

PCI potpourri

The intent of this column is to provide updates on developments related to PCI in the airline industry and to discuss issues of general interest. Feel free to contact us at [Industry Card Services](#).

Balancing PCI DSS requirements with the risks

An Airline accepting card payment for in-flight sales was confronted with the requirement on the storage of credit card sales slips while in the air (PCI DSS Requirement 9: Restrict physical access to cardholder data; 9.6 Physically secure all paper and electronic media that contain cardholder data.)

The QSA working for this airline suggested installing safes in the planes. A radical approach that leads to question whether the cost involved (purchase and installation of a strongbox, not to mention the additional weight to be carried by the plane), is commensurate with the risk of data compromise in that specific situation.

IATA contacted an International Card Scheme, who proposed three possible ways to find a solution:

- 1) Submit the question to the PCI Security Standards Council 1)
- 2) Ask the QSA for recommendations that would service as compensating controls.
- 3) Obtain the opinion of another QSA.

This example illustrates that the PCI DSS Requirements need to be interpreted and that the costs and measures to remediate a situation have to be proportional to the risk incurred.

1) Payment Card Industry Security Standards Council:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Questions can be submitted to the PCI SSC:

On the above website, click on "FAQ" (left hand column) and then click on "Submit a Question" (top row).

Geneva, 23 January 2009

Protecting Cardholder Data on the CCCF

Requirement 3: Protect stored cardholder data.

In their efforts towards PCI DSS compliance, GDS have started to mask the card number on the CCCF (Credit Card Charge Form), in accordance with PCI DSS requirement 3.3, which states: "Mask PAN (Primary Account Number) when displayed (the first six and last four digits are the maximum number of digits to be displayed). "

The "Guidance" provided by the Payment Card Industry Security Standard Council on this subject reads as follows:

The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by

unauthorized individuals and used fraudulently. The PAN can be displayed in full form on the “merchant copy” receipts; however the paper receipts should adhere to the same security requirements as electronic copies and follow the guidelines of the PCI Data Security Standard, especially Requirement 9 regarding physical security. The full PAN can also be displayed for those with a legitimate business need to see the full PAN.

For a complete description of the 12 PCI DSS requirements, “along with guidance to explain the intent of each requirement”, please click on

https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf

Geneva, 26 January 2009

Looking for a PCI DSS compliant Payment Service Provider?

Both, MasterCard Worldwide and Visa are providing a list of card processors that have successfully completed their PCI DSS assessment.

MasterCard Worldwide:

<http://www.mastercard.com/us/sdp/assets/pdf/Compliant%20Service%20Providers%20-%20January%2015%202009.pdf>

Visa Inc.

<http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf>

Please note that you may have to copy and paste this link directly in your Internet browser.

Visa Europe

http://www.visaeurope.com/documents/ais/visa_europe_ais_certified_service_providersjan_2009.pdf

Geneva, 13 February 2009