



# Fighting Identity Theft

## PCI-Compliant Networks Help Retailers Manage Security Risks

**M**assive cases of identity theft are making big news today at an alarming rate. The rise of customer identity theft threatens not only individual consumers, but also the security—and the reputation—of every retailer. Security breaches undermine customer trust in online transactions and can have far-reaching financial consequences for customers, retailers, and credit card issuers.

In response to rising security concerns, VISA and MasterCard jointly developed the Payment Card Industry Data Security Standard (PCI DSS) in 2004 to assure customers that their bank card transactions would be secure from identity theft. The PCI standard requires merchants to meet stringent security objectives such as maintaining a secure network, protecting cardholder data, regularly monitoring networks, and maintaining an information security policy.

Non-compliance with the PCI standard can have costly consequences, ranging from stiff fines to being banned from processing credit, debit, and gift cards—effectively strangling a company's operations.

### Progress toward Compliance

Hughes conducted an informal survey of restaurant executives attending *Hospitality Magazine's* 2007 MURTEC tradeshow in March to learn about the progress businesses are making toward PCI compliance. The survey found that four out of five executives surveyed believed that their companies had made significant progress toward PCI compliance by addressing their point-of-sale and back office systems. Although the vast majority had yet to achieve full end-to-end network PCI compliance, nearly all of those surveyed indicated that the standard is important to their business and they are actively working to achieve compliance.

### Making It Easier

Because the cost and complexity of establishing a PCI DSS-compliant transaction architecture can be significant, many retailers are choosing to work with service providers such as Hughes who can make the job easier. Hughes offers a range of PCI DSS-compliant services from the retailer's remote store LAN to the credit card authorizer from its network operations center (NOC) that fully complies with the stringent PCI DSS requirements.



Hughes' solutions can achieve compliance across multiple network architectures, including satellite and DSL access technologies. As one of only a handful of managed network service providers to have received the PCI DSS certification, Hughes can create solutions that readily interface with a retailer's existing equipment, making it easier to deploy PCI-compliant solutions.

"There is clearly both awareness and urgency at the national brand management level, but the industry still needs to ensure that merchants, including franchisees, understand that PCI compliance is more than protecting their point-of-sale systems," said Douglas Medina, Hughes senior director of enterprise marketing. "Complete end-to-end compliance—including data, point-of-sale devices, networks, and physical security—is the responsibility of all individual merchants regardless of size."

PCI compliance is one of the important steps that businesses can take to stem the rise of identify theft. When a single, high-profile security incident can expose customer identities and irrevocably damage a company's credibility and reputation, network security compliance brings its own unique return on investment. And Hughes simplifies the job, so businesses can stay focused on business.

LEARN MORE: visit [enterprise.hughesnet.com](http://enterprise.hughesnet.com) to obtain a "Low Risk, High Reward" white paper about PCI compliance. ■