StoreNext

Update Bulletin

PCI New Position on Scope and Tokenization

August 12, 2011

PCI issued an amendment today to the PCI DSS Tokenization Guidelines.

The change will put some data and systems back into PCI scope that were previously considered exempt on account of their use of tokenization. The effect of the change is disruptive: merchants that had relied on tokenization services to limit their PCI scope may now find themselves back to square one and exposed.

> ***Spoiler alert!*** Connected Payments is not affected. The strength of the Connected Payments tokenization scheme makes it invulnerable to the concern that PCI is addressing.

Tokenization is a common security technique that replaces real data with a "token," which is typically a randomly generated number. The token itself is meaningless and therefore of no value if stolen, thereby protecting the actual data from fraudulent use. The real data can only be accessed via a secured token server system, which cross-references the individual tokens to the data elements they replaced. Encryption is different than tokenization: encrypted data can be recreated only if the encryption key is known; tokenized data can only be recreated via its unique cross-reference provided by the token server.

PCI is concerned because a customer's token, if widely used, could essentially take on a life of its own and become a surrogate for the customer's Primary Account Number (PAN). If so, the token itself could conceivably be used to make fraudulent purchases just the same as if it were the actual PAN.

PCI therefore amended their guidelines by stating that tokenized data may be in scope after all, but stopped short of establishing a clear line, instead giving individual financial institutions the case-by-case say-so for now. Although PCI promised additional guidance in the future, merchants relying on tokenization services to reduce their PCI exposure are suddenly up in the air since their PCI status just became wholly dependent upon decisions that their up-stream chain of commercial interests will need to make:

> *"Additionally, tokens that can be used to initiate a transaction might be in scope for PCI DSS, even if they cannot directly be used to retrieve PAN or other cardholder data; merchants should therefore consult with their acquirer and/or the Payment Brands directly to determine specific requirements for tokens that can be used as payment instruments."*

Merchants using Connected Payments are exempt from this problem since our system uses a more secure multiple-token architecture that makes tokenized PANs useless for initiating new or fraudulent transactions.

To Your Success,

Antony van Seventer