



AN ACONITE WHITE PAPER

**Exploiting EMV Risk
Management**





Introduction

Successful card issuing, like any other aspect of the banking industry, is about managing risk. 'Managing' does not mean 'eliminating' risk (impossible anyway) since in the business of advancing credit, the gains can be proportional to the risk taken. The objectives are to maximise revenue while minimising losses and the cost of managing the portfolio. The successful card issuer uses all the tools available to achieve these goals, and the introduction of EMV smart cards adds significantly to that toolkit.

EMV introduces features that control how cards behave. EMV allows the card issuer to control the outcome of transactions that may be completed off-line and to modify the way the card will behave in future.

The true value of EMV

Ask people in the cards business what EMV is all about, and the reply invariably concerns fraud and security. While it is true that fraud prevention – attacking the use of cloned, counterfeit and stolen cards – formed the initial justification for the migration to EMV in markets where card fraud was (and in some cases remains) prevalent, such as the UK, it is in the potential to control risk where EMV's real value will be realised. Many card issuers have so far neglected this opportunity and have yet to understand the potential for EMV to deliver significant bottom-line benefits.

Migration to EMV has been seen as a technology led initiative and has been sponsored by IT and/or compliance departments. Risk managers have largely been left out of the loop. That situation is now changing amongst switched-on card issuers.

Old versus New World

In the world of magnetic stripe cards, an issuer's ability to control how their cards are used is severely limited and once the card – a passive token – has given up the information stored in the magnetic stripe, it (and the issuer) plays no further part in the decision making at the terminal. A transaction will be sent online for authorisation only if terminal rules dictate. Card issuers have little or no influence on the content or application of those rules; guidelines for terminal floor limits and random selection for authorisation may be adopted at scheme or association level, but acquirers and merchants can (and do) manipulate these 'rules' in the search for competitive advantage over other acquirers and merchants, balancing this advantage against the risk of chargeback. The interests of card issuers come some way down their list of priorities.

Giving Issuers Control

EMV smart cards turn that situation on its head; the card becomes an active component, giving the card issuer a controlling presence at the point of service. The decision to go on-line for authorisation is taken away from the terminal, and therefore away from the acquirer. Most importantly, the card issuer can dynamically control card state and behaviour through EMV scripting – post-issuance updates to the card that are sent as part of the response to an on-line authorisation request.

Credit and Debit Risk Management

The objectives of card risk management differ between the credit card business and debit card issuing. Credit cards offer revolving credit up to a limit with a minimum monthly repayment whereas debit cards are intended primarily as current (checking) account access devices, although borrowing up to an overdraft limit may be allowed. The credit card issuer wants to maximise the level of borrowing whilst ensuring that the cardholder is able to continue making the minimum repayment. The debit issuer wants to keep the account "in order" and to balance customer service against the risk of unauthorised spending which may lead to bad debt.

So the card issuer faces a dilemma; revenue, directly and indirectly, is driven by card usage, which must therefore be encouraged; risk, which ultimately leads to those write-offs, is introduced by unauthorised card usage, which must therefore be prevented. Unfortunately, card usage does not take place in a perfectly controlled environment; depending on the territory, a certain proportion of transactions will take place at off-line devices. In markets where a significant proportion is off-line, such as the UK, the exposure to risk and therefore potential bad debt is much greater.



Trend to Off-Line

However, the trend in the global market is towards more off-line transactions. Indeed, the ability of merchants and acquirers to expand card usage opportunities is, to an extent, dependent on a growth in off-line devices forming a major part of that expansion, GPRS, Wi-Fi etc. notwithstanding. This is especially true in markets where the telecoms infrastructure is either expensive to use (e.g. Europe), unreliable (Middle East) or non-existent (large parts of Africa). The ability to perform secure off-line transactions – genuine card, genuine cardholder – will lead to significant growth in card usage in areas such as vending and ticketing and where low value payments make it uneconomic to go on-line for authorisation.

EMV provides some resolution of this dilemma by effectively extending a part of the card issuer's authorisation processing from their host systems onto the card and into the device. The issuer is now represented at the point of service and can therefore implement elements of their risk management policy at the card level, on a card-by-card basis.

Dynamic Risk Management

The mechanisms that EMV provides for risk management, as opposed to fraud prevention, have been augmented by the card schemes' own features and are largely based on controlling the amount of off-line usage that a card will permit before forcing the transaction on-line for authorisation. This control can be based on both the number and the accumulated value of consecutive off-line transactions. When thresholds set by the card issuer are crossed, the transaction can be forced on-line. If, for some reason, the device is unable to go on-line, the card will either permit or decline the transaction, again according to the card issuer's settings. However, these controls would be a fairly blunt instrument were it not for the card issuer's ability to vary the parameters that determine the outcome of the card's risk management processing on an individual card-by-card basis. This is achieved by sending scripts to the card during an on-line transaction to update these parameters. It is when this ability to dynamically control card behaviour is teamed with a risk management system that is monitoring the level of risk at account or cardholder level that the power of EMV is really unlocked.

Before EMV, the card issuer had to rely on the card coming on-line for authorisation; a decision based almost entirely on the value of the transaction or the type of terminal, and was then able to make an 'approve' or 'decline' decision based on a risk assessment of that transaction in the context of the cardholder's account status and behaviour. EMV allows that process to be much more granular and for action to be taken earlier in the cycle of events. When risk management processing detects that an account is in the early stages of going from an acceptable to an increased risk, subtle changes to card behaviour can be made by returning an EMV script. The range of risk-based card profiles – combinations of the EMV risk parameters that result in pre-determined card behaviour – can be broadened to provide this granularity.

A card may be moved through five or ten or even more profiles as cardholder behaviour is monitored, since progressively increasing the frequency with which the card comes on-line not only provides the issuer with more opportunities to decline a transaction, but before that stage is reached, additional data on which to base successive risk assessments will be gathered. 'Micro-management' of an account in this way will reduce both the issuer's exposure to bad debt, but will also allow the issuer's risk management processes to determine with greater accuracy when to take the decision to decline which on the one hand, may prevent an unrecoverable debt, but on the other may irretrievably damage the relationship with a potentially profitable customer.

The converse also applies as an account moves back from a position of heightened risk. The severity of the risk profile can be reduced progressively, continuing to provide enhanced account monitoring information while the risk remains higher than normal.

Conclusion

It can be seen that the migration to EMV cards not only attacks the immediate issues of counterfeit and lost and stolen fraud, but opens up a new dimension in the management and control of risk for both credit and debit card issuers. EMV scripting supports the introduction of a dynamic card risk profiling approach that gives issuers an unprecedented degree of control. This in turn requires new ways of using risk management tools, whose strategies and outcomes can now be fine-tuned to manipulate card behaviour, in addition to initiating account management actions and making authorisation decisions. Forward-thinking issuers who grasp this opportunity and take advantage of these features will gain competitive advantage by reducing the cost of referrals, collections and write-offs, ensuring that optimum use is made of credit lines and ultimately using the enhanced control of risk to extend card issuance to previously off-limits applicants.



About the Author

Nigel Beatty is an experienced business consultant with a broad and extensive knowledge of the payments industry. He has worked with clients providing consultancy at senior levels within the UK's leading financial institutions and has particular expertise in the area of EMV smart cards. Nigel works with clients to develop strategies, define business cases and deliver solutions throughout the electronic payments industry.

About Aconite Technology Ltd.

Aconite delivers smart card payment solutions and consulting expertise to card issuers and processors around the world, providing a rapid and cost-effective route to smart card deployment and the delivery of innovative card payment solutions to new and existing markets.

Incorporating a unique blend of proven software solutions and professional services, Aconite solutions can be tailored to meet individual business requirements without the need to replace legacy systems and with minimal impact on staff and processes. Based in the UK, Aconite has a presence in five regions: Europe, Middle East, Asia, The Americas and Southern Africa.



Aconite Technology Ltd
Amadeus House
27b Floral Street
Covent Garden
London WC2E 9DP

Tel: +44 (0)20 7182 7150
Fax: +44 (0)20 7182 7151
Email: enquiries@aconite.net