

# Protecting Cardholder Data

## A case study in enterprise Payment Card Industry (PCI) Compliance

When customers provide their credit card information to a merchant, whether in person or online, each transaction is an expression of trust. Customers are handing over the keys to sensitive, private data and it is the responsibility of companies that process credit card transactions to guard against unauthorized access or theft. It's quite clear from the number of high-profile data exploits in the media that consumers are becoming concerned.

Compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) is one way that businesses can improve the safety of their customers' valuable information and protect the trust they have established in their brands.

To meet and continually maintain compliance with the stringent PCI requirements, and to avoid increased processing fees or fines, forward-thinking companies such as Marriott International are using the security expertise of Cigital, Inc. to enact accelerated, enterprise-wide compliance programs for PCI requirements.

### New Standards in a Demanding Environment

U.S. consumers use credit cards more frequently than cash and checks combined. The top four credit card brands generated over \$2.4 trillion in spending in 2006. By 2010 Americans will make 70 billion purchases with credit and debit cards. The security of these transactions is the cornerstone of the global economy and of utmost value to businesses, the payment card industry and consumers.

In the interest of merchants, consumers and credit card processors PCI mandates and now enforces compliance with their standards for security management, network architecture, software design and other critical protective measures. Companies with high transaction volumes are regularly audited; in the event of a security breach, fines of up to \$500,000 per incident may be levied. To secure cardholder data, measures must be taken wherever card data is stored, processed or transmitted.

Protecting credit card data is particularly challenging for the hospitality industry; cardholder data captured by point-of-sale systems at the front desk, at a variety of merchant and partner locations, and through self-service applications is often stored or processed by disparate systems, from Customer Relationship Management to Enterprise Resource Planning and everything in between. While newer software applications may be somewhat more secure they must share data with legacy applications that do not support the strong authentication and audit capabilities required for PCI compliance.



Given the volume and complexity of in-house and third-party applications deployed at large hospitality businesses, remediating every existing application for PCI compliance in time for enforcement deadlines could be a daunting, enormously costly task. Marriott found the solution to best fit their needs.

Marriott International is one of the world's largest hoteliers with a variety of brands and more than 2,900 properties in 67 countries and territories worldwide. Strategic insight is one hallmark of an industry leader and Marriott is committed to executing the most robust strategy possible to protect their customers' data. They also must achieve a balance among security infrastructure spending, business benefits and business risks.

Marriott evaluated tools and services marketed for PCI compliance but found none that provided a cost-effective, enterprise-wide solution. One tool might address data at rest but not in transit. Another company's proposal required a device at every single property, adding unacceptable cost and maintenance issues. There were challenges in network architecture such that the different systems could require conflicting translation engines.

*"We set an aggressive goal of reaching full PCI compliance and sought out a trusted partner with a holistic approach to securing enterprise systems,"* says Kathy Memenza, Vice President, Enterprise Security for Marriott International, Inc. That partner was Cigital, a company with a depth of knowledge and long-term focus on security.

### Cigital's Secure Credit Card Proxy

Years of experience serving large companies equips Cigital consultants to assess complex situations, identify vulnerabilities, develop strategic plans and manage both business risks and business realities. For Marriott, Cigital recommended a Secure Credit Card Proxy to provide a strong security framework.

*"Cigital's Secure Proxy Solution had exactly the right combination of software components and processes to help us reach our goal at considerably less expense than we would have incurred by doing it alone,"* says Memenza.

At the core of Cigital's Secure Proxy Solution is a cryptographic algorithm that provides a transparent, drop-in replacement or "proxy" for credit or debit card numbers. This means that legacy systems can overcome one of the biggest obstacles to PCI compliance without massive application and database rework, securing sensitive data quickly and cost-effectively.

Strict “need to know” access privileges with controls were defined. All access transactions are recorded in fully-auditable logs. The Transport Layer Security (TLS) maintains data security and integrity in transit.

Data access is implemented through industry-standard Service-Oriented Architecture (SOA) technologies and public-key encryption which can integrate into a company’s existing Public Key Infrastructure (PKI). This solution is designed to be highly-available and easily scales to support even the most demanding environments. It overcomes the weak link of legacy applications and is flexible enough to support future applications that are acquired or developed.

### A Successful Alliance

Great organizations thrive because of outstanding people and commitment to service. Marriott realized that collaborating with a software security and quality consulting firm of Cigital’s caliber was both strategic and economical. Cigital grasped the complexity of Marriott’s issues and designed solutions that met or exceeded their goals. Marriott addressed many of the key PCI requirements in record time and favorably positioned the company for future changes in its software landscape.

*“We appreciate that Marriott had the foresight to meet their security challenges early and head-on,” says Dr. Gary McGraw, CTO of Cigital. “It’s a pleasure working with a company that takes the responsibility of protecting customer data in their applications extremely seriously.”*

The hospitality industry is built upon time-honored traditions of catering to the various needs and concerns of guests. By proactively protecting its customers from the new and growing sophisticated threats Marriott leads that tradition into the digital age.

### PCI Requirements Addressed by Cigital’s Secure Proxy Solution

#### 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 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

#### Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

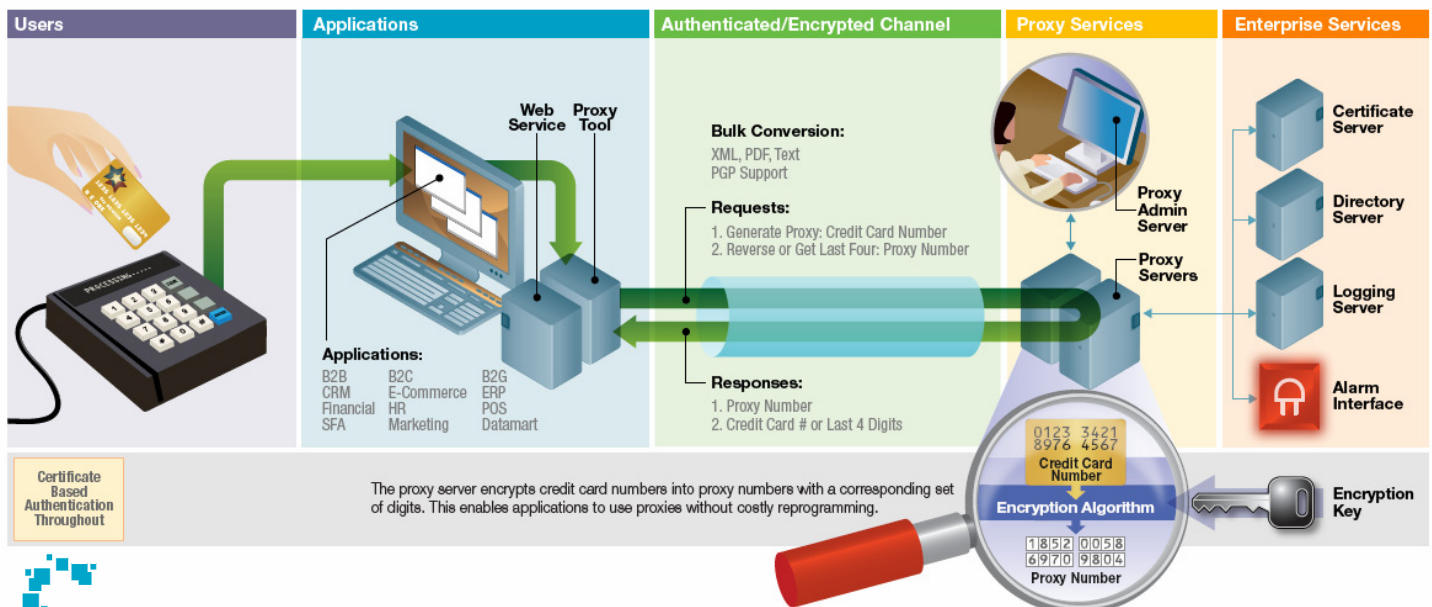
#### About Marriott

Marriott International, Inc. traces its heritage to a root beer stand opened in Washington, D.C. in 1927 by J. Willard and Alice S. Marriott. Marriott is a leading lodging company with more than 2,900 lodging properties in the U.S. and 67 other countries and territories. The company is headquartered in Washington, D.C. In 2006 the company had about 151,000 employees and ranked as the industry’s most admired company and one of the best places to work by FORTUNE®. It is also an EPA ENERGY STAR® partner. In fiscal 2006 the company reported sales from continuing operations of \$12.2 billion. [www.marriott.com](http://www.marriott.com).

#### About Cigital

Since 1992 Cigital has specialized in software risk management and data security. Cigital consultants help companies protect some of their most valuable assets: company information, customer data, shareholder value and brand. Each client’s unique requirements are served through a combination of proven methodologies, tools and best practices. Cigital assures the reliable delivery and deployment of software that organizations build, buy and integrate. [www.cigital.com](http://www.cigital.com)

### Secure Credit Card Proxy Solution



Certificate Based Authentication Throughout

The proxy server encrypts credit card numbers into proxy numbers with a corresponding set of digits. This enables applications to use proxies without costly reprogramming.

