

## Secure Quest Takeaways

### PCI Requirements:

<b>Requirement</b>	<b>Description</b>
<b>Requirement 1:</b> <i>Install and maintain a firewall configuration to protect data.</i>	Proper filters must be in place to make sure that you really understand who is entering into your system. Make sure that only authorized personal can access your data. Wireless access points also need to be plugged into the firewall so that predators can't use these points to bypass the firewall
<b>Requirement 2:</b> <i>Do not use vendor-supplied defaults</i>	Only use unique passwords that you create when setting up your system. This also includes passwords associated with wireless technology.
<b>Requirement 3:</b> <i>Protect stored data</i>	Make sure stored credit card data is encrypted. If your credit card data can't be encrypted, then there are other compensating controls that need to put in place in order to protect your credit card data. Don't just rely on one source to secure your entire network. You must rely on layered access controls to protect that data.
<b>Requirement 4:</b> <i>Encrypt transmission of cardholder data and sensitive information across public networks</i>	Encrypt any cardholder data that travels through the public domain (aka. Internet). Any wireless network is considered a public network. WEP transmission encryption by itself isn't adequate protection for credit card data. WPA and WPA2 are the recommended protocols for wireless networks.
<b>Requirement 5:</b> <i>Use and regularly update anti-virus software</i>	Make sure you have adequate virus scanning technology on your network. Remember to keep up to date with security patches for your virus scanning software.
<b>Requirement 6:</b> <i>Develop and Maintain Secure Systems and Applications</i>	To be fully secure you must have a documented systems protection life cycle. Make sure your test system is separate from your production system. Make sure that all applications are coded and compliant with OWASP (Open Web Application Security Project) guidelines. By June 2008, you will have to have an application layer firewall in front of all web facing applications or perform code review of your web applications. Make sure your web applications don't allow SQL injection.
<b>Requirement 7:</b> <i>Restrict access to data by business need-to-know</i>	Access to card information should be assigned on a need to know basis. Don't give someone more access than they need to do their job.
<b>Requirement 8:</b> <i>Assign a Unique ID to Each Person with Computer Access</i>	Do not use Group ID's. Access to credit card data is restricted to only people who need that access. Practice good password management. Age your passwords and make sure enforce password expiration. Use alphanumeric passwords.
<b>Requirement 9:</b> <i>Restrict physical access to cardholder data</i>	Where ever you store the machines that hold your credit card data make sure you have good security procedures that limit access to these machines. Precautions such as key or card access protection, ID badges, security cameras or visitor escorts are examples of proper precautions. When sending data offsite, make sure that the end location for your data has the same security procedures that you would follow.
<b>Requirement 10:</b> <i>Track and Monitor Access to Network and Card Data</i>	You need to have sufficient audit logging in place to unravel the 'what', 'when', 'who', and 'how' when you have a security breach. Have a system in place that will alert you to when a person is in your system when they shouldn't be.
<b>Requirement 11:</b> <i>Regularly Test Security Systems and Processes</i>	Test your processes to prove that they are working adequately to make sure that they are detecting unauthorized data and will shut down the system when a breach has been made. Monitor the integrity of your critical files. Add a monitoring system that alerts you when any change has been made to your critical files. Do annual penetration tests on your internal network and do quarterly external network scans.
<b>Requirement 12:</b> <i>Maintain a policy that addresses information security</i>	Have an information security policy in place. If a security breach does happen, have documented processes in place that discuss how to handle the situation. Know what to do and who's going to handle each specific task.

**What do merchants have to do?**

Level	Selection Criteria (based on Visa transactions)	Validation Actions	Validation Process	Merchant Requirements
1	<ul style="list-style-type: none"> <li>&gt;6 million annual trans. (all acceptance channels)</li> <li>Incurred a compromise</li> </ul>	<ul style="list-style-type: none"> <li>Annual onsite security visit - and -</li> <li>Quarterly network scan</li> </ul>	Qualified Independent Security Assessor or Internal Audit Staff with CISA designation if signed by company officer	<ul style="list-style-type: none"> <li>Submission of successful Report on Compliance (ROC)</li> <li>Quarterly scan showing no high vulnerabilities</li> </ul>
2	<ul style="list-style-type: none"> <li>1 to 6 million annual trans. (all acceptance channels)</li> </ul>	<ul style="list-style-type: none"> <li>Annual PCI self-assessment questionnaire - and -</li> <li>Quarterly network scan</li> </ul>	<ul style="list-style-type: none"> <li>Validated by merchant</li> <li>Qualified independent scan vendor</li> </ul>	<ul style="list-style-type: none"> <li>Submission of PCI self-assessment questionnaire with green rating</li> <li>Results of quarterly scan showing no high vulnerabilities</li> </ul>
3	20,000 – 1 million e-commerce trans.	<ul style="list-style-type: none"> <li>Annual PCI self-assessment questionnaire - and -</li> <li>Quarterly network scan</li> </ul>	<ul style="list-style-type: none"> <li>Validated by merchant</li> <li>Qualified independent scan vendor</li> </ul>	<ul style="list-style-type: none"> <li>Submission of PCI self-assessment questionnaire with green rating</li> <li>Results of quarterly scan showing no high vulnerabilities</li> </ul>
4	Less than 20,000 e-commerce transactions or less than 1 million transactions (any acceptance channel)	<ul style="list-style-type: none"> <li>Recommended annual PCI self-assessment questionnaire - and -</li> <li>Recommended quarterly network scan</li> </ul>	<ul style="list-style-type: none"> <li>Validated by merchant</li> <li>Qualified independent scan vendor</li> </ul>	<ul style="list-style-type: none"> <li>Compliance mandatory</li> <li>Validation optional</li> </ul>

**What happens if merchants do not comply?**

Visa Fines	MasterCard Fines
PCI Compliance Accélération Program Fines <ul style="list-style-type: none"> <li>Applies to all Level 1 and 2 merchants identified prior to 2007</li> <li>Merchants storing prohibited data after March 31, 2007               <ul style="list-style-type: none"> <li>Level 1 - up to \$100,000 monthly</li> <li>Level 2 – up to \$50,000 monthly</li> </ul> </li> <li>Non-compliance with PCI Data Security Standards               <ul style="list-style-type: none"> <li>Level 1- \$25,000 monthly after September 30, 2007</li> <li>Level 2 - \$5,000 monthly after December 31, 2007</li> </ul> </li> </ul>	Failure to comply with the SDP mandate <ul style="list-style-type: none"> <li>Level 1 Merchants – Up to \$25,000</li> <li>Level 2 Merchants – Up to \$5,000</li> <li>Level 3 Merchants – Up to \$5,000</li> </ul>

**Where can we get more help?**

Resource	Web Site
Chase Paymentech	<a href="http://www.chasepaymentech.com/solfraproccarnotpredatsec.do">http://www.chasepaymentech.com/solfraproccarnotpredatsec.do</a>
AmbironTrustWave Strategic Partner Vendor providing PCI compliance services	<a href="http://www.ATWCorp.com">www.ATWCorp.com</a>

Resource	Position	Phone	Email
Don Roeber	Chase Paymentech's IT Internal Audit Director	214.849.3394	<a href="mailto:Don.Roeber@chasepaymentech.com">Don.Roeber@chasepaymentech.com</a>
Cary Bresloff	AmbironTrustWave Account Manager	312.873.7266	<a href="mailto:cbresloff@atwcorp.com">cbresloff@atwcorp.com</a>