Increasing Security and Reducing Fraud with EMV Chip and PCI Standards

When data is exposed, it puts your customers and your reputation as a business at serious risk. EMV chip technology combined with PCI Security Standards offer a powerful combination for increasing card data security and reducing fraud.

What they are – Fraud protection & data security

EMV chip:

- Technology that uses secret cryptographic keys to help protect against fraud at the point of sale and make payment cards more difficult to counterfeit.

PCI Security Standards:

- Security controls for making sure that customers' card data is kept secure throughout the entire transaction process.

How they're different: Authentication technology vs. data security controls

EMV chip:

- Authentication technology for the point of sale part of the transaction when the physical card is actually present.
- When this chip is embedded on a card, it helps ensure the card being used is real and that it belongs to the person using it. It drastically reduces the chances of your business accepting lost, stolen or counterfeit cards.

PCI Security Standards:

- Security controls to protect the cardholder's confidential information on payment cards, not just at the moment the card is swiped or dipped, but all the way through the transaction process.
- They also apply when payments are made online or via telephone, where the card is not present, to make sure your customers' card data is kept safe.

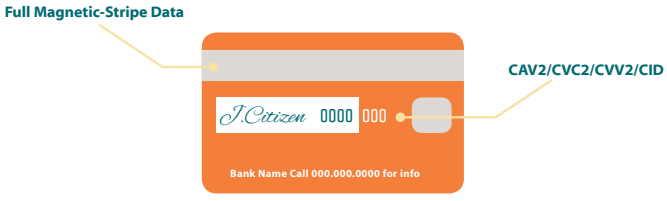
How they work together: A layered approach for securing multi-channel transactions

- EMV chip provides an additional level of authentication at the point of sale that increases the security of a payment transaction and reduces chances of fraud.
- Once the card is entered into the merchant's system, the cardholder's confidential information (see chart below) is transmitted and stored on their network in a clear, easily accessible form, meaning it's vulnerable for attack and use for fraud by criminals in online and other channels.
- Which is where PCI Standards come in. On top of EMV chip at the point of sale, they offer protections for the point of sale device* itself and provide layers of additional security controls** for businesses to use throughout the transaction process and across payment channels to keep card data safe - such as patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data.

How it's done: Here's a break-down of existing data elements

	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. Enables the issuer to validate the card verification code or value if also included.
	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.

	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. The Track 2 Equivalent Data is typically included in an EMV on-line authorization requests available in clear-text. When a unique chip card verification code or value is used, the equivalent track 2 data changes from the magnetic-stripe data and cannot be used to create fraudulent cards. In this instance, only the cardholder data elements 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	EMV allows for off-line verification of the cardholder through the use of the PIN in the chip itself. Other CVM are also supported.



Abbreviations and Terms

A glossary of important terms to help you understand & improve your security efforts.

CNP Card-not-present

CVM & CVR Card verification methods & results

DAC Data authentication code

EMV Europay, MasterCard, Visa. Visit www.emvco.com for more info

ICC Integrated circuit card

iCVV ICC Verification Value

POS Point of sale

SEPA Single Euro Payments Area

TRM Terminal risk management

Hybrid card A card that contains both an EMV chip and a magnetic stripe

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.

When used together, EMV chip and PCI Standards are a powerful combination to increase security and reduce fraud. Protect your customers' data and your business today.

Visit **www.emvco.com** and **www.pcisecuritystandards.org** to learn more.

PCI Security Standards Council

*See PCI PIN Transaction Security Requirements **See PCI Data Security Standard (PCI DSS) and PCI Payment Application Data Security Standard (PA-DSS)