

frequently asked questions about **Card Data Security**

Q. What is PCI and why is a POS upgrade needed?

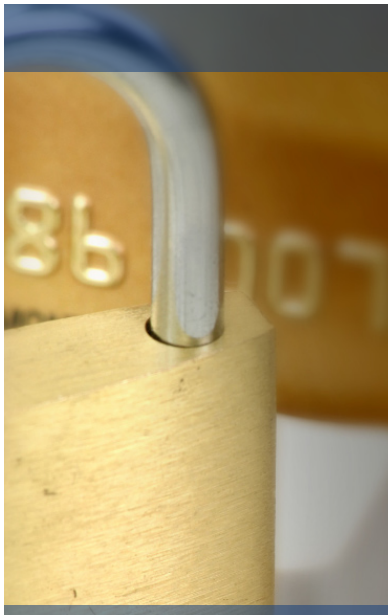
A. PCI is the acronym associated with the Payment Card Industry Data Security Standard, which details 12 standards for the secure storage and handling of card data. The PCI standard applies to all card brands. In a merchant's credit card processing contract, the merchant agrees to hold such data in a secure fashion and is contractually responsible for damages if it is stolen. The bankcard associations (Visa, MasterCard, etc.) have been aggressive in fining merchants with little to no leniency.

If you are using an older system, you are at a higher risk of card data theft. Contact your POS dealer about upgrading to a Payment Application Best Practices (PABP)-compliant

version of software. To see a list of PABP-validated systems, go to www.visa.com/pabp. Once transactions have been settled, there is no longer a need to store the data except in a truncated form. Mercury can provide the full card number associated with a transaction if it is ever required in the future.

Q. Who is liable for a data security breach?

A. The merchant is responsible. The fines are levied in proportion to the number of card numbers that are lost and also can be increased if additional factors are involved such as the storage of full track data (which is strictly prohibited). We have seen fines that exceeded \$100,000 for the loss of a modest number of cards.



Q. Why is this happening now?

A. The payment card industry became aware of the enormity of the dangers of the electronic storage of card data after several high-profile thefts. The first to receive scrutiny were payment processing companies. The next groups were large merchants and e-commerce sites. Now, mandates have been announced requiring that even small merchants become PCI compliant. By 2010, every merchant must use a PABP-compliant system.

Q. What else is needed besides the upgrade?

A. Take basic steps to ensure computer and network security. Internet connected sites should have a firewall protecting them

from unsolicited external connections. Remote access passwords should be complex and not shared amongst sites. But the main thing that can be done is to reduce the amount of sensitive data that is stored and to encrypt whatever is stored. This is the focus of the upgrades for PCI compliance.

Q. Will there be a charge for this upgrade?

A. PCI compliance is mandated by the bankcard associations (Visa, MasterCard, etc.), who have put an enormous burden on the POS systems developers and dealers to comply and certify their products. The POS systems providers are working very hard to protect your interests and will

likely request compensation for the upgrades/services depending on your individual relationship and business agreements.

Q. Why is Mercury doing this?

A. We feel we have a duty to inform our merchants about this issue since you have primary liability in the event a card data theft is traced back to your business. Getting the latest software version installed is insurance against this liability.

