contains considerable potential for additional fraud reduction that will enable them to keep up with ever-changing fraud patterns and activities.

Fraudsters continually refine their activities in response to industry countermeasures. In the early stages of the introduction of the UK's chip and PIN scheme, while banks were rolling out new cards, fraudsters concentrated on mail interception fraud. With the UK rollout complete, they are now focusing on card-not-present fraud – primarily mail order and telephone order which is even more vulnerable than e-commerce – and on exporting fraud activities to countries which have not yet completed an EMV rollout. And as the £1million skimming fraud at UK Shell petrol stations discovered in May 2006 shows, chip and PIN is not 100 percent impervious while cards still have magnetic stripes.

“It’s probably true that EMV data has not yet been used to its full potential,” says John Griffiths, senior manager, fraud department, Visa Europe. “Maybe that’s because it’s early days but at Visa we’re interested in rolling out EMV and we’re interested in leveraging it as far as possible.”

It’s not as if some of the newest frauds are that difficult to perpetrate, even in an EMV environment. To make an EMV card fallback to using the magnetic stripe, the fraudster need only damage the chip. A service code rewrite means simply rewriting or replacing the magnetic stripe, and card-not-present fraud bypasses the chip or magnetic stripe entirely.

Data - EMV's Biggest Asset

Clearly banks need to stay abreast of the newest frauds and their remedies. Strange then that so many so far have overlooked one of EMV's biggest assets – the data generated by EMV transactions. The standard EMV smart card contains a wealth of currently unexploited data. “There are around 50 pieces of EMV data on the chip and they are all concerned with risk management,” says Gareth Ellis, senior solutions consultant at leading enterprise payment solutions provider ACI Worldwide. Analysing this data could help beat fraud.

“It’s probably true that EMV data has not yet been used to its full potential,” says John Griffiths, senior manager, fraud department, Visa Europe. “Maybe that’s because it’s early days but at Visa we’re interested in rolling out EMV and we’re interested in leveraging it as far as possible.”

“This is about being proactive, moving things up the timescale and using risk management to control the valve in both an opening and a closing direction,” says Mike Hendry an independent payment systems consultant who worked on the UK's chip and PIN rollout. “It’s not only a prevention tool – EMV can also be used to give good customers more freedom to use their money.”

During EMV transactions, data about the transaction is generated from both the card authentication and from the cardholder verification processes, stored on the card and passed to the issuer host. But in general, for the use that issuers make of it at present, it might as well stay on the card untapped by fraud analysis. “It’s astonishing how many banks didn’t even check all the discretionary data on a magstripe transaction. Unless they are doing that, they haven’t got an earthly chance of learning to use EMV data correctly,” says Hendry.

EMV Data

Yet if this data were fully analysed by the issuer, it could be used to identify fraud patterns and credit risk situations, for post-authorisation checks and to enhance customer service.

“There are two types of data, from the current transaction and from previous transactions, on the card,” says Ellis. “Just one use of this data is to search for patterns of fraud that we have struggled to identify before by looking at the previous transactions that have occurred on this card.”

“Go back to basics and look at all the information we get in the card and terminal verification results and work out what those mean both singly and in combination,” says Hendry. He points out that a piece of transaction data that looks ambiguous alone, may, in combination with other data, point to fraud.

The sort of information that the card stores and passes includes:

- ▶ A note of whether offline static or dynamic data authentication has failed.
- ▶ How often fallback occurs.
- ▶ Whether there has been a service code rewrite.
- ▶ Incomplete transactions.
- ▶ Script processing has failed, where previously a card block script has been run.
- ▶ The authorisation request cryptogram verification (ARQC) has failed.
- ▶ A high number of repeated uses in unattended terminals.
- ▶ Evidence that merchants have repeatedly forced the card online because they are suspicious about the purchaser.

Many of these parameters concern offline transactions, which are particularly prone to fraud.

Acquirers Benefit Too

Acquirers equally may be interested to know that card data can highlight whether a particular merchant experiences a suspiciously high level of fallbacks or of PIN bypasses, suggesting a collusive merchant. “Acquirers can also be quite proactive in using data to determine how outlets are processing transactions and if they are processing them as intended. While the focus has always fallen on the issuer, the acquirer does have all that data and can gain quite a lot of useful information as well,” says Hendry.

At present, banks use EMV data to authenticate the card or check for fallback or see if the offline PIN has been blocked. “What most banks have done is to take their legacy magstripe processes and to map chip fields onto those magstripe criteria. That’s a real loss of opportunity,” comments Hendry. The card associations may also monitor some data – Visa for example has a compliance team that examines fallback data to look for suspicious activity.

However, not only could banks make more use of the information that’s already available, EMV also has the potential to generate further data. “In the future there’s potential to expand information about the offline transactions – that’s not being completely passed back at the moment,” says Ellis. “However what we’re trying to do at present is to exploit the information that is already there but is not being used.”

In the future ACI sees banks using this information with integrated fraud detection solutions that help card issuers, merchants, acquirers and financial institutions combat fraud schemes. These systems use user-defined rules and neural network technology using custom modelling techniques to reduce losses and limit an organisation’s risk exposure.

The new data could also help fraud analysts create rules to look out for new types of suspicious activity. ACI’s senior solutions consultant Michelle Trappitt used to be a fraud analyst with a major bank. “By passing EMV data you are able to provide newer or more complex rules to identify the latest fraud types,” she says.

Complex Fraud Needs Complex Rules

Rules using the limited amount of data currently analysed by banks may miss out on even standard fraud scenarios. “Lost and stolen fraud can be quite difficult to flag up with those sorts of rules because the transaction behaviour patterns of a fraudster can be quite similar to those of a normal person. So by having extra information fed to the fraud monitoring system you can pick up hard to detect fraud types,” says Trappitt.

At the same time, this means that the risk of flagging up false positives is also reduced.

Close interrogation of the data can allow analysts to build a detailed user profile, giving them a far better idea of the risk associated with a particular card. If they are unhappy with the level of risk they could, for example, lower the card’s floor limits. That means that banks don’t

EMV Data

just cut down on fraudulent activity, they can also tighten their control over legitimate cardholders using their cards in a delinquent fashion. That means reducing bad debt and operational difficulties.

“What analysts need is the ability to change profiles on the card in order to do credit risk management,” says Ellis.

A complete cycle of this process would be a two-way interaction with the card sending EMV data to an authorisation system. This sends EMV transaction data to a fraud monitoring system. Fraud analysts can then update EMV parameter values held in a smart card management system. Finally, the smart card management system updates data elements on the chip. “That’s the stage that gets me most interested - recognising that the card is meant to act as the issuer’s delegated authority at the point of sale. So what we should be doing is using and updating the on-card parameters to replicate the decisions we would make in the authorisation system. Therefore trapping more incidences before they happen so we get the first transaction and not the second or third,” says Hendry.

“EMV has a long history. People tried to put in there what they felt would be useful in future or that they found useful with other products, like electronic purses,” says Toni Merschen, group head, Chip Centre of Excellence, MasterCard International.

This can be automated even further by setting up user defined business rules in the monitoring system that automatically update chip parameter values after the firing of a particular rule.

So did the architects of EMV, working in the early to mid ‘90s envisage this sort of use of EMV data? “EMV has a long history. People tried to put in there what they felt would be useful in future or that they found useful with other products, like electronic purses,” says Toni Merschen, group head, Chip Centre of Excellence, MasterCard International. “The EMV standard is full of options and it offers a wealth of parameters that you can either use in the standardised way that the associations suggest or in a non-standardised way that your risk management or customer services department recommend. EMV is full of these things but in that respect, EMV deployment is still in its infancy.”

Why aren’t banks taking advantage of this data already? “UK issuers were 100 percent preoccupied with chip and PIN – get it running, get it working,” says Merschen. Retail banking analyst Clare Buckmaster of Datamonitor agrees. “Given that the [UK] deadline for chip and PIN was February this year, up until very recently, there hasn’t necessarily been that much for banks to gain by trying to take advantage of this data. They’ve been waiting till everything is in place and they are more likely to look at this from now onwards,” she says.

“This is something that the risk management guys are only now understanding – what the potential is in EMV and how they can leverage it, how they can customise it for their portfolio and segments in their portfolio,” adds Merschen.

In fact, there is already some interest in the UK, according to banking body APACS. Their spokesman comments, “Yes, banks are actively looking into using EMV data in this way. The primary reason for introducing the chip was to tackle counterfeit card fraud. But card issuers are aware that the memory capacity of the chip gives them the platform to use the chip in other risk management ways. This would be a commercial decision for each issuer to make on how they best utilise what the chip can do for them but our (APACS’s) view is that they are aware of the potential in EMV cards. Over time they will make more and more use of these features to control and monitor use of the card.”

Offline Data

One EMV application that already makes some use of data from offline transactions for risk management is MasterCard’s OneSmart Pre-Authorised, which forms part of MasterCard’s MChip4 EMV implementation. It uses EMV parameters to set money aside for offline usage. “MChip4 is a richer product. The constructs that support pre-authorized are built on EMV but are MasterCard specific. It is fully EMV compliant but it is a little richer in its elements,” says Merschen.

When the card goes online, the issuer looks at the behaviour and cardholder attempts to make offline transactions to a preset limit. “The whole story with pre-authorized is that it starts low and then you see that the customer behaves,” says Merschen.

For banks who have not yet implemented EMV, leveraging this chip data during the rollout can make a big difference to managing changing

EMV Data

fraud patterns. For example issuers could reduce and maybe even avoid the 62 percent increase in mail intercept fraud that the UK experienced during the early part of its rollout in 2004; although, as Visa's Griffiths points out, banks in some countries may not mail out cards. Fraud in each country will therefore vary according to banking practice. Banks could also look carefully at occurrences of fallback during the rollout phase. After all it's easier for the fraudster to attack the magstripe. "For any given fallback transaction people should try to understand why it has happened in fallback mode. But they are simply looking at it as an acceptable magstripe transaction," says Hendry.

So with fraud still a top concern for European banks, where will EMV take fraud management? As the Shell fraud shows, fraudsters are becoming more and more ingenious and banks have to be increasingly on their guard. Increased use of EMV data can only help improve risk management. As ACI's Gareth Ellis says, "To get the most out of EMV, issuers should be talking to their fraud analysts and risk managers to understand how EMV data could better meet their needs."

ACI Worldwide

Whether you need an end-to-end solution to meet EMV mandates and enhance transaction security, manage your smart card portfolio, or enhance your authorisation services to help you deliver greater value to your customers, ACI Worldwide can help.

The ACI Payments Framework™ delivers a suite of products for all aspects of payments processing, which integrates with existing environments. Components of this framework will enable a flexible infrastructure to take full advantage of the fraud control and business opportunities presented by EMV, both today and in the future:

ACI Proactive Risk Manager™

- ▶ Fraud detection across institutional business lines and customer accounts
- ▶ Risk analysis
- ▶ Real time or near real time options
- ▶ Expert defined rules and/or neural network technology
- ▶ Case management for business process creation and
- ▶ System integration

BASE24-es™

- ▶ Multi-platform, electronic payment transaction processing
- ▶ Real time authorisation of transactions
- ▶ Flexible authorisation decisions (for example based on merchant category code, region or cardholder)
- ▶ EMV parameter update process management

ACI Card Management System™

- ▶ Full cardholder and merchant management
- ▶ Support for EMV cards
- ▶ Support for pre-authorised debit

ACI Smart Chip Manager™

- ▶ Chip card issuance, starting from single-application EMV to any level of sophistication
- ▶ Application, personalisation and parameter data retained for future real time updates or reissuance
- ▶ Central repository of EMV parameter updates for real time
- ▶ Delivery via payment engines