



Frequently Asked Questions About Card Data Security

What is PCI Compliance?

Visa, MasterCard, American Express and Discover have joined forces to establish standards for handling and storing credit card data that are intended to prevent the theft of credit card data. They have identified twelve components to ensuring the security of credit card data and published them in a document known as the Payment Card Industry Data Security Standard. PCI and DSS are acronyms used to describe this document.

POS Systems that handle and store credit card data in a manner consistent with these 12 standards are deemed to be "PCI Compliant". A key element of PCI Compliance in a POS System relates to the handling of personal and account information stored on the magnetic stripe on the back of a credit card. Storage of "full track data" is strictly prohibited and whatever truncated data is stored must be protected in very complex and specific ways.

Visa and MasterCard have a strict certification process for determining which POS Systems are PCI Compliant. Restaurant Manager v17 meets the standard for certification as a PCI Compliant POS System.

Who is liable for a card data security breach?

All merchants that accept Visa or MasterCard sign a credit card processing contract which holds them responsible for handling credit card data in a secure fashion and makes the merchant responsible for damages if credit card data is stolen. In other words, the credit card processing contract holds merchants responsible for any breaches in security.

Fines are levied in proportion to the number of card numbers that are lost and whether or not the merchant was storing full track data. Fines in excess of \$100,000 have already been levied even for the loss of a modest number of cards.

How can a data security breach be prevented?

First and foremost, merchants must upgrade to a PCI Compliant POS System. They must also delete previously recorded credit card data from existing electronic files and backups. And finally, they must enhance the overall security of their computers and network. Internet connected sites should have a firewall protecting them from unsolicited external connections. Remote access passwords should be complex and not shared amongst sites.

How much does it cost to upgrade to a PCI Compliant POS System?

The cost of PCI Compliant POS software is based on the number of POS stations on the network. However, installation of new software is only one step in establishing PCI Compliance. Identifying and deleting all existing files that contain credit card information can be a time consuming task, the scope of which must be determined by a professional survey. The cost of installing a firewall and further enhancing the overall security of a computer system is also dependent on the scope of the work and the security systems already in place.