PNC MERCHANT SERVICES EDUCATIONAL SERIES

PCI DSS:
The Security Your Customers Are Looking For

It happens all the time: Internet shoppers abandon their shopping cart and cancel an online transaction ... just seconds before hitting the payment button.

The reason? Often, it is because they don't have confidence in the online retailer's security measures. In the back of their mind is the nagging fear that they, too, will become one of the millions of consumers whose personal data — from credit card numbers to bank account information — is hacked by wily cyber thieves.

"What, Me a Target?"

Unfortunately, this scenario plays out all too often in the world of brick-and-mortar businesses, too.

Cybercriminals are just like any other criminal — they prey on the weak and vulnerable. And they are discovering that many small merchants have not implemented even the most basic security measures. As a result, attackers increasingly target small merchants using automated attacks that often go undetected for long periods of time due to a lack of monitoring by merchants.[1] In fact, a Visa® analysis found that small merchants account for more than 80 percent of data security breaches.

In the end, these security breaches may not only expose your business to fines from bank regulators and the card associations — they also rob you of your customers' trust. And, that's hard to win back.

Are You PCI DSS-Compliant?

One way you can protect yourself — and your customers — is by following the Payment Card Industry Data Security Standard (PCI DSS). Created in 2006, the PCI DSS is a set of mandatory security standards designed to protect cardholder information and reduce data theft. PCI DSS applies to all businesses that store, process or transmit cardholder data. PCI DSS is required by PNC Merchant Services® and is enforced by the founding members of the PCI Security Standards Council – Visa®, MasterCard®, American Express® and Discover® Financial Services.

Understanding the Requirements

PCI DSS validation requirements vary according to the number and type of payment transactions you process. A merchant using a sophisticated payment system connected to the Internet that captures and electronically stores large amounts of cardholder information may fall under different requirements than one who simply uses a manual card imprint machine or standalone dial-out terminal.

So it's important that you become familiar with the specific requirements that apply to your business. But you can start by following these basic PCI DSS data security requirements:

Network Security

- Install and maintain a secure network firewall to protect cardholder data across public networks.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

See back for additional details. >

For more information

> Stop by any branch
> Call 1-855-PNC-CF05 (1-855-762-2365)
> Visit pnc.com/merchantservices

PNC MERCHANT SERVICES

Cardholder Data

- Protect stored cardholder data and encrypt transmission of cardholder data across open, public networks.
- Do not store or retain magnetic stripe data, PIN data or Address Verification System (AVS) data. Only the cardholder account number, name and expiration date should be retained after transaction authorization.
- Do not store or retain Card Validation Codes, the three-digit values printed in the signature panel of most cards (four-digit code printed on the front of an American Express card) after transaction authorization.
- Do not transmit cardholder account numbers to cardholders for Internet transactions.

Vulnerability

- Use and regularly update anti-virus software on all systems commonly affected by malware and keep security patches up to date.

Access

- Restrict access to cardholder data in your business on a “need-to-know” basis.
- Assign a unique ID to each person with computer access to cardholder data and use this ID to track access to the data.

Monitoring and Testing

- Maintain a policy that addresses information security for employees and contractors.
- Regularly test security systems and processes.

Validation

- Complete a PCI DSS Self Assessment Questionnaire (SAQ) to self-evaluate your compliance with PCI DSS.
- If your business uses point-of-sale software instead of terminals to process card payments, you may need to answer an expanded questionnaire and participate in a PCI DSS External Vulnerability Scan (Network Scan).

You Can’t Put a Price on Trust

It’s all about trust: When customers hand you their credit or debit card or provide their account information, they expect you to safeguard that sensitive information. In a way, being PCI DSS compliant signifies you are following best practices to protect your customers’ card data. If they’re not confident that you will protect their data, they won’t do business with you. It’s as simple as that.

PNC Merchant Services is a leader in the payment processing industry. We provide businesses with innovative payment acceptance capabilities and back them up with service, financial strength and stability to help keep your receivables flowing.

Supporting merchants throughout the United States, ranging in size from single-outlet merchants to super-regional enterprises with thousands of locations, you can count on PNC Merchant Services. We have the industry experience, personal attention and customer service you need to keep your payment processing systems secure and operating smoothly. Contact us at 1-800-742-5030 to discuss how PNC Merchant Services makes payment options easier for your customers, and better acceptance options for your business.

[1] Why is PCI important to my small business? Advancing Commerce™. MasterCard Worldwide. ©2012 MasterCard.

Merchant Services provided by PNC Merchant Services Company and are subject to credit approval.
PNC Merchant Services is a registered trademark of the PNC Financial Services Group, Inc.

PNC®
MERCHANT SERVICES