

How PCI Affects Restaurateurs

Given consumers' expectation of universal acceptance of credit and debit cards, a restaurateur's validation that they are protecting their customer's personal information is good for business: In any competitive business – no restaurant owner would want to be named as the eatery where card data was stolen.

Protects Ability to Accept Credit / Debit Card Payments – non-compliance and/or a breach can endanger a restaurant owner's ability to accept credit/debit payments. There are many cases that 80% to 90% of transactions are from credit/debit card accounts. Losing your store's ability to accept credit cards means reduced customers.

Impact of State Privacy Laws

A breach that discloses personal credit card information with any of the 40+ States governed with privacy laws may experience double impact on the side of the restaurateur. Being off-side with PCI could result in fines and litigation costs. Being off-side with State Privacy Laws is a felony with potentially more serious penalties.

Compliance / Security Strategy

Ensure you are using a PA-DSS or PABP validated POS system. Make sure you're using an approved PED. Have regular security awareness training for your staff – particularly supervisors. Doing a background check on your employees with administrative access to your system is a must. Have a 'Confidentiality Agreement' contract with your employees. Carefully and accurately complete the PCI Self Assessment Questionnaire (SAQ) – if you are not sure – ask. If gaps in PCI compliance are identified, develop a realistic plan to correct them. Maintain mature controls to sustain compliance. Proper storing of your strong passwords and secure passwords and monitoring to detect attack and record evidence is critical. Control your wireless access points and maintain a secure configuration for each network. Have an Incident Response Plan and test it to make sure that it's always ready for action.

For less than \$15,000 a qualified security specialist can visit your restaurant and make sure you are compliant with today's rules which are subject to change with each future revision to the PA-DSS standard.