comforte

COMFORTE QUICK GUIDE

Tokenization Explained

How to protect your customers' data

When it comes to tokenization, can you really identify the important distinctions between high-value (payment) and low-value (security) tokens?

Here are some tips for understanding the differences:

Features of high-value tokens

1. High-value tokens (HVTs) are values that act as surrogates for actual PANs in payment transactions.
2. An HVT solution (e.g., Apple Pay) enables the HVT itself to be used as an instrument for completing a payment transaction. To function, HVTs must look like actual PANs. (This guide offers more on Apple Pay.)
3. Multiple HVTs can map back to a single PAN, without the owner being aware of it.
4. HVTs limit the range of fraud. The payment/HVTs usage can be limited to certain networks (e.g., Apple Pay) and/or merchants (e.g., Apple, Amazon, etc.) whereas PANs cannot.
5. HVTs can be bound to specific devices. Tokens can be correlated to some physical device identifier along with historical location data. Anomalies between token use, physical devices, and geographic locations could then be flagged as potentially fraudulent.

For more documentation on tokens, see the Payment Card Industry Data Security Standard's (PCI DSS) detailed guidance. Then see our full post, "Demystifying Tokenization: Payment Versus Security Tokens"

Features of low-value tokens

1. Low-value tokens (LVTs) also act as surrogates for actual PANs in payment transactions.
2. LVTs cannot be used in and of themselves to complete a payment transaction. For LVTs to work at all, it must be possible to match them back to the actual PANs they represent.
3. A consumer's PAN is tokenized by replacing the actual value with the surrogate value, the token. The token must always be matched back to the actual PAN to complete a payment transaction. This mapping from LVT to actual PAN is done within a "tokenization system."

Contact us to discuss your tokenization and security requirements.