



CISP BULLETIN

Clarifications to PCI Requirements 3.4 and 10.2-10.3

July 28, 2006

It has come to Visa's attention that certain assessors and merchants require clarification about the intent of two PCI DSS requirements. The following information is provided to help ensure your staff and customers understand these requirements.

Clarification for Requirement 3.4

PCI Requirement 3.4 states:

Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, in logs and data received from or stored by wireless networks) by using any of the following approaches:

- One-way hashes (hashed indexes) such as SHA -1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.

The MINIMUM account information that needs to be rendered unreadable is the payment card account number.

Clarification:

The use of encryption to render cardholder data unreadable is a highly effective and readily accepted way to security data. For companies that are unable to employ sufficient encryption solutions due to technical constraints, compensating controls may be considered. Only companies that have undertaken a risk analysis and have legitimate technological or business constraints will be considered for use of compensating controls to achieve compliance. Compensating controls must provide additional protection to mitigate any additional risk posed by the unencrypted data. Compensating controls considered must be in addition to controls required in the PCI DSS. It is not a compensating control to simply be in compliance with other PCI requirements.

Encryption, while a desirable approach, is not the only approach to meeting PCI 3.4.



Clarification for Requirements 10.2 and 10.3

PCI Requirement 10.2 and 10.3 state, respectively:

Implement automated audit trails to reconstruct the following events, for all system components (a series of detailed events follows at 10.2.1 through 10.2.7).

Record at least the following audit trail entries for each event, for all system components: (a series of detailed entries to be recorded follows at 10.3.1 through 10.3.6).

Clarification:

The intent of these logging requirements is twofold: 1) logs, when properly implemented and reviewed, are a widely accepted control to detect unauthorized access, and 2) adequate logs provide good forensic evidence in the event of a compromise.

Each and every log does not necessarily have to log all the data as specified in the details under 10.2 and 10.3, as long as the specified log items and events can be easily gathered in the event of a compromise from the various logs and/or logging tools in use.

There is an additional clarification specifically for requirement 10.2.1, which states "Log all individual accesses to cardholder data." The intent of requirement 10.2.1 is that if an individual (person) accesses cardholder data on their own, with their own user ID, and does not go through an application (or stored procedure, etc.) for this access, that should be logged. This requirement is often confused to mean that if an individual accesses cardholder data through an application, then all application access to cardholder data needs to be logged. It is not necessary to log all application access to cardholder data if the following is true (and verified by assessors):

- Applications that provide access to cardholder data do so only after making sure the users are authorized
- Such access is authenticated via requirements 7.1 and 7.2, with user IDs set up in accordance with requirement 8, and
- Application logs exist to provide evidence in the event of a "compromise."

We appreciate your efforts in addressing any confusion pertaining to these requirements.

For more information on Visa's Cardholder Information Security Program, please visit <http://www.visa.com/cisp>. Questions about this bulletin may be directed to CISP@Visa.com.