

# New Security Standards in 2011

Revised payment-processing guidelines will go into effect Jan. 1 for restaurateurs accepting credit or debit cards. [By Barney Wolf](#)



Restaurants and other businesses that capture and store credit and debit card data on their computers will be required to meet updated security standards beginning next year.

Version 2.0 of the guidelines, developed by the PCI Security Standards Council, doesn't include major new requirements. Instead, it contains some revisions and clearer guidance for merchants and others who must make sure that security meets the council's criterion.

"Feedback that we've gotten really didn't call for any major changes to the standards," says Bob Russo, general manager of the council, which was established by the payment card industry. "That is a testament that the standards are pretty solid."

The new version was announced in late October and becomes effective January 1. Systems that met the standards' previous version have additional time to make sure they comply.

Russo says the new guidelines deal with security of payment account data as well as payment applications—the computer software that processes, transmits, and/or stores card data electronically, including restaurant point-of-sale systems.

"One of the biggest things that merchants, including restaurants, need to understand is where the cardholder data is on their network," he says. "We are finding that the information is being stored in areas that the business never knew about."

To help small businesses comply with PCI standards, the council updated its website, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org), to include more user-friendly language, forms to help merchants self-evaluate their compliance, and a list of software that meets the guidelines.

Experts say fraud resulting from the theft of payment-card data remains a huge problem in America, despite security improvements. Card fraud costs the U.S. card-payments industry \$8.6 annually, according to a report by Boston-based research firm Aite Group.

“We’ve been seeing an increase in different types of attacks,” says Eric Knight, senior knowledge engineer with LogRhythm, a Boulder, Colorado-based security management company. “Cyber criminals are willing to use more creative and innovative methods. Card fraud used to be more opportunistic. Now, it is more organized.”

In one recent cyber attack, for instance, a retailer’s payment terminals were manipulated in dozens of stores, resulting in possible data theft from thousands of payment cards.

“This isn’t some kid tampering with the magnetic strip reader,” Knight says.

Data theft can have severe repercussions for merchants. They may suffer financial losses, fines from card providers, and, more importantly, damage to their reputations, which would create long-term consequences, such as losing customers and sales.

Consumers worry about payment card scams and the potential for identity theft, as well. Nearly two-thirds of Americans say they are seriously concerned about credit and debit fraud, according to a survey conducted earlier this year for Unisys Corp.

As a result, many restaurants and other businesses are looking more seriously at protecting their information systems, including the development of data retention and disposal programs, password management rules, and anti-virus benchmarks.

“When the PCI [standards] first came out, a lot of organizations, retailers, restaurants, and others, looked at these as nice guidelines, but not much more,” says Barak Feldman, senior systems engineer with Cyber-Ark Software, an information security company with offices in Newton, Massachusetts.

One of the biggest things that merchants, including restaurants, need to understand is where the cardholder data is on their network.”

He says a company’s risk assessment a few years ago could have determined that the cost of losses and fines outweighed the price of meeting the standard. Not anymore.

“Today, if you are not PCI-compliant, you are considered to be backward,” Feldman says. In addition to addressing current security issues, the new standards also have an eye on the future, says PCI councilman Russo.

“Going forward in 2011,” he says, “we are concentrating on some of the other technologies that will be a growing part of the payment-card industry, including point-to-point encryption, mobile-pay systems, and payment cards that have integrated chips.

The updated PCI standards will be covered in greater depth, followed by a question-and-answer period, during a webinar at 3 p.m. (Eastern Time) November 16 and at 11 a.m. (ET) November 18. To register go to <https://www.pcisecuritystandards.org/training/webinars.php>.

The PCI Security Standards Council was formed in 2006 by MasterCard, Visa, and other networks to manage the evolution of the payment-card industry. The latest standards were developed in response to thousands of comments from merchants, banks, processors, and others, and after a pair of community meetings in the U.S. and Europe.

Barney Wolf is an Ohio-based freelancer for QSR magazine.