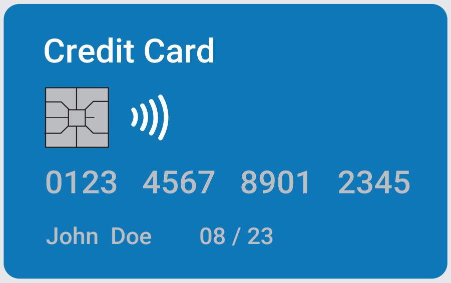
SpeedLine
Rely on it.

Credit Card Security

Credit card fraud is a serious risk for restaurant operators.



Did you know that more cases of credit card fraud or identity theft happen in restaurants than anywhere else? According to payment industry statistics, it is safer to use a credit card on the internet than at a restaurant or bar.

Fraudsters specifically target restaurants because they are one of the only businesses where customers have typically given their credit cards to someone who leaves their sight to process the payment. And they're targeting independents and small chains in particular because they have fewer resources to put into payment card security and PCI compliance. Skimming, tip fraud, and hacking are real dangers for restaurant operators.

In fact, a recent study by global payment security consultant Trustwave showed that nine out 10 cardholder data compromise incidents were aimed at small merchants: *52% of them in foodservice*. More than twice as many attacks targeted card-present transactions at the point of sale as targeted online transactions.

A feature article on RestaurantPartner.com, "Restaurants and Credit Cards – A Dangerous Combination," related this example from an Atlanta Bread Co. restaurant in Kansas City:

> When a hacker compromised their credit card processing system it tallied up a bill of over $25,000 and counting. They were threatened with fines up to $1 million and had $16,000 pulled from their bank account without notice. This prohibited them from buying food for a period of time and then they had to spend $7000 upgrading their POS system. Luckily, they were able to weather the storm and stay afloat. Unfortunately, many restaurants maintain a very tight cash flow and such a blow could easily put them out of business.

A breach can be devastating to a restaurant, leaving the operator or franchisor financially liable and forced to rebuild a damaged reputation.

The Payment Card Industry (PCI) standards have been established to help you safeguard your customers' cardholder data – and protect your business.

Your POS System is a Key Factor in Safeguarding Your Business

One of the most important requirements of the PCI Data Security Standard is the use of point of sale/payment processing software such as SpeedLine POS that has been validated compliant.

Why You Should Care

The risk to your business in the event of a breach, of course, is the #1 reason to be careful about choosing a PA-DSS validated point of sale application. But there's another reason, too: Since 2010, merchants (including restaurant operators) have been required to use only PCI PA-DSS validated point of sale and payment applications.

Financial institutions enforce the requirement for an annual PCI security self-assessment and quarterly network scans, and can levy fines for non-compliance. If your POS system is non-compliant, you will *automatically fail* your PCI assessment, and could lose the ability to accept credit cards.

SPEEDLINE™
Rely on it.

Credit Card Security

PCI Compliance At SpeedLine

A credit card data breach can be devastating to a restaurant, leaving the operator or franchisor financially liable and forced to rebuild a damaged reputation. That's why we made the decision to submit the entire SpeedLine product to a rigorous security audit.

And this is critical:

Some POS companies have chosen not to make the sizable investment required to earn PA-DSS validation. Others have taken a short-term approach, submitting only the payment processing components of their software for validation.

At SpeedLine, we chose instead to give our customers the assurance of PCI compliance by validating the entire SpeedLine POS product line. This involved an intensive third-party audit of all of our products, peripheral applications, and all company processes relating to product development, training, and data security.

The SpeedLine software has been secured and verified top to bottom. Safeguards are in place at multiple levels to prevent unauthorized access to confidential data, and training and documentation is available to help you install SpeedLine securely as a key component of a PCI-compliant restaurant operation.

Qualified Integrator And Reseller (QIR) Certification

Organizations like SpeedLine that are qualified by the PCI Security Standards Council as Qualified Integrator and Reseller Companies (QIR Companies) are authorized to implement, configure, support, and perform Qualified installations of validated PA-DSS Payment Applications. The QIR certification means you can be confident that SpeedLine has been installed in a manner that supports your PCI DSS compliance.

EMV

Effective October 1, 2015, liability for card present transaction fraud was shifted to the merchant. You can avoid this liability by processing card present chip card transactions through an EMV PIN pad. SpeedLine supports EMV and provides compatible PIN pads.

E2EE and P2PE

Beyond EMV, adding encrypted PIN pads on all stations allows you to safeguard your customers' data with end-to-end (or point-to-point) encryption. This ensures that no credit card information is stored or transmitted through the POS system. With end-to-end encryption, you can greatly reduce the restaurant's PCI scope, security costs, and risk.

Contact Us:

SpeedLine Solutions Inc.
1-888-400-9185 | www.speedlinesolutions.com