Elavon Arches

Commentary on payment initiatives and trends impacting merchants, VARs, ISOs and Processors

Protecting Cardholder Data: EMV, Point-to-Point Encryption & Tokenization

To protect cardholder data and related fraud, businesses need to embrace technologies such as EMV, Point-to-Point Encryption (P2PE) and Tokenization that prevent the types of system attacks associated with a data breach.

A Modern Strategy to an Evolving Threat

Hackers target businesses that process and store cardholder data because it is both valuable and portable. PCI compliance alone does not guarantee security. To successfully combat evolving security threats, companies must adapt, update and modernize their security strategy by implementing advanced encryption and tokenization solutions that:

- Remove actual card data from the payments stream
- Protect card data at every point in the transaction lifecycle: in use, in transit, at rest
- Ensure the continuity of existing business processes that require the use of card data
- Mitigate the costs and complexities of PCI compliance

Elavon's SAFE-T Suite: End-to-End Data Protection

SAFE-T Suite (Secure and Flexible Encryption & Tokenization) provides end-to-end data protection by eliminating actual cardholder data from your environment. It protects your bottom line by avoiding the fees, fines and costs associated with a breach. And it protects your reputation because your customer card data isn't' compromised.

EMV Prevents Counterfeit Card Use

EMV terminals read advanced algorithms contained on Chip cards to authenticate that the card is not a counterfeit. The data is not encrypted or secured for processing the transactions.

Encryption Protects Data in Transit

Point-to-point encryption (P2PE) protects card data presented to a business from the consumer until it is received by Elavon. Terminals — can be the same as EMV devices — containing a tamper resistant security module (TRSM) encrypt the data through the application of an algorithm and a secret key, thus eliminating usable information before it enters the POS or network.

Tokenization Protects Data in Use and at Rest

Tokenization always eliminates the possibility of having real card data stolen because it no longer exists in your environment. Tokenization uses a randomly-generated unique ID ("token") in place of the Primary Account Number (PAN) so that the actual card number is not stored.

One of the key advantages to tokenization is that it allows you to continue to use customer card information for important business processes, including card-on-file transactions, shopping analytics, and loyalty programs. Since actual card data is replaced with unique IDs, it can be stored indefinitely and used with multiple business applications without fear of compromising sensitive data.

SAFE-T Suite Reduces PCI Costs

SAFE-T Suite reduces the costs and labor and simplifies the annual PCI validation process, allowing businesses to redeploy valuable resources. Removing actual card data de-scopes the POS and PMS systems, while shifting responsibility and risk to Elavon by moving elements of the security process "upstream" in the transaction lifecycle.

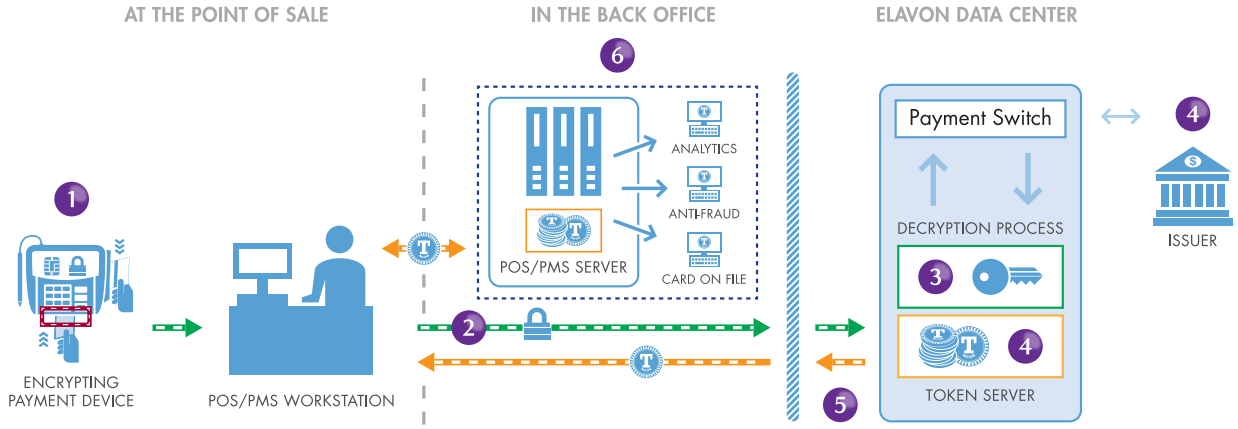
Protect Cardholder Data in Use, in Transit, and at Rest

A Worthwhile Investment for Peace of Mind

These are exciting times. EMV will act as a catalyst for point-of-sale upgrades throughout the payment ecosystem. This is one of a handful of transformative initiatives to impact the payment industry in the past thirty years: first was the transition from paper to electronic processing in the 80's, following by the adoption of PIN debit in the 90's, and most recently the e-commerce wave that gained momentum in the early '00's.

Businesses are encouraged to capitalize on that investment by implementing EMV terminals that support point-to-point encryption and de-scope the POS. The reduction in PCI compliance costs will quickly result in a positive return on investment. And the combination of EMV, P2PE and Tokenization will extend peace of mind to financial, security and operational executives, allowing them to focus on initiatives that drive their business forward, knowing that card data cannot be compromised.

SAFE-T Suite Protects Data In Use, In Transit and At Rest



1. Consumer presents card at point of sale
2. Card data is encrypted and transmitted to Elavon
3. Elavon decrypts the data payload
4. Card data is sent in to the issuing bank for authorization and, in parallel, tokenized
5. Token is paired with authorization response and sent back to the POS
6. Token is stored in the POS/PMS server in place of the actual card data and is used for all subsequent business processes

Elavon