



PCI Compliance: Low Risk, High Reward

***How Hughes' PCI Compliant Network Solutions Reduce
Costs, Save Time, and Preserve Customer Loyalty***

September 2007



Low Risk, High Reward

Overview: Data Security and Reputation Management in the New Economy

Reputation is the most prized asset for any business. When your business' reputation is damaged from a breach of data security, customer trust suffers. When customer trust suffers, sales are impacted and market position threatened.

The public relations costs alone of repairing the damage done to a retailer's reputation can be catastrophically high—and even at that, the customer loyalty that was lost may never be regained. A golden rule in business is that it is less costly to retain your existing customers than to find new customers.

In today's economy, the biggest threat to a retailer's reputation is customer identity theft by hackers and ever more sophisticated organized crime attacks. Security breaches damage the customers' trust in online or electronic transactions with the retailer. The financial impact to a retailer from a breach can be enormous.

To stem the rise of identity theft, a group of payment card issuers established a standard in 2004 to bolster electronic networks against customer identity theft. Known as the Payment Card Industry Data Security Standard (PCI DSS), compliance with this set of security requirements is now a mandatory requirement with many credit card issuers, including Visa, MasterCard, American Express, and Discover. Retailers who engage in electronic transactions and are not compliant with the PCI DSS requirements are subject to stiff penalties in the event of credit card data theft.

The cost and complexity of establishing PCI DSS-compliant transaction architecture is not insignificant. The time required by retailers to establish total end-to-end compliance on their own, compounded with the time and expense of PCI DSS audits by third-party security certification companies, build a compelling case for working with vendors and service providers who can make the job easier.

Hughes Network Systems, LLC (Hughes) offers a range of PCI DSS-compliant WAN services that fully complies with the stringent PCI DSS requirements and greatly facilitates retailers' attainment of PCI certification.

This white paper reviews the PCI DSS requirements and penalties for noncompliance, as well as the elements of a compliant transaction network such as those offered by Hughes.

When your company's reputation can be irrevocably damaged by a single high-profile incident of identity theft, network security compliance is a small price to pay. Hughes simplifies the job, so you can focus on your business.

1.0 The Business Impact of Identify Theft

From security breaches at BJ's Wholesale Club in 2004 and CardSystems in 2005 to Citibank in 2006, high-profile incidents of identity theft over retailers' transaction networks are numerous and

Low Risk, High Reward

widespread. And there's no sign that the trend is slowing. In fact, the San Diego-based research group Privacy Rights Clearinghouse said more than 100 million records of U.S. residents have been exposed by security breaches since February 2005.

According to a Gartner report written by Avivah Litan and John Pescatore entitled "Answers to Common Questions about PCI Compliance," by year-end 2007, Visa and MasterCard will have levied fines on up to 50 Level 1 and Level 2 merchants for non-PCI compliance related to storing magnetic card data. Recently Visa started paying much more attention to about 800 Level 2 merchants, who must be compliant by 30 September 2007. According to the report, "most will miss their deadline¹."

The PCI DSS standard was developed jointly by Visa and MasterCard in 2004, just as these incidents first were garnering media exposure. The standard was intended to assure customers that their bankcard transactions would be secure from identity theft at the point of sale, over the Internet, on the phone, or even through the mail.

Complete end-to-end compliance—including point-of-sale devices, networks, and physical security—is the responsibility of all individual merchants regardless of size or volume transactions they process.

"When your company's reputation can be irrevocably damaged by one high-profile incident of identity theft, network security compliance is a small price to pay. Hughes simplifies the job, so you can focus on your business."

The consequences of noncompliance with the standard will, at a minimum, be costly to retailers and can be disastrous. Fines to a merchant for a single incident of identity theft over a noncompliant network were originally set as high as \$500,000. The merchant could also be restricted from card acceptance programs—or expelled altogether. If this were to happen, the merchant would be prohibited from accepting credit cards, stored-value/gift cards, etc., which could put a small- to medium-sized retailer out of business in a hurry.

These fines increased on March 31, 2007. Noncompliance fees for storage of sensitive authorization data are levied at the rate of \$10,000 per month for any company that fails to confirm that their Level 1 and 2 merchants are not storing full track data, PIN block data, or CVV2/CVC2/CID post-authorization. The penalties mount up if progress is not made to correct the problem. On June 1, 2007 the fines were increased to \$50,000 per month. Beginning September 2007 the same violation will be punishable by a \$100,000 per month fine.

2.0 PCI DSS Background and Requirements

The PCI DSS standard is an outgrowth of Visa's Cardholder Information Security Program (CISP). In effect since June 2001, CISP was created as a means of protecting Visa cardholder data in the transaction network—ensuring members, merchants, and service providers of the highest possible information security.

¹ Answer to Common Questions About PCI Compliance, Gartner Report by Avivah Litan and John Pescatore

Low Risk, High Reward

The CISP requirements were incorporated into PCI DSS to create a common set of industry security standards. Since September 7, 2006, the PCI Security Standards Council owns, maintains, and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Visa USA, however, continues to manage all CISP compliance enforcement and validation initiatives.

The PCI DSS requires merchants and member banks to demonstrate that they meet 6 security objectives, following 12 separate operational requirements and 221 sub-requirements. The 12 high-level requirements are as follows:

- **Build and Maintain a Secure Network**
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
 - Requirement 5: Use and regularly update antivirus software
 - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - Requirement 12: Maintain a policy that addresses information security

These security requirements apply to all “system components”—that is, any network component, server, or application that deals with cardholder data or sensitive authentication data.

Network components scrutinized under this standard include firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers are also affected, including Web, database, authentication, mail, proxy, network time protocol (NTP), and domain name servers (DNSs). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Not only is there an impact to brand reputation and the expense of large fines if found not compliant, deploying a network that adheres to the standard can be costly. If you process credit card information and an audit indicates that you are not end-to-end compliant with the PCI DSS standard from the time the customer’s credit card data is taken to final credit authorization, your company

Low Risk, High Reward

may be required to rework major portions of your application code or install additional network components to your architecture to protect applications.

In light of the complexity of implementing and maintaining PCI compliance, merchants and retailers can benefit greatly by working with vendors and service providers that can help meet the standard.

As a provider of certified PCI-compliant broadband networking solutions, Hughes can help reduce the overall expense and time of deploying a retail network that meets the stringent PCI guidelines.

3.0 Architecture and Network Compliance

A compliant architecture establishes a data “demilitarized zone” between the end customer and the merchant’s headquarters-based payment processing applications. Payment processing applications pass through a firewall—a Web-application firewall, for example—then through a network firewall, through the network itself, and ultimately connect with the end customer through a variety of point-of-sale interfaces such as credit card terminal, cash machines, etc.

There are three major segments in PCI DSS-compliant retail architecture (see **Figure 3-1**):

1. The retail store local area network (LAN) and devices
2. The credit card authorizer storage servers
3. The wide area network (WAN) that extends from the store LAN to the credit card authorizer

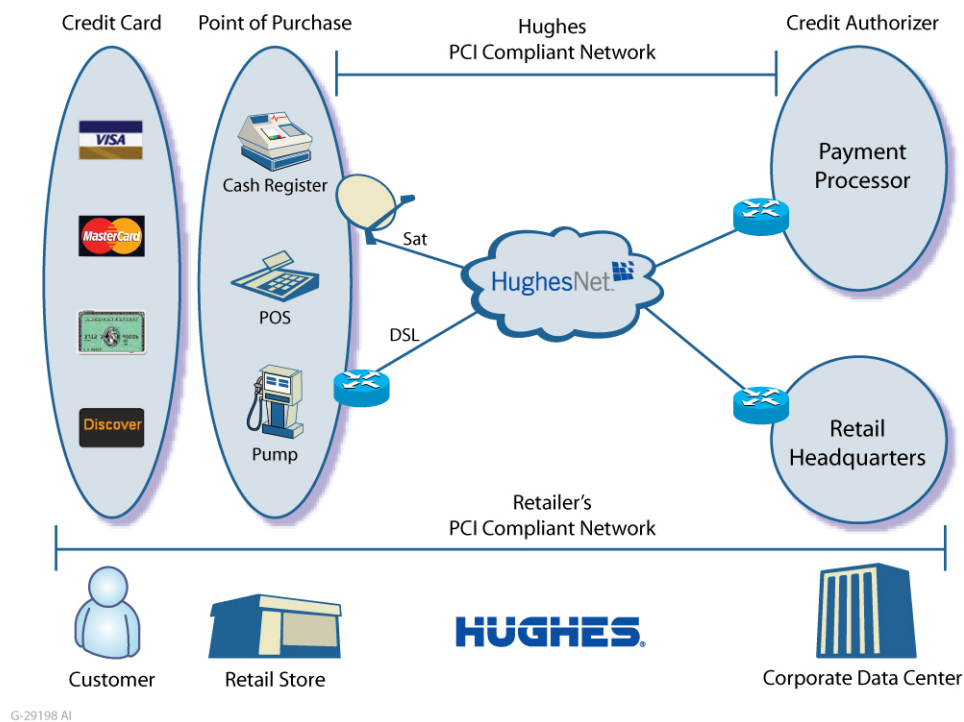


Figure 3-1. End-to-End PCI Compliant Network with HughesNet®

Low Risk, High Reward

Perhaps the largest part of PCI DSS-compliant architecture is the WAN itself.

Hughes, the global leader in managed network services utilizing both broadband satellite and terrestrial technologies, is one of only a handful of managed network service providers to have received a Protection of Cardholder Information (PCI) Data Security certification. Of over 250 companies considered compliant by the Cardholder Information Security Program (CISP), Hughes is one of only nine companies certified for transmission of credit card information. Of those nine, Hughes is the largest managed network services company, with more sites under management than any other provider on the list.

To be a PCI-compliant service provider, networking companies must address network operations processes and procedures, as well as network architecture. To this end, Hughes has made significant investments in Network Operations Center (NOC) infrastructure, remote equipment, and day-to-day business processes to address the full scope of PCI security requirements. Hughes' system engineers and professional service experts understand the complexities of PCI DSS compliance. As a result, the company can create solutions that readily interface with a customer's existing equipment, making it easier to deploy PCI-compliant solutions for its customers. Thus, Hughes' certification ensures the retailer's WAN meets PCI standards.

Hughes PCI-compliant network architectures, involving both satellite and DSL access technologies, encompass the following key attributes:

- The Hughes NOC is PCI DSS compliant in both technology and business processes
- HughesNet® Network Services, comprising Optimized VPNs and High Availability VPNs, can be configured to be fully private, never touching the Internet from credit terminal to authorizer, or encrypted if a public network is traversed
- Hughes' customer-premise equipment (DSL or satellite routers) can interface with a customer's secure point-of-sale device without any modifications
- Hughes can provide purpose-built interfaces to convert legacy protocols, such as serial, to IP and secure the transport of transactional data

As part of its initiative to develop and provide fully compliant and certified solutions, Hughes engaged Internet Security Systems (ISS). ISS is a business unit of IBM and is a recognized Qualified Payment Application Security Company (QPASC) that has met the requirements to perform PCI Application Security Assessments to validate payment applications. This independent analysis played a key role in the design and implementation of Hughes' PCI-complaint solutions.

4.0 Conclusion

In light of the risks involved with credit transaction security and the key role the WAN plays in data security, choosing a managed network service provider with experience in this critical aspect of your transaction processing environment can greatly speed and simplify attainment of overall PCI compliance. Hughes offers PCI DSS-compliant solutions for both VPN over the Internet and private network configurations, offering retailers maximum flexibility in deployment of a network solution that is best suited to their overall business needs and priorities. When you ask for PCI

Low Risk, High Reward

DSS-compliant architecture for your network from Hughes, you have simplified PCI compliance for your company.

The PCI DSS compliance requirements for any business that takes credit cards can be truly daunting both from the WAN and LAN perspectives. The retailer's headquarters-based, back-office applications and servers, not to mention the possibly hundreds of remote locations/stores LAN architectures, all must be PCI complaint. Why not rely on a service provider, like Hughes, with the experience and know how to manage your WAN with a fully PCI-compliant network architecture. Investing in PCI DSS compliant architecture from Hughes frees you to focus on your business and your customers.

5.0 Case Study: BP Speeds Customers on their Way... Securely

Consumers expect a very quick stop when it's time to fuel up at the local gas station. Most customers swipe a credit card, pump their gas, perhaps pick up a gallon of milk or a cup of coffee, and move on in a matter of minutes.

Those customers don't think a lot about the network that keeps operations running smoothly behind the scenes—from credit and debit card authorizations, to tank-level monitoring, to inventory management. But nothing is more important to BP Products North America than the efficient operation of its 14,000 stations nationwide.

To help speed its millions of customers on their way, BP deployed HughesNet Optimized VPN service to connect its retail locations throughout the U.S. HughesNet Optimized VPN service, part of the suite of Hughes Managed Network Services, is a fully managed broadband offering that creates a seamless network service by using the most efficient and cost-effective technology available at each site—whether satellite or terrestrial.

With the HughesNet solution, not only do the store POS systems have access to secure high-speed networking, the network connections can be made available at each fuel pump as well. While connections were installed to improve credit and debit card authorization and security, they opened doors for c-store proprietors. For example, with broadband access to the site, proprietors can improve operations by remotely monitoring tank levels. For BP's proprietors, some of whom own several sites, these connections allow faster communications between store locations. According to Mike Cook, senior vice president of Hughes, "In one initiative, BP created a solution that solves its legacy protocol issues and creates a managed network built around both DSL and satellite, which serves current and future applications for its stores."

Remote video-camera monitoring is also enabled via network connections that provide greater security for c-store workers and reductions in shrink (from in-store resources as well as drive-offs). BP, for example, is also pilot-testing BP TV, which is media streaming through an IP-based network to allow messages and entertainment at the pump.

Low Risk, High Reward

The HughesNet PCI-compliant managed service provides BP with transport-level services at each station, hub operations, network management and proactive monitoring. The solution also includes installation, field maintenance, and ISP-class services.

About Hughes Network Systems, LLC

Hughes Network Systems, LLC (HUGHES) is the global leader in providing broadband satellite networks and services for large enterprises, governments, small businesses, and consumers. HughesNet encompasses all broadband solutions and managed services from Hughes, bridging the best of satellite and terrestrial technologies. To date, Hughes has shipped more than 1.2 million systems to customers in over 100 countries. Its broadband satellite products are based on the IPoS (IP over Satellite) global standard, approved by the TIA, ETSI, and ITU standards organizations. Hughes is a wholly owned subsidiary of Hughes Communications, Inc. (NASDAQ: HUGH). For additional information, please visit www.hughes.com.

©2007 Hughes Network Systems, LLC. Hughes, HughesNet, and Broadband Unbound are trademarks of Hughes Network Systems, LLC. All rights reserved. All information is subject to change.