

January 15, 2008

This statement is in response to the questions posed by Jim Booth representing PRISM International.

In Regards to Storage of Cardholder Data at a Third Party Facility:

PCI DSS does not prohibit the transfer of the Primary Account Number (PAN) to third-parties if it is necessary to support a merchant's business process. However, it is the responsibility of a merchant to protect the Primary Account Number wherever it may be stored, processed or transmitted. If a merchant does store PAN with a third-party, it is the responsibility of the merchant to assure that the storage of that data remains secure even when the merchant is no longer in possession of that information, as stated in Requirement 12.8. Furthermore, it is the responsibility of a merchant or service provider to assure that any third-party that stores, processes, or transmits cardholder data on their behalf is compliant with PCI DSS.

If a third-party, such as a storage facility, receives only truncated data, and the third party did not perform the truncation, the media no longer contains PAN and the merchant or service provider does not need to assure the third party's PCI DSS compliance.

If a third-party receives encrypted data which contains PAN, although the risk of exposure has been significantly reduced the resident data still contains the PAN and therefore is still at risk.

Consequently, a merchant should be confident that encrypted data at a third-party storage facility follows all relevant PCI DSS requirements. A third-party storage facility may not be required to perform an exhaustive PCI DSS assessment but rather evaluate all relevant controls depending on their business relationship with the merchant or service provider. For example, if a third party facility only provides physical storage and no cardholder data is transferred electronically to that facility then only those physical and logical controls prescribed in Requirements 7, 8, 9 and 12 of the PCI DSS would be required to be evaluated. It is recommended that a Qualified Security Assessor evaluate the relationship to determine the scope of the assessment.

In Regards to the CISP Program:

CISP is a Visa-operated program outside the influence of the PCI Security Standards Council. Any action requested of the CISP team should be directed to Visa USA.

We hope this clarifies our position for the PRISM Association and your members.