PCI Compliance and Data Security Best Practices

Becoming PCI compliant and reducing the exposure to payment data can significantly reduce the risks and costs associated with payment processing.

BluePay

www.bluepay.com

WHAT IS PCI COMPLIANCE?

The PCI Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing payment account data security developed by the major credit card providers that make up the PCI Security Standards Council, including Visa, MasterCard, American Express, Discover and JCB. The standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective procedures.[1]

PCI CORE REQUIREMENTS[1]:

Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement strong access control measures

- Restrict access to cardholder data by business need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an information security policy

- Maintain a policy that addresses information security

WHY PCI COMPLIANCE?

PCI compliance provides guidelines for securing customer data and reducing the liability associated with payment processing. It also allows merchants to avoid heavy fines for non-compliance. Acquiring banks can be fined anywhere from $5,000 to $100,000 per month for non-compliance, which eventually will get passed on to the merchant and can result in the cancellation of a contract or higher fees.[2] Additionally, if a breach occurs, a fine of up to $500,000 can be imposed for merchants that are not compliant.

MORE THAN COMPLIANCE

Securing the acceptance, transmission and storage of payment data involves more than PCI compliance; compliance in itself will not protect a company from security breaches. Many compliant companies have been the victims of security breaches. It is estimated that a security breach can cost a business between $90 and $350 per record.[3] These costs include not only fines, but also the costs of notification, employee time, restitution, security audits and many other associated costs, which can depend on the organization. On average, a breach can cost a company $6.6 million.[4]

> **"The best practice for securing payment data is for a company to completely remove itself from the data. By outsourcing, the merchant has minimal exposure to data security risks."**

BluePay

BRAND PROTECTION

Perhaps the most significant cost of a security breach is the damage done to a brand and the resulting lost business. The cost of lost business due to a data breach accounts for 69 percent of data breach costs and averages $139 per record, totaling $4.59 million.[4] A breach causes customers to lose trust in the merchant. Once the trust is lost, it is very difficult to rebuild. Moreover, not only is the current customer lost, but also it becomes even more difficult to attract new ones. The resources, time and effort required to repair a brand image can be insurmountable.

EFFECTIVELY SECURING PAYMENT DATA

The best practice for securing payment data is for a company to completely remove itself from the data. This can be done by outsourcing payment processes to a payment processing provider. The payment processor will then handle the data collection, storage and transmission. By outsourcing, the merchant has minimal exposure to data security risks.

THE PROCESS

Customer payment data exposure is eliminated through a process called tokenization.

Payment information is collected by the payment processor through a secure payment gateway and stored on their secured servers. The merchant is then given a payment token which replaces the need for credit card numbers in the merchant's system. The merchant only has this token in its system so that in the event of a security breach, there is no payment information to be stolen and all of the customer payment data remains secure. The token is only identifiable by the payment processor. For all subsequent charges or recurring billings, the merchant is able to use the token and process the payment through the payment processor.

Tokenization effectively allows a merchant to take a large portion of the risk away from itself and place it onto the payment processor, substantially reducing the associated costs of payment processing and data security.

CONCLUSION

Security breaches can be very costly and can even mean the end for many small businesses. To protect themselves against these events and associated costs, businesses should not only seek PCI compliance, but implement tokenization with a payment processor to eliminate the exposure to payment data. It comes down to protecting customers and ultimately protecting the brand.

[1] PCI Security Standards Council [2] PCI Compliance Guide [3] Forrester Research, Inc. [4] *2008 Annual Study: Cost of a Data Breach*, Ponemon Institute, LLC

BluePay is a single source provider for merchant payment processing needs. We are a full-service, Tier 1 credit card processor based out of Naperville, Illinois, with offices in Chicago, New York, and Toronto, Canada. At BluePay, we leverage our extensive industry experience and a comprehensive suite of credit card merchant account services to provide businesses a complete system of credit card processing solutions at the most competitive rates.

Working with BluePay provides your business with a partner who covers all the aspects of your credit card processing and payment transaction needs. We customize our payment solutions and advanced technology to fit the unique needs demanded by your industry and business type. Our innovative technology includes our secure electronic payment gateway, which is constantly updated to stay on the cutting edge of PCI compliance, providing you with a reliable, safe, and efficient payment solution. Using The BluePay Gateway, we integrate payments into hundreds of different types of business software to streamline the payment process and better serve companies across the United States and Canada.

BluePay makes it easy to accept credit cards, including Visa, Discover Network, MasterCard and American Express, and can incorporate less commonly used payment methods including ACH eChecks and IVR telephone payments to make your business even more convenient for your customers.

PHONE	800-350-2983
EMAIL	GETSTARTED@BLUEPAY.COM
CONNECT	

BluePay
www.bluepay.com