Automated Fuel Dispenser (AFD) Fraud Prevention Best Practices

- **Monitor suspicious activity at automated fuel dispensers. Managers and employees should be continually on the lookout for the warning signs of automated fuel dispenser fraud, which can include:**
  - A single customer activating multiple automated fuel dispensers
  - Filling multiple vehicles from one automated fuel dispenser transaction.
  - Filling large non-vehicle containers.
  - Fueling several times a day (system wide and location specific).
  - Card testing (swiping, inserting, or waving payment card for authorization without pumping).
  - Island surfing (individuals walking around offering to pump fuel with their payment card in exchange for cash)
- **Routinely inspect automated fuel dispensers to ensure skimming devices and foreign hardware/software are not present.**
- **Eliminate "church key" access to mitigate automated fuel dispenser tampering. Some older automated fuel dispensers share common keys that allow service station employees and service technicians to easily gain access to the dispenser's interior. Unfortunately, fraudsters have exploited this ease-of-entry feature, using copies of the keys to gain unauthorized access.**
- **Routinely walk around automated fuel dispensers to spot suspicious activity.**
- **Apply system offline (authorization system not available) procedures as needed.**
  - Alert owner/operator headquarters of all offline issues.
  - Verify transmission is not blocked or purposely interrupted.
  - Temporarily have dispensers direct cardholders to "See Attendant" for all transactions.
  - Call the Visa Authorization Center for authorization requests that exceed predetermined transaction amount. Set lower limits at high-risk locations.
  - Make sure to imprint front of card for all manually authorized transactions.
  - For manually authorized transactions, retain card while receiving authorization and verify card security features.
  - Obtain cardholder signature and compare to back of card.
- **Minimize opportunities for attendants to engage in fraudulent behavior.**
  - Stay current on trends regarding attended fraud, such as pump attendants who accept cash while using fraudulent cards to activate the dispenser.
  - Ensure the POS communicates authorized amounts directly to the pump for dispensing.
  - Have all pump attendants enter an identification code whenever using the POS.
  - To avoid card compromise, use wireless POS so that the cardholder never loses sight of the card (or preferably, retains possession of the card).
- **Set a delay time between authorization requests to help prevent automated fuel dispenser card testing. Setting delays between authorization requests may make it less convenient for fraudsters to test stolen or re-encoded cards.**
- **Monitor quantity of fallback of chip card transactions for both magnetic-stripe read and key-entered transactions by location, POS terminal and clerk ID. A high number of key-entered transactions can be indicative of internal/external fraud or equipment maintenance issues.**
- **Clearly communicate to managers and employees the potential for automated fuel dispenser fraud, as well as security measures and procedures they can employ to minimize fraud exposure.**