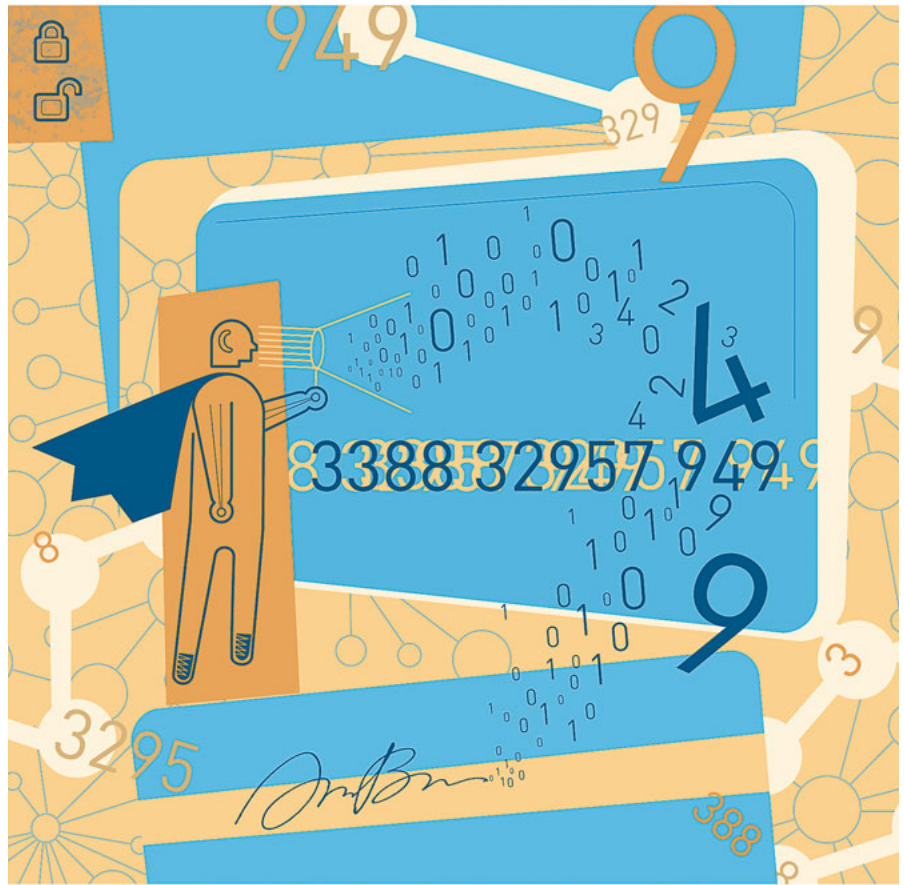


# Extra credit

The Payment Card Industry standard—and what it means to your business.

BY TRACY THOMPSON

Illustration by Celia Johnson



**LOVE 'EM OR HATE 'EM**, credit cards are a way of life—for businesses as well as for consumers. Because credit card acceptance is almost a necessity, more and more merchants are adopting Internet-based point-of-sales systems. These systems speed up transaction processing and capture a wealth of customer and inventory data. But to reap these rewards, merchants must take measures to protect cardholder information.

The Payment Card Industry (PCI) security standard ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) mandated by Visa, MasterCard, and other card issuers requires that “all merchants with internal systems that store, process, or transmit cardholder data” comply with 12 key data protection measures and submit to security audits. Companies that fail to play by the rules could face penalties of up to \$500,000 in the event of a security breach.

Compliance requirements kick in with more than 500,000 transactions per year or \$125,000 in transactions per month, depending upon the card issuer. However, merchants who fall well under those levels still face significant risk. Every

company in the payments supply chain is potentially subject to penalties and costs should a security breach occur.

“PCI requirements include maintaining a working firewall, updating security patches and antivirus programs, encrypting cardholder data transmitted across public networks, and assigning unique IDs to employees with computer access,” says Scott Gaines, director of security sales at F5 Networks. “Even if your company isn’t directly affected by PCI rules, these measures can help prevent a potentially costly and embarrassing security breach.”

## F5 offers protection

F5 products address many of the PCI requirements for protecting sensitive data. For example, the BIG-IP Local Traffic Manager inspects traffic flow and can identify malicious activity deeply embedded in network and application protocols.

F5’s FirePass, an SSL VPN device that provides secure remote access for people working at home or on the road, enables selective SSL encryption to efficiently protect data in transit between the end

user and the applications. It can also monitor network connections for policy compliance, and control and restrict access to applications and data. All F5 products address the issue of unique user identification and management, working together to create a secure, role-based data access path.

The specifics of the PCI standard continue to evolve to address changing security threats. PCI version 1.1 was released in September 2006 when American Express, Discover, JCB, MasterCard, and Visa jointly announced the formation of an independent council designed to manage the standard.

The new rules require that merchants implement a Web application firewall such as F5’s Application Security Manager. This product guards against both targeted and generalized application attacks and can detect information loss—imperative for businesses that literally can’t afford to have credit card data fall into the wrong hands. \*

Tracy Thompson is editor in chief of F5 World.