Credit Card PCI Requirements

Resources:

- Section 02-04.00 Credit Card Payments for card receipting requirements
- One of many examples on the Internet of 'skimmers'
- Payment Card Industry Data Security Standard
- Section 03-04.03 Forms and instructions for documents such as "Sharing Access to EMV Inspections Responses Document"
- Court Learning Management System (LMS)

Policy:

1. Employees who process or reconcile credit card payments will annually certify through the Court Learning Management System (LMS) that they understand Payment Card Industry standards (PCI) by August 1, of each year.
2. Credit CARD EMV devices are secured if not in daily use (i.e. court sites that use devices infrequently should keep them locked; court sites that use devices regularly should secure them so person(s) who do not need to access the EMV device cannot access it).
3. Keep devices away from direct reach of the public, and only accessible when making a card payment.
4. Court standards require that any chip/swipe devices ("EMV devices") in service for the day (or any part thereof) be reviewed for any evidence of tampering.
5. Payment Card Industry (PCI) standards require periodic inspection of EMV devices to assure they have not been tampered with. Court standards require inspections be performed monthly on all equipment updating the Google "EMV Device Inspection Form."
6. Clerks of Court are responsible to add newly acquired EMV machines to their local inspection list as well as the Google doc "EMV Counter Computer Inventory" supported by IT.
7. Clerks of Court (or their assigned designee) will ensure periodic reviews are conducted and recorded.
8. Inspection forms are 'shared' with Audit.

Procedure:

Responsibility Action

1. At the beginning of each business day (or at the time the machine is first used) assure that no peripheral device has been attached to an EMV device and that the seal or sticker is intact and the device has not been opened. If there is evidence of tampering, immediately cease using the machine and notify AOC Finance. Secure the device to preserve evidence.
2. Monthly the Google Doc "EMV Device Inspection Form" is completed recording review of all devices.
3. Faulty equipment should be replaced and new devices added to both the IT inventory list as well as the local inspection forms. Contact AOC Finance for replacement machines and for proper disposal.
4. When a cashier is required to enter a virtual phone/manual payment, the card number **should not be written down** but entered directly into the EMV machine as the card holder provides the information.
5. Payment Card Industry Data Security Standard –The Payment Card Industry (PCI) Data Security Standard is required by credit card companies to ensure the safe handling of sensitive payment information and safeguarding of cardholder data.