

## Payment Card Industry / Compliance Services



### FISHNET SECURITY IS APPROVED TO PROVIDE THE FOLLOWING PCI COMPLIANCE SERVICES

- Quarterly Scanning
- Pre-Assessment Readiness
- Cardholder Data Inventory / Lifecycle
- Payment Card Risk Management
- On-site Security Audit
- Remediation Guidance
- DSS Gap Analysis Review

### UNDERSTANDING AND COMPLYING

with PCI—and the many other privacy and security regulations that exist today—can be a serious challenge. FishNet Security understands the process of PCI compliance; is an authorized provider of PCI auditing and scanning services; and has the experience to guide you toward a sustainable compliance program.

### THE HISTORY OF PAYMENT SERVICES REGULATIONS

In December 2004, Visa and MasterCard standards were endorsed by four other brands creating the Payment Card Industry (PCI) Data Security Standard. This single, unified security program is designed to protect credit card data based upon twelve fundamental security controls. Compliance with the PCI Data Security Standard (DSS) is now required of all merchants and service providers that store, process, or transmit cardholder data.

### FISHNET SECURITY MAINTAINS THE FOLLOWING PCI STATUS:

#### QUALIFIED DATA SECURITY COMPANY

- Performs on site security audits to determine compliance with the PCI Data Security Standard (DSS)

#### QUALIFIED INDEPENDENT SCANNING VENDOR

- Performs the required PCI quarterly security scans

### METHODOLOGY

The road to maintaining compliance is often perceived as a race through a series of hoops (checklists) to keep up. FishNet Security can stop the race and start managing the risk imposed by regulated data. Sustaining compliance is possible at an enterprise level.

### THE FISHNET SECURITY ADVANTAGE

FishNet Security deploys risk management programs empowering you to meet compliance in a business context, instead of simply running down a checklist of requirements. Our approach extends your compliance budget by providing a framework of safeguards to sustain compliance across the board.

*For information regarding FishNet Security's Payment Services Compliance offerings please refer to the back of this document.*

*For more information, please contact FishNet Security at [pci@fishnetsecurity.com](mailto:pci@fishnetsecurity.com), or call at (888) 732.9406.*

#### PCI COMPLIANCE ON-SITE AUDIT SERVICES
















- Authorized PCI QDSPs involved on all On-Site Audit engagements.
- Tested, adaptable and scalable compliance methodology utilized for global enterprise environments.
- Authoritative approach blends cross industry & global best practices to refine control sets that make business sense.
- Consultative approach migrates from compliance focus to security partnership framework.
- Standard reporting speaks business case for executives, matrix prioritization for managers, and technical detail for procedural and project-oriented positions.
- Reputation for time sensitive project completion and ongoing PCI compliance support.

#### PCI COMPLIANCE SCANNING SERVICES

- Authorized Certified PCI Security Scanning Vendor
- Dedicated PCI Security Scanning Team ([scans@fishnetsecurity.com](mailto:scans@fishnetsecurity.com))
- PCI executive summary, management status and progress reports for acquirers
- PCI Compliance Report provided (per device)
- PCI quarterly vulnerability trending reports
- PCI quarterly phone support with vulnerability scanning expert included
- Multiple commercial grade vulnerability and penetration testing tools utilized

# Payment Card Industry / Compliance Services

## PCI DATA SECURITY STANDARD

Actions Taken			Classification	Description						
Annual On site Audit	Quarterly Scans	Self Assessment Questionnaire								
				<table border="1"> <tr> <td>BUILD AND MAINTAIN A SECURE NETWORK</td> <td>IMPLEMENT STRONG ACCESS CONTROL MEASURES</td> </tr> <tr> <td>PROTECT CARDHOLDER DATA</td> <td>REGULARLY MONITOR AND TEST NETWORKS</td> </tr> <tr> <td>MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM</td> <td>MAINTAIN AN INFORMATION SECURITY POLICY</td> </tr> </table>	BUILD AND MAINTAIN A SECURE NETWORK	IMPLEMENT STRONG ACCESS CONTROL MEASURES	PROTECT CARDHOLDER DATA	REGULARLY MONITOR AND TEST NETWORKS	MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	MAINTAIN AN INFORMATION SECURITY POLICY
BUILD AND MAINTAIN A SECURE NETWORK	IMPLEMENT STRONG ACCESS CONTROL MEASURES									
PROTECT CARDHOLDER DATA	REGULARLY MONITOR AND TEST NETWORKS									
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	MAINTAIN AN INFORMATION SECURITY POLICY									
			Service Provider Levels	1 All credit card processors (member and Nonmember) and all payment gateways.*						
				2 Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 credit card accounts/transactions annually.						
				3 Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 credit card accounts/transactions annually.						
			Merchant Levels	1 <ul style="list-style-type: none"> <li>- Any merchant-regardless of acceptance channel-processing over 6,000,000 transactions per year.</li> <li>- Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</li> <li>- Any merchant that the credit card companies, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the credit card company's system.</li> <li>- Any merchant identified by any other payment card brand as Level 1.</li> </ul>						
OR 				2 Any merchant processing 1,000,000 to 6,000,000 e-commerce transactions per year.						
				3 Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.						
				4 Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants processing up to 1,000,000 transactions per year.						
	 (opt)	 (opt)								

\*Payment gateways are a category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction. Specifically, they enable payment transactions (e.g., authorization or settlement) between merchants and processors. Merchants may send their payment transactions directly to an endpoint, or indirectly to a payment gateway.



denotes that a QSA must perform the indicated action.



denotes that an organization can conduct the On-Site Audit internally with executive-level signoff of the Report On Compliance (ROC).

(opt)

denotes that the action is optional for the particular level of merchant or service provider



denotes that an organization can conduct the indicated action internally.