Payment Card Industry (PCI)

Data Security Standard

PCI DSS Applicability in an EMV Environment

A Guidance Document

Version 1

Release date: 5 October 2010

Table of Contents

1 Executive Summary

This document compares and contrasts the current fraud-reduction capabilities of EMV within the security framework of the Payment Card Industry Data Security Standard (PCI DSS) and examines the rationale for why it remains necessary to implement PCI DSS in the EMV environments that exist today.

1.1 The Role of EMV

EMV smartcards were designed and introduced to reduce fraud occurring in magnetic-stripe face-to-face environments, by using integrated-circuit (IC) based cards that use secret cryptographic keys to generate authentication and authorization data. As such, robust implementations of the EMV specifications can mitigate the risk of compromised card data being used to commit face-to-face fraud. EMV implementations that utilize different card verification values maintained on the chip from those maintained in the magnetic-stripe image provide an effective barrier to creating counterfeit magnetic-stripe cards from compromised EMV magnetic-stripe image data. In addition, when implemented in conjunction with PIN for cardholder verification, EMV limits the impact of the lost/stolen/never-received categories of fraud. Evidence has clearly shown that in those countries where EMV has been deployed, there has been a measurable and significant reduction in face-to-face fraud[1].

However, EMV by itself does not protect the confidentiality of, or inappropriate access to sensitive authentication data and/or cardholder data. Current EMV acceptance and processing environments may process both EMV and non-EMV transactions, (such as magnetic stripe, or primary account number (PAN) key-entry when technical reasons require). These non-EMV transactions do not have the same fraud-reduction capabilities of EMV transactions and, consequently, require additional protection. In addition, it is important to note that in EMV environments the PAN is not kept confidential at any point in the transaction, indeed, it is necessary for the PAN to be processed by the point-of-sale terminal in the clear in order to complete critical steps in the EMV transaction process. The expiry date and other cardholder data are also transmitted in clear-text.

The potential for these transaction types and/or data elements to be exposed and used fraudulently within both the face-to-face channel and the card-not-present channel are the reasons why it is necessary to implement PCI DSS in today's EMV acceptance environment(s)

[1] Financial Fraud Action UK and the UK Cards Association. "Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it". Available On-line: http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

1.2 The Role of the PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) contains 12 key technical and operational requirements set by the PCI Security Standards Council (PCI SSC). Rather than focusing on a specific category of fraud, the PCI DSS seeks to protect cardholder and sensitive authentication data anywhere this data is present within the payment eco-system, thus limiting the availability of this data to fraudsters. PCI DSS achieves its security objectives in two ways:

- Ensuring the integrity of system components that are conduits to cardholder and sensitive authentication data against physical and logical attack.
- Protecting the confidentiality of cardholder data when stored within a given environment, or cardholder and sensitive authentication data when transmitted over an open or public network.

1.3 Conclusions

Acceptance environments that effectively utilize EMV can substantially reduce fraud in face-to-face environments but, as detailed above, an EMV environment as implemented today does not automatically fulfill PCI DSS requirements nor does it protect the confidentiality of cardholder and sensitive authentication data. Add to this the capability of merchants to process both EMV and non-EMV transactions, and it becomes obvious that protecting the confidentiality of cardholder and sensitive authentication data is essential.

By design, PCI DSS does not distinguish between underlying transaction security mechanisms, but instead seeks to protect the PAN and other sensitive authentication data as a goal in and of itself without examining the underlying fraud risk should this data be compromised. In the future, should EMV become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly. Until such time, EMV and PCI DSS together create a powerful two-pronged approach to the objectives of reducing fraud and increasing security.

Therefore, in securing the current face-to-face acceptance environment one should not consider it to be a case of either EMV or PCI DSS, but rather EMV and PCI DSS. Both are essential elements in the fight against fraud and data exposure. Together they provide the greatest level of security for cardholder data throughout the entire transaction process.

2 Scope

This document is intended for adopters of EMV technology, including but not limited to retailers, acquirers, processors, and issuers, or those that validate PCI DSS environments such as Qualified Security Assessors (QSA) and Internal Security Assessors (ISA).

It is understood and accepted that different markets in various regions around the world are at different stages of EMV roll-out and maturity. Those markets which are not yet in a mature state will be working toward achieving the recommendations of the payment card brands and EMVCo.

The document does not provide technical details about EMV or PCI DSS, nor instructions on how to implement EMV or PCI DSS, but does assume that the reader is familiar with both of these standards. It also assumes that the IC card and terminal manufacturers will have incorporated the latest EMV guidance into their products. It is understood that the best security is provided by those terminals which have been approved against the latest version of the PCI PIN Transaction Security Testing Program.

For the interested reader, details of the EMV and PCI standards and specifications can be found on the relevant web sites *www.emvco.com and www.pcisecuritystandards.org*, as well as within brand-specific guidelines and documents.

The reader is reminded that the role of the PCI Security Standards Council is to generate security standards and other supporting guidance documents. All aspects relating to compliance, enforcement, and adoption of these standards, including all issues relating to risk, are the responsibility of the individual card schemes. Any questions readers may have in this regard should be directed to their relevant PCI DSS contact.

3 EMV Security and PCI DSS

To understand how current EMV acceptance and processing environments relate to the PCI DSS, one must examine the data elements present in EMV transactions and understand how this information may be used in a fraudulent manner. In addition, it is important to understand the limited protection inherent in non-EMV transactions and how this information is susceptible to fraudulent use should it be disclosed.

The table below presents the data elements which are present on an EMV chip card and/or available during EMV transaction processing as well as the rationale for why they are present. In doing so, it is important to highlight that both data maintained on an EMV enabled chip as well as data sent during an EMV transaction contains elements of cardholder and sensitive authentication data that PCI DSS seeks to protect.

	Data Element	Rationale
Cardholder Data	Primary Account Number (PAN)	Necessary in clear-text for EMV transactions to: ▪ Identify the cardholder and settle the transaction ▪ Facilitate transaction routing ▪ Perform data authentication at the point of sale ▪ Enable key derivation by the Issuer
	Cardholder Name	Present in an EMV chip. Not required to be transmitted in an authorization message.
	Service Code	Present in Track 2 Equivalent Data on chip. Its purpose in EMV is to enable the issuer to validate the card verification code or value if also included in the Track 2 Equivalent Data.
	Expiration Date	Always available on EMV cards in the clear with specific expiration date tag. In case of online authorization, the expiration date included in Track 2 Equivalent Data will be included in the authorization message. This data is available in clear-text.

	Data Element	Rationale
Sensitive Authentication Data	Full Magnetic-Stripe Data	EMV may optionally contain Track 1 and 2 Equivalent Data, which contains the same fields as that of a magnetic stripe. For legacy purposes, the Track 2 Equivalent Data is typically included in an EMV on-line authorization requests. This data is available in clear-text. When a unique chip card verification code or value is used, however, the equivalent track 2 data is now different than the magnetic-stripe track 2 data and thus cannot be used to create fraudulent magnetic-stripe cards. In this instance only the cardholder data elements as described above remain sensitive.
	CAV2/CVC2/CVV2/CID	Not part of EMV Specification. EMV chips do not contain this information. This code is only printed on the card itself.
	PIN/PIN Block	The EMV Specification allows for off-line verification of the cardholder through the use of the PIN in the chip itself so the PIN block never leaves the point-of-sale environment. Other CVM are also supported, including on-line PIN.

3.1 The Payment Card Environment

Most environments processing EMV transactions today are hybrid environments, handling both EMV and non-EMV transactions. In such circumstances, protecting the confidentiality of cardholder and sensitive authentication data remains essential to ensuring the integrity of the payment chain.

3.1.1 Magnetic-Stripe Transactions

In a magnetic-stripe transaction, cardholder and sensitive authentication data is read from the static data encoded on the magnetic stripe of the card and forwarded to the issuer (typically in the clear) for authorization. Given the static nature of this data, it can be easily copied either directly from the card or by interception during transaction processing. Captured magnetic-stripe data can then be used to create counterfeit magnetic-stripe cards for use in face-to-face and ATM fraud. In addition, PAN and expiry date can be extracted from the magnetic-stripe data for use in card-not-present (CNP) fraud, where the CNP channel does not use additional authentication data beyond what is available in the face-to-face channel.

3.1.2 Technical Fallback

Most EMV cards contain a magnetic stripe, for either backwards compatibility in non-EMV environments or to support technical fallback if the EMV enabled chip is unreadable. “Technical fallback” describes an exception process wherein the magnetic stripe rather than the chip data on an EMV card is read by an EMV-capable device. In such situations the security mechanisms provided by EMV are effectively bypassed, and the transaction security reverts to that of a magnetic stripe. In many mature EMV markets, however, technical fallback is usually restricted and controlled, limiting this type of fraud.

3.1.3 PAN Key Entry

PAN key entry occurs as a fallback when a magnetic stripe or a chip cannot be read. To complete a PAN key-entry transaction, only the PAN, expiration date, and customer signature are necessary, making this technique easily susceptible to fraud from cardholder data compromised in any acceptance channel. While PAN key entry requires the forgery of the cardholder signature, this method of cardholder verification is potentially less reliable as it may be either incorrectly verified by a merchant or simply not checked. This method of data entry is restricted, controlled, and used infrequently in a mature EMV environment, thus limiting PAN key-entry fraud.

3.1.4 Mail Order/Telephone Order-based Transactions

Merchants sometimes use this method to accept remote transactions in their EMV acceptance environments. Like PAN key entry, the retailer will manually input the PAN and expiry date; however, in addition to this data the retailer will often input the card security code (three-digit code printed on the physical card) as part of transaction authorization.

3.1.5 EMV Transactions

In EMV acceptance environments the EMV transaction contains data that is of value to a fraudster. Scenarios in which that data is at risk can be broadly categorized as follows:

- Lack of unique chip CVV/CVC: If an EMV card maintains the same CVV/CVC as the magnetic stripe, captured equivalent track 2 data could be used to create magnetic-stripe cards for use in face-to-face and ATM fraud.
- "Deep dip" reading: When the card is fully inserted into a reader, such as an ATM, the actual magnetic stripe can be read and the captured data used to create magnetic-stripe cards.
- PAN & expiry date exposure: EMVCo does not require that the PAN and expiry date be kept confidential in EMV transaction processing. In today's payment-acceptance infrastructure, it is possible that payment transactions may be presented for approval and authorized based solely on the PAN and expiry date. This information is typically available in clear-text as part of both EMV and magnetic-stripe transactions, and may be used fraudulently in other payment-acceptance channels, such as card-not-present (CNP), which do not use additional authentication data beyond what is available in the face-to-face channel.

As a consequence of these threats, native EMV transaction data requires protection beyond what is inherently provided by EMV itself.

3.2 PCI DSS and the Current EMV Environment

The EMV standard provides transaction security and global interoperability within an EMV transaction environment. EMV implementations that use card verification values which are different from those maintained in the magnetic stripe mitigate the risk of compromised EMV transaction data being used to create counterfeit cards. Likewise, EMV actively prevents card-cloning attacks through the use of enhanced card authentication methods and, when implemented in conjunction with PIN as a method of cardholder verification, limits the impact of lost/stolen/never-received categories of fraud. However, EMV does not protect the confidentiality, nor prevent the compromise of certain transaction data elements.

In all acceptance environments as discussed in Section 3.1 above, payment transactions presented for approval based solely on static data—such as magnetic stripe, manually key-entered data, mail-order/telephone-order-based transactions, and PAN and expiry dates—are inherently valuable and can be used to conduct fraudulent transactions unless appropriate measures are taken to prevent access to that data. For these reasons, PCI DSS remains an essential tool to protect static data.

PCI DSS applies to all possible payment channels and ways that cardholder data might be used to perform a transaction.

3.3 Future Developments in Transaction Security

Changes, improvements, and new payment opportunities are continually being developed. By using the authentication methods provided by EMV and introducing additional authentication into the CNP channel, the PAN and expiry date on their own would no longer be sufficient to complete a transaction. Other changes could see the introduction of enhanced authentication procedures and processes for all transaction channels such that:

- EMV is the sole method of effecting payment in a given face-to-face channel. In a mature EMV environment this could involve a migration to an EMV-only card, which would reduce the hybrid environment threat while still allowing transmission of the cardholder PAN and other sensitive data in clear-text.
- For environments which do not migrate to an EMV-only card, but where EMV is the only method for face-to-face payment, the use of differing card verification values maintained on the chip and in the magnetic stripe is essential.
- The card-not-present channel uses additional authentication data to perform cardholder verification that cannot be obtained through the compromise of the face-to-face acceptance environment.

In such circumstances, the need to keep the PAN and other sensitive authentication data confidential is significantly reduced. As a consequence, the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly.

3.4 Summary

EMV must be considered in the context of the current transaction-processing environment where the confidentiality of cardholder data from EMV transactions, along with sensitive authentication data from non-EMV transactions, remains fundamental to ensuring the integrity of the payment system.

While EMV can substantially reduce fraud in card-present transactions, it does not automatically satisfy PCI DSS requirements for the protection of cardholder and sensitive authentication data. Within this context of current EMV deployments, the need to protect the confidentiality of cardholder and sensitive authentication data as prescribed by PCI DSS is still a critical part of the industry's overall effort to prevent that data being used for fraudulent transactions in other environments.

In the future, should EMV become the sole means of payment in a given face-to-face channel, coupled with a globally adopted robust authentication process for card-not-present (CNP) transactions, the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. As a consequence, the PCI DSS would be updated to bring it in line with the threat landscape that would then exist, and its applicability in relation to EMV reduced accordingly.

Today EMV and the PCI DSS, as well as the PA-DSS and PTS standards, are complementary and form important layers in providing a holistic approach to the objectives of reducing overall fraud and securing cardholder data in the payment industry. In those markets which have migrated or are in the process of migrating to EMV, payment industry stakeholders should use EMV and PCI DSS together to reduce fraud and increase security.

4 Reference & Glossary

4.1 References

1. *EMV 4.2 Book 2 Security* – www.emvco.com
2. *EMV 4.2 Book 3 Application Specification* – www.emvco.com
3. *PCI Data Security Standard, v1.2* – www.pcisecuritystandards.org
4. *EMV Issuer and Application Security Guidelines, v2.2 May, 2009* – www.emvco.com
5. *EMV 4.2 Book 4 Cardholder, Attendant, and Acquirer Interface Requirements* – www.emvco.com
6. *PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms*
7. *PCI PTS Security Requirements*
8. *Recommendations for EMV Processing for Industry-Specific Transaction Types, December 2008, v1.1* – www.emvco.com
9. Financial Fraud Action UK and the UK Cards Association. "Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it." Available online: http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

4.2 Abbreviations & Glossary

Abbreviations and definitions may be found in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms*

Additional abbreviations and definitions are defined below.

Term	Definition
CNP	Card-not-present
CVM	Card verification methods
CVR	Card verification results
DAC	Data authentication code
EMV	Formally Europay, MasterCard, Visa – Integrated Circuit Card Specifications for Payment Systems. www.emvco.com
ICC	Integrated circuit card
iCVV	ICC Card Verification Value
MO/TO	Mail-order/telephone-order
POS	Point of sale
SEPA	Single Euro Payments Area
TRM	Terminal risk management
Card-not-present	A type of payment transaction—performed, for example, via mail, telephone, or Internet—where the cardholder does not present the card to the merchant
Hybrid card	A card that contains both an EMV chip and a magnetic stripe.
EMV environment	An environment in which an EMV chip is read by a point of sale terminal and used to perform an EMV transaction. This may be part of a Hybrid environment that also processes magnetic-stripe transactions and data.
Hybrid environment	An environment in which both the EMV chip or magnetic stripe can be read by the point of sale and used to process EMV or magnetic-stripe transactions.
Technical fallback	A state in which a chip cannot be used and another type of entry such as magnetic-stripe read or PAN key is used to complete a transaction.

4.3 Acknowledgements

Many organizations have contributed individually and collectively to create this document, including: Members of PCI Board of Advisors, the Scoping Special Interest Group, members of the QSA community, EMVCo, banks, vendors, merchants and independent consultants. All of their valuable input and support was greatly appreciated.