PCI SSC Issues Statement On Scope of Encrypted Data via FAQ 10359

Issued 11/10/2009

Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS?

The Council will be developing more formal guidance around this topic, leveraging information that is received through the various channels of the DSS lifecycle feedback process. Until further guidance is provided by the Council, the following should be taken into consideration regarding encrypted cardholder data. Encryption solutions are only as good as the industry-approved algorithms and key management practices used, including security controls surrounding the encryption/decryption keys ("Keys"). If Keys are left unprotected and accessible, anyone can decrypt the data. The DSS has specific encryption key management controls (DSS 3.5 and 3.6), however, other DSS controls such as firewalls, user access controls, vulnerability management, scanning, logging and application security provide additional layers of security to prevent malicious users from gaining privileged access to networks or cardholder data environments that may grant them access to Keys. It is for this reason that encrypted cardholder data is in scope for PCI DSS. However, encrypted data may be deemed out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it. Any technological implementation or vendor solution should be validated to ensure both physical and logical controls are in place in accordance with industry best practices, prohibiting the entity, or malicious users that may gain access to the entity's environment, from obtaining access to Keys. Furthermore, service providers or vendors that provide encryption solutions to merchants who have administrative access and controls to Keys along with the management of termination points for encryption to process transactions, are required to demonstrate physical and logical controls to protect cryptographic keys in accordance with industry best practices (such as NIST referenced in PCI DSS requirement 3.6), along with full compliance with PCI DSS. Merchants should ensure their solution providers who provide key management services and/or act as the point of encryption/decryption are in compliance with PCI DSS. Merchants should be aware that encryption solutions most likely do not remove them completely from PCI DSS. Examples of where DSS would still be applicable include usage policies, agreements with service providers that deploy payment solutions, physical protection of payment assets and any legacy data and processes (such as billing, loyalty, marketing databases) within the merchant's environment that may still store, process or transmit clear text cardholder data, as that would remain in scope for PCI DSS.