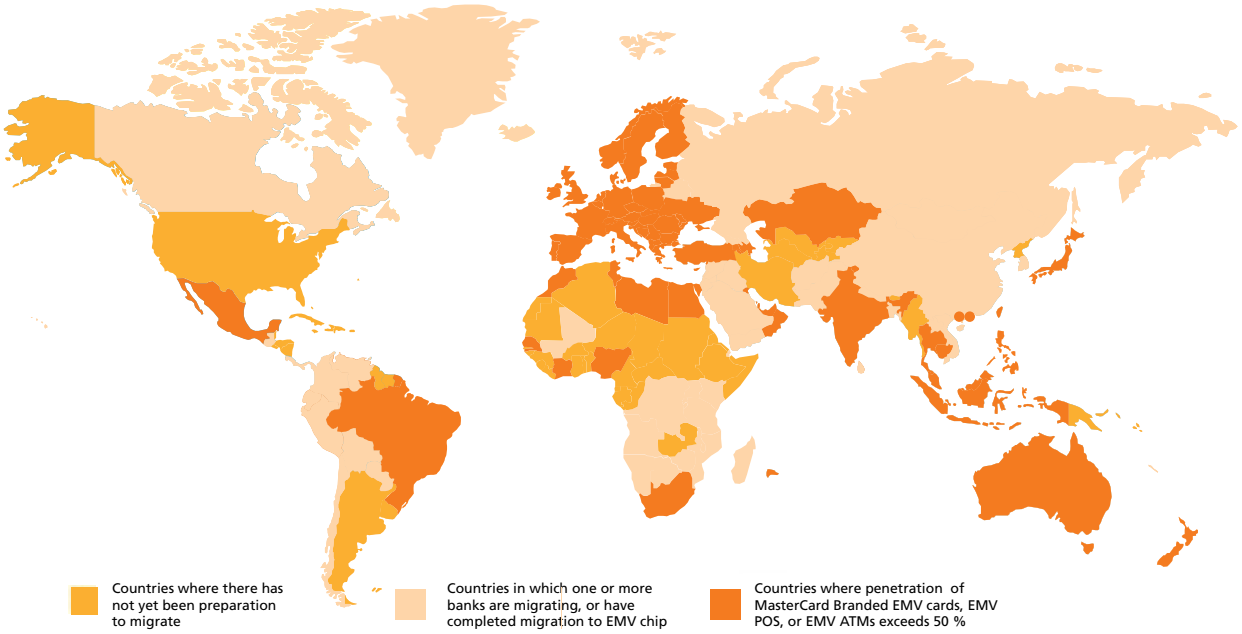
MANAGING FRAUD WITH EMV –
A RISK MANAGER CHECKLIST FOR DEPLOYING CHIP TECHNOLOGY

Worldwide rollout of EMV continues to gather pace. Several markets and regions around the world have the completion of EMV migration in sight or are making large strides as they begin to introduce the authentication technology in their regions:

- The Single European Payments Area (SEPA) will have a cards payment market that is largely chip-based as of 2011
- Canada and Mexico are in the early stages of EMV deployment
- Much of Southeast Asia and parts of Africa also operate EMV-enabled payment networks



As of Q2 2009, there were 487 million MasterCard branded cards (including Maestro) compliant with EMV, 14 million EMV capable POS terminals, and over 3,000 active MasterCard Chip migration projects underway in 119 countries

The secure data authentication provided by chip technology protects both online and offline transactions against counterfeit fraud. Given the ongoing spread of EMV technology around the world, what other steps should issuers take to protect their investment as the chip infrastructure matures?

Card Issuance Considerations

The first and most important consideration in deploying EMV technology is to ensure that there is no risk of track data cross-contamination with data stolen from one interface being used to produce counterfeit cards using a different technology. Simply personalizing chip cards without the complete magnetic stripe track 2 data means that if chip transaction data is compromised, then it cannot be used to create a counterfeit magnetic stripe card (i.e., using a Card Validation Code [CVC] 1 in the track 2 equivalent data element on the chip so that track data copied to the magnetic stripe can be detected).

The opportunity to switch from signature verification to PIN is another option to consider. Issuer-controlled PIN is a step forward from subjective signature-checking, which relies on the diligence of the merchant. In addition, replacement of signature with PIN is a positive step for merchants resulting in reduced exception handling and streamlining POS processing (e.g., signed slip handling, objective acceptance).

In addition, issuers should take appropriate steps to employ appropriate authentication technologies moving beyond Static Data Authentication (SDA). While Dynamic Data Authentication (DDA) provides a higher degree of security that protects against chip data cloning, the most secure EMV implementation uses Combined Dynamic Data Authentication/ Application Cryptogram Generation (CDA), where the card produces a dynamic digital signature on a random challenge that it has received from the terminal and other sensitive data, and on the value of the Application Cryptogram (AC) generated by the card.

By verifying this dynamic signature, the terminal can authenticate the card and confirm the legitimacy of sensitive data, including the AC and the proof that the card has verified the PIN.

The big advantage of CDA is that it not only provides the dynamic aspects of DDA (hence protection against cloning), but also ensures the integrity of sensitive data communicated between the card and terminal, hence protecting against complicated wedge attacks.

Optimizing Authorization Processes

Although chip technology gives the issuer the opportunity to manage the volume of online authorizations — so they can match their risk control against their operations and performance objectives — it must be remembered that chip technology should be used hand-in-hand with transaction fraud controls and predictive fraud systems to fight the fraudster.

A primary consideration is transactions that have been completed as technical fallback from chip to magnetic stripe. These transactions can be fraud prone as the fraudster seeks to avoid the protection of the chip by disabling it. The risk of fallback transactions should be carefully considered and action taken either to contact cardholders or decline transactions where there is significant risk. The frequency of fallback should be tracked and cards that appear prone to failure should be quickly replaced.

When a chip transaction does occur, the additional chip authorization data will give issuers additional information that can be used to detect fraud attacks. The following key authorization checks should be considered:

- Authenticate the card using the cryptogram received in the authorization message. Although an invalid cryptogram can be caused by data integrity issues, an invalid cryptogram is a clear indication of a higher risk transaction
- Review the Terminal and Card Risk Management information received. This will reveal why the transaction came online and subsequent tracking of this information across a sequence of transactions will help to identify unusual card usage patterns
- Check what cardholder verification method has been used for the transaction. It is particularly important to validate that the card that supports PIN has successfully checked the PIN if the terminal supports PIN
- Manage the use of signature fallback. Many issuers will allow signature to be used instead of PIN, especially as cardholders become accustomed to using PIN. But the exception can be a trade off between customer service and fraud risk and once PIN is well established, signature fallback transactions should be considered as higher risk

EMV provides a significant opportunity to manage down the risk of card transactions. Use of the chip cryptogram to properly handle chip card and POS authentication means that valuable fraud resources need not be directed to checking out the authenticity of transactions which are obviously not counterfeit.

The technical platform provided by EMV is very powerful. However, it is crucial that banks also consider how EMV, and in particular the introduction of PIN, impacts cardholders. Simple measures that encourage cardholders to use and remember their PIN are important to a smooth transition. For example, offering PIN change functionality at ATMs enhances the likelihood of cardholders remembering their PIN without writing it down for a fraudster to discover.

Although the migration to the chip technology gives the banks a vital tool in the fight against fraud, it is not the technology alone that creates a total solution. Rather, it is the way the bank uses the opportunity. By following the above simple steps, banks can deliver on the business case for the investment in chip and give a better service to their cardholders.

EMV PAYMENT CARDS SECURITY MEASURES TO PREVENT WEDGE ATTACKS

Earlier this year, reports by media alleged EMV payment cards are vulnerable to wedge or "man-in-the-middle" attacks. Wedge attacks, as described in the reports, occur when a fraudster inserts a wedge device between a lost or stolen card and point-of-sale (POS) terminal, thereby causing the terminal to erroneously determine that the card has been verified by the PIN. Additional allegations also claim that issuers may not be able to detect that a wedge attack has occurred during the online authorization process.

In response to these allegations, EMVCo — the global standard for credit and debit payment cards based on chip card technology — issued a statement to ensure that the marketplace understands the robust security measures EMV cards employ to prevent wedge-type attacks from succeeding. MasterCard supports EMVCo's position on the matter. The complete statement can be read at **www.emvco.com**.

This wedge, or man-in-the-middle attack, is technically difficult and suitable countermeasures are already available when the full picture of the payment process is taken into account. The interoperability and security features provided by the EMV card-terminal specifications are building blocks for the payment systems and financial institutions that design their products and processes in accordance with wider risk management needs.

The opportunity to launch the wedge attack is limited and countermeasures do exist:

- The attack is focused exclusively on lost and stolen fraud. This fraud type has additional controls in place to mitigate it outside EMV and by its nature the fraud is limited to the single stolen card
- The attack is not relevant to ATM transactions and does not compromise the valid PIN
- Countermeasures are already available either explicitly in EMV, or within payment system products and networks, or within issuer host systems. Indeed, the issuer can already detect if the PIN has not been verified and can decline or refer the transaction in order to minimize risks associated with signature fallback

The risks and challenges faced by fraudsters would be major. They must:

- Steal a card
- Install the card into wedge electronics so that it can be used unobtrusively
- Perform the attack before the card is reported stolen
- Risk detection by the merchant during the fraud attempt with the resulting legal consequences
- Hope that the issuer does not have intelligent fraud detection based on behavioral and geographic data

While such an attack might be theoretically possible, it would be extremely difficult and expensive to carry out successfully. Current compensating controls are likely to detect or limit the fraud. The possible financial gain from the attack is minimal while the risk of a declined transaction or exposure of the fraudster is significant.