10. Primary Account Number (PAN) Policy for Masking & Displaying the PAN Digits

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Administrative Systems PCI Compliance Services has established a formal policy and supporting procedures concerning the masking & displaying of the Primary Account Number (PAN). This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Administrative Systems PCI Compliance Services’ needs and goals.

Policy
Administrative Systems PCI Compliance Services will ensure that the masking & displaying of the Primary Account Number (PAN) adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed, such that only personnel with a legitimate business need can see the full PAN).
- A list of roles that need access to displays of full PAN is appropriately documented, along with a legitimate business need for each role having access to such information.
- All other roles not specifically authorized to see the full PAN must only see the masked PAN.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see full PAN.

Responsibility for Policy Maintenance
Administrative Systems PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.