

A large, brass padlock with a silver key inserted is positioned diagonally across the top half of the page. The padlock is resting on a stack of credit cards, including a blue one in the foreground and a red one partially visible behind it. The background is white.

# Fighting Fraud

## Credit Card Security Protects Your Bottom Line

Where once cash was king, now credit cards have become the life's blood for operators in the foodservice and hospitality industries. Customers enjoy the convenience and ease of paying from their table, and operators enjoy increased profits and a happier, more loyal customer base. But as credit card use increases, opportunities for credit card fraud also rise. This is a big worry for the consumer, of course, but it's the operator who could face audits and large fines from credit card companies. For this reason, operators need a reliable partner who can help them comply with the rigorous standards of the credit card industry.

MICROS Systems, Inc.—a long-time industry leader in point-of-sale systems and a SYSCO iCare partner—fills this need. As Director of Operations for North American Distribution, David Straub points out that MICROS works hard to adhere to the steep guidelines of the Payment Card Industry Data Security Standard (PCI DSS). “It’s an initiative that was started by Visa/MasterCard about three years ago,” says Straub.

"We go through a rigorous certification process with Visa to become PABP (Payment Application Best Practices) compliant with their standards," Straub says. "In fact, all of our products listed on the Visa Web site are PABP certified."

MICROS's compliance is as important to the operator as it is to the consumer, as fines for non-compliance are hefty. "Some merchants are being fined upwards of \$100,000 because there was a breach and their credit card security practices aren't up to PCI standards," Straub said. In fact, according to Visa's Web site (<http://usa.visa.com>), operators can be penalized up to \$500,000 *per incident* if their system is compromised while not in compliance.

have the R&D resources to put into new software enhancements and to quickly deploy the upgrades to the merchant," Straub says. "We stay on top of software development. We've been on the forefront, trying to educate our merchants that this is an issue."

In the past, some credit card scanning machines could store data that was embedded in the magnetic stripe of the card. This stored information was sometimes used to reprint receipts—a convenience for both the operator and the customer. But it also opened up a vulnerability that could be exploited. "Hackers can penetrate systems that are not secure," Straub says. "They can capture sensitive information and use it to create fraudulent cards. It's something that's taken very seriously in the industry."

## "Some merchants are being fined upwards of \$100,000 because there was a breach and their credit card security practices aren't up to PCI standards ..."

"The credit card companies lose a lot of money from credit card fraud," says Straub, which could be considered an understatement. According to the Federal Trade Commission's Consumer Fraud and Identity Theft Complaint Data report, credit card fraud was to blame for a loss of \$56.6 billion in 2006.

MICROS is pushing forward on the compliance issue by continually upgrading its software and encryption technology. "We work hard to stay on top of the changing requirements that Visa mandates. We

How can merchants help prevent this kind of fraud? Straub recommends getting the latest software updates that are listed as PABP certified on Visa's Web site and considering equipment upgrades as well. "Only the latest versions of our software are completely PABP certified," says Straub. "It's the merchant's responsibility to make sure they're meeting Visa's guidelines."



To learn more about how SYSCO *iCare* and MICROS can help you secure your credit card transactions and become PCI compliant, visit the *iCare* Web site at [www.syscoicare.com](http://www.syscoicare.com).