



INETCO and the Personal Cardholder Information Data Security Standard

The INETCO system has been designed to meet PCI DSS requirements 3.2, 3.3, 3.4, 4.1, 6.3, and 6.5 concerning storage, display, and handling of sensitive cardholder information. This means that information including Track 1, Track 2, PANs, CVVs, and encrypted PIN blocks is discarded, truncated, or subjected to a one-way hash as appropriate in the operation of the INETCO system.

As a result, sensitive information is never stored by INETCO nor displayed to users of the product in normal operation.

Implementation Details

- The INETCO Collector component, which monitors traffic and passes it onto the INETCO Processor over an SSL-encrypted data link does not store data. For further security, the INETCO Collector and INETCO Insight Processor may reside on the same physical machine if so desired.
- The INETCO Processor and Collector generates a one-way hash of the PAN to use for transaction correlation. It then truncates the PAN by inserting “*” characters prior to storage or display, leaving behind the first 6 and the last 4 characters of the PAN. The original PAN is then discarded.
- The INETCO Processor and Collector also discards any other sensitive information.
- Special memory management capabilities are used to ensure sensitive information is never swapped to disk.
- Users access the INETCO system over a web link. This link, like the Collector to Processor link, is encrypted via SSL.

Diagnostics Logging

The INETCO system offers a diagnostics logging mode that allows INETCO support engineers to work with systems administrators to fine-tune transaction decoding capabilities during the early phases of a roll-out. This feature is turned off by default. Activating it causes INETCO to generate a log of transactions it did not decode properly. This log is kept for 7 days before deletion and may contain sensitive cardholder information. INETCO recommends administrators only use diagnostics logging when absolutely necessary and take appropriate measures to protect and/or destroy the contents of the log file. Customers can also activate file encryption on the INETCO server to protect against access to this log.