



# Critical Security Alert

## What Every Merchant Needs To Know About Consumer Data Security

Your customers want to be assured that their credit card information is safe. Offering your customers a safe and secure way to pay is more than good business practice— it is also a requirement. Each and every merchant that accesses credit card account information is responsible for safeguarding that information and can be held responsible for security breaches if they have not taken appropriate and required security measures.

To help merchants understand and abide by their requirements, Visa and Mastercard have aligned the compliance levels and validation requirements of their cardholder data security programs (CISP and SDP), creating the payment card industry (PCI) Data Security Standard. This program is intended to protect the cardholder data— wherever it may be— thus ensuring that banks, merchants, and service providers maintain the highest possible information security levels.

*The Payment Card Industry (PCI) Data Security Standard is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

### PCI Data Security Standard

#### Build and Maintain a Secure Network

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

#### Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.

#### Maintain a Vulnerability Management Program

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

#### Implement Strong Access Control Measures

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

#### Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

#### Maintain an Information Security Policy

12. Maintain a policy that addresses information security.

### Visa Non-Compliance Fines

First Violation	Up To \$ 50,000
Second Violation	Up To \$100,000
Third Violation	Up To VISA Management Discretion
Failure to report a compromise	Up To \$100,000
Egregious Violation	Up To \$500,000

### Mastercard Non-Compliance Fines

Level 1 Merchants	Up To \$100,000, if not compliant in 60 days then additional fines of \$10,000 per day, not to exceed \$500,000
Level 2 Merchants	Up To \$50,000, if not compliant in 60 days then additional fines of \$10,000 per day not to exceed \$500,000
Level 3 Merchants	Up To \$25,000, if not compliant in 60 days then additional fines of \$10,000 per day, not to exceed \$500,000



## Frequently Asked Questions

### Does this apply to me?

The PCI Data Security Standard Program applies to all US entities that store, transmit or process cardholder data (i.e., Visa, MasterCard, American Express, Discover), regardless of payment method (on-line, mail/telephone orders or "brick and mortar"). Additionally, these security requirements apply to all "system components," which are defined as "any network component, server or application included in, or connected to, the cardholder environment".

### Why do I have to go through the compliance process?

The simple answer is to avoid potential fines that the card brands may levy. In addition, you need to protect your customers' confidential information and safeguard your valuable reputation.

### How do I ensure my company is compliant?

Visit [www.visa.com/cisp](http://www.visa.com/cisp) to view PCI compliance standards and complete the self assessment questionnaire.

Have your network scanned by a third party provider. Renaissance associates recognizes the importance of security scans for all merchants and has partnered with Security Metrics to provide an easy, cost-effective security scan solution. Register at [www.securitymetrics.com/register](http://www.securitymetrics.com/register) and choose **Renaissance Associates** from the drop down box for special pricing. Merchants may also call Security Metrics directly at **801-705-5665**.

### Once I become compliant, how long am I considered compliant?

You must maintain compliance throughout the year. If your company suffers a security incident and is found to be operating in a non-compliant manner, your company will be subject to fines and other penalties.

### Are there any additional fees?

Please be advised, once you are considered compliant, if you are a level 1, 2 or 3 merchant, we must register your company with MasterCard. If your company is storing credit card information, MasterCard will charge us with an annual \$200 registration fee, which we will pass on to you.

	Compliance Actions	Validation Actions		
Merchant Level	Comply With PCI Security Standards	On Site Security Audit	Self-Assessment Questionnaire	Network Scan
<p><b><u>Level 1</u></b></p> <ul style="list-style-type: none"> <li>Any merchant, regardless of acceptance channel processing over 6,000,000 Visa transactions per year.</li> <li>Any merchant that has suffered a breach that resulted in an account data compromise.</li> <li>Any merchant that Visa, at its sole discretion, should meet the Level 1 requirements to minimize risk to the Visa system.</li> <li>Any merchant identified by any other payment card brand as Level 1</li> </ul>	Required	Required Annually		Required Quarterly
<p><b><u>Level 2 Merchants</u></b></p> <ul style="list-style-type: none"> <li>Any merchant processing 150,000 to 6,000,000 e-commerce transactions per year</li> </ul>	Required		Required Annually	Required Quarterly
<p><b><u>Level 3 Merchants</u></b></p> <ul style="list-style-type: none"> <li>Any merchant processing 20,000 to 150,000 e-commerce transactions per year</li> </ul>	Required		Required Annually	Required Quarterly
<p><b><u>Level 4</u></b></p> <ul style="list-style-type: none"> <li>All other merchants not in Levels 1,2, or 3, regardless of acceptance channels</li> </ul>	Required		Recommended Annually	Recommended Annually

Visa USA, Visa Canada and MasterCard have warned that they may restrict or terminate the merchant's or service provider's acceptance privileges for issues of non-compliance. Many consumers are becoming more and more aware of security relating to their personal information. Your compliance demonstrates that you are protecting your customers' personal data. A breach in security may cause irreparable damage to the relationships you have built with your customers, and ultimately negatively impact your bottom line. To discuss this document with Renaissance Associates call 1-888-267-5772.