Sinclair's PCI Program FAQ

YOU'VE GOT QUESTIONS. WE CAN HELP.

Do I need to spend money upgrading my pumps for PCI compliance?

Visa requires that all new pumps have PCI approved pin pads (called EPP or Encrypted Pin Pad) that will help to secure debit card PINs. EMV (Chip & PIN) support is currently slated as a requirement by October 1, 2017 for fuel transactions. If you currently do not accept debit, but decide to accept debit, Visa considers that a new installation. Any PRE-PCI devices are required to be replaced with a PCI compliant device by December 31, 2014. Visa PIN requirements can be found at http://usa.visa.com/merchants/risk_management/cisp_pin_security.html

Do I need to upgrade my point-of-sale software every time a new version is released?

It has never been Visa's or the PCI Councils intent that you change POS software every time a new version is released. At a minimum you should ensure you have a PCI compliant version to avoid fines or noncompliance fees. Sinclair posts minimum acceptable versions at https://www.sinclairoil.com/pciprogram/pdfs/pos_matrix.pdf

Skimming seems to be a hot topic, where should I focus my attention?

The most cost effective solution at this point is to secure your physical pumps using unique keys that replace the generic keys that are currently used to secure the credit card system. If you have solutions in place to prevent gas theft – training, cameras, etc – make some adjustments to include the credit card system. Skimming devices are often designed to fit over or inside credit card readers and will often store data or transmit it nearby using Wi-Fi or Bluetooth signals. Employees should regularly look for any unusual signs of tampering with the pumps. Visible cameras can be a great deterrent.

Do I need to get my store employees involved in of this?

Employees should not be overlooked when it comes to protecting your location from data theft. They can play a significant role in protecting your customers and your locations reputation. Sinclair provides a set of policies, procedures and basic security awareness training that should be used at a minimum to show you are aware of and have an interest in protecting your customer data.

My local equipment provider says I need to install this new "PCI" or "Data Security" device because Sinclair said so, how do I confirm this?

Many locations have saved time and money by contacting our tech support group before upgrading equipment. Call Sinclair Tech Support at 800-524-4799 or contact the PCI Program at 800-576-3466.

Does this new "PCI Gap and Skimming Coverage" mean I don't have to worry about PCI Compliance?

The new PCI Gap and Skimming Coverage helps cover losses that PCI Compliance cannot completely prevent – like skimming and employee fraud. PCI Compliance is a contractual requirement of accepting Visa, MasterCard, American Express and Discover credit cards. Ignoring PCI Compliance is a business risk that could mean increased fines, fees or inability to process cards.

I want to provide wireless internet access to my customers. Do I need to worry about data security?

Anytime a signal is being sent wirelessly there is a chance of it being intercepted or altered, it is generally much better to use a wired transmission system and also necessary to completely separate the payment and other data connections. Payment data should never be sent across a wireless network.

Have a question you don't see here? Contact the PCI Program at 800-576-3466

Last Revision 11/07/2013