

IT'S NOT A MATTER OF IF YOU'RE HACKED



IT'S WHEN

Data Security and Your Business:

What you need to know

Our services and equipment meet all Payment Card Industry (PCI) Data Security Standards. Every merchant who touches credit card account information is responsible for safeguarding that information and can be held liable for security compromises if they have not taken the required precautions.

Merchants must currently meet all Payment Card Industry Data Security Standard requirements as specified by the PCI Data Security Council. In addition, Visa mandates that merchants must be using PCI compliant processing equipment by July 1, 2010. Failure to meet PCI compliance regulations will result in fines and possibly the loss of the ability to accept card-based payments.

The PCI Data Security Council—an organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.—provides a comprehensive guide to meeting compliance requirements. The Retail Solutions Providers Association offers an educational video and other informative PCI compliance materials on its website: <http://www.gorspa.org/i4a/pages/index.cfm?pageid=3329>.

Merchants must currently meet all PCI Data Security Standard (PCI DSS) requirements

Merchants must meet all PCI DSS requirements and use PCI compliant processing equipment. Failure to meet PCI compliance regulations will result in fines and possibly the inability to accept card-based payments.

Important facts

Merchants who don't comply with the PCI Data Security Standard may face fines from the credit card companies. Additionally, the credit card companies have reserved the right to terminate credit card acceptance privileges for merchants who don't comply with the PCI Data Security Standard.

Following the PCI Data Security Standard helps protect you and your customers from hacking and other fraudulent credit card activities.

PIN Entry Devices (PED)

The PCI PED Security Requirements focus on protection of the cardholder's PIN when used in connection with a financial transaction. To gain approval by the PCI Security Standards Council, PIN entry devices must comply with the requirements and guidelines specified by the Council.

More information about PCI PED and a listing of PCI Security Standards Council approved PIN entry devices is available online at https://www.pcisecuritystandards.org/security_standards/ped/index.shtml.

Payment Application Data Security Standard (PA-DSS)

PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with PCI DSS. More information about PA-DSS is available online at https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml.

PCI DSS Core Requirements

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 anti-virus 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

DON'T WAIT.

FOLLOW THESE SIMPLE STEPS TO AVOID PENALTIES.

Protecting the security of your credit card data is a mandated process that must be certified annually, beginning now.

- No lengthy paperwork.
- No tricky questions.
- No wasted time.
- No worrying about the security of your data.

Just a short and simple way to protect your customers and your business, and meet guidelines mandated by Visa and MasterCard.

Get compliant today.

Please follow these steps for each of your MIDs to assure that your business is operating within mandated guidelines:

1. Log into VIMAS. (Screen 1)
2. Complete the registration steps. Make sure you verify your email address prior to submitting the registration. (Screens 2-5)
3. Once you submit your registration, a password will be sent to the email address you submitted. (Screen 6)

Continues on the reverse...

1 Username:
Password:
login

2 Merchant ID:
Password:
Sign In
I forgot my password
Don't Have a Password?
Register Now
Begin by clicking on the Register Now link

3 PCI Certification
Account Registration
Return to Login Page
Enter your Merchant ID and click Register Now.
99999950001 Merchant ID
Register Now
Enter the Merchant ID in the text box and click the Register Now button

4 PCI Certification
Account Registration
The Account Information page is where the user confirms the pre-populated information and enters any information that is missing
All fields marked with an asterisks(*) are required:
Merchant ID: * 99999950001
Contact First Name: *
Contact Last Name: *
Contact Title: Owner
Company Name: * SecurePay
Company Web Site: https://www.securepay.com

5 Street Address 1: 4400 North Point Parkway
Address 2: Suite 260
City: * Alpharetta
State: * Georgia
Zip Code: * 30045
Phone Number: * 678-867-6000 (Ex: 123-123-4567)
Email Address: * webmaster@securepay.com
Submit Registration
Enter the required information and click the Submit Registration button

6 PCI Certification
Account Registration
A Registration Email is sent to the Merchant's Email Address
Your registration information has been emailed to you.
Return to Login Page

DON'T WAIT.

FOLLOW THESE SIMPLE STEPS TO AVOID PENALTIES.

...Continued from the reverse.

4. Use this password to access the self-assessment questionnaire (SAQ) designed for your business. (Screen 7)
5. The self-assessment questionnaire (SAQ) is comprised of a few short “yes or no” questions. Your answers to each of these questions determines the questions that follow them. (Screen 8)
6. As you complete the SAQ, areas of non-compliance will be highlighted and remedies suggested. (Screens 9-10)
7. Upon finishing successfully, you will be asked to attest to the information you have entered, and issued a certificate of compliance. Please print this certificate for your records and keep it in a safe place. (Screen 11)

For more information about DSS Compliance, visit our website, or the website of the PCI DSS Security Council at: <https://www.pcisecuritystandards.org>

