# Service Provider Management Frequently Asked Questions

Requirement 12.8 of the PCI DSS requires merchants to *manage* service providers. The PCI DSS does not provide general guidelines to manage service providers which includes due diligence prior to engagement. The following is a compilation of frequently asked questions we have received over the past several years.

## General:

- Is Shift4 Corporation a PCI DSS compliant service provider? **YES**
  - The Shift4 Corporation PCI DSS Certificate of Compliance is available for download on the Security Corner.
  - The Shift4 Corporation PCI DSS Attestation of Compliance is available for download on the Security Corner.
  - Shift4 Corporation is listed on both MasterCard and Visa's list of PCI DSS validated service providers.
  - Shift4 is not a shared hosting provider.

- Do you have security policies in place for all required security standards and processes? **YES**
  - Without exception we have security policies in place for each and every PCI DSS requirement.
  - As a Nevada based company, we also have strict policies governing Personally Identifiable Information over and above what we do for PCI DSS.
  - We have also adopted other security frameworks and enforce security policies that are far more restrictive than the PCI DSS.

- Do you have SAS 70 audits completed on your data centers? **NO**
  - We are not a publicly held company and are not required to have independent SAS 70 audits.

## Financial and Corporate Governance:

- Are you a publicly held company and/or subsidiary to a parent company? **NO**
  - We are a privately held, self-funded, independent Nevada corporation.
  - We are not wholly or partially owned by another institutional entity.
  - There are no venture capitalists, or independent or institutional investors funding Shift4 Corporation.

- Do you wholly or partially own other business entities? **NO**

- What mechanism do you have in place to show the financial stability of your company?
  - Since we are not publicly held, there is no legal requirement for Shift4 Corporation to disclose any sort of financial information.

- Is your company's corporate structure publicly available? **YES**
  - Information on Shift4's corporate structure is available here http://www.shift4.com/About_Us.cfm.

- Do you have an internal audit department? **NO**
  - We retain an independent financial auditor to audit our financials.
  - Our Security and Compliance team is deeply involved with internal IT governance and ongoing security and PCI compliance reviews and spot checks.

- Do you have insurance? **YES**
  - Umbrella coverage for up to $10,000,000.
  - Errors and omissions coverage for up to $5,000,000.

- Do you have a pre-employment screening process? **YES**
  - Financial background checks.
  - Criminal background checks
  - Drug & alcohol screening via hair and urine samples.

## Security and IT Governance:

- Do you have a business continuity plan in place? **YES**
  - Disaster recovery and business continuance plans are in place and are reviewed and tested at least annually.

- Do you have change control and backup procedures? **YES**
  - The Shift4 change control procedures are based on industry best practices with segregation of duties.
  - Backup procedures include full weekly backups with periodic incremental backups and a Grandfather / Father / Son backup tape rotation. Backup tapes are stored off site in fire proof security containers.
  - All backup media is exclusively handled by the most trusted employees.
  - Cardholder data is encrypted everywhere it is stored.

- Do you use third party service providers? **NO**
  - We do not use third party service providers for any PCI related function.

- Do you have redundant systems and connectivity to ensure survivability? **YES**
  - All of our data centers include redundancy in all aspects of IT operations from telecommunications providers, the power grid / UPS / backup power generator, and HVAC systems.

- What level of service could you provide in the event of a disaster? How would you notify customers?
  - It depends on the type of the disaster. We have fully redundant data centers. We perform periodic risk assessments and make adjustments to our plans as needed.

- Our plans include detailed procedures to contact all affected customers, partners, and upstream processors.

## Logical Security Processes:

- Do you have written security policies and procedures? **YES**
  - New employees receive initial orientation on all security policies and procedures and are required to read and acknowledge receipt of the end-user computing statutes.
  - Recurring training is performed at least annually.

- Do you have a documented process for cardholder data access control, encryption, and key management? **YES**

- Do you have systems security vulnerability and patch management policies? **YES**
  - Our procedures include the use of third party security management tools to scan our systems for security vulnerabilities and patch requirements. Only those patches that are relevant to our systems are applied and they are fully tested prior to full implementation.

- Do you have a data retention policy? **YES**
  - Cardholder data is retained for up to 24 months, based on the customers' requirements. Sensitive authentication data is never retained post-authorization.
  - All other media follows explicit handling and destruction processes from shredding or pulping, to degaussing, software wiping, or actual physical destruction.

- Are your security systems monitored and updated on a regular basis? **YES**

## Physical Security Processes:

- Do your data centers have fire detection and suppression systems? **YES**

- Do your data centers have adequate HVAC systems with alerting capability? **YES**

- Is access to Shift4 controlled areas restricted to only those employees whose job responsibilities require it? **YES**
  - Access to Shift4 controlled areas is centrally controlled by a card swipe system. Employees have access to controlled areas based on their job responsibility. All controlled area ingress and egress activity is logged.

- Are Shift4 premises under video surveillance? Are videos retained on DVRs and backed up to tape? **YES**

- Are sensitive, controlled areas alarmed and monitored by an armed response company? **YES**