

Service Provider Management Frequently Asked Questions

Shift4 Corporation (Shift4) often receives questionnaires regarding its PCI DSS compliance status as a service provider, as well as its internal management processes, financial position, and survivability as a business entity. Service provider management is called out in PCI DSS Requirement 12.8. Rather than answer each questionnaire individually, a comprehensive list of frequently asked questions along with their responses has been compiled.

If additional information is needed or answers to more specific questions are required regarding Shift4's in-place security controls, security processes, and/or other management controls, that information may possibly be provided under a non-disclosure agreement.

All questions and/or comments about this document should be directed to Stephen Ames, CISSP, Director of Security and Compliance, at PCI@Shift4.com.

General:

- Is Shift4 PCI DSS Compliant? **YES**
 - On an annual basis Shift4 completes the required SAQ-D for Level 1 Service Providers, has an on-site PCI assessment performed by a QSA, and has the compulsory penetration testing performed by an ASV.
 - Shift4 also has an ASV perform monthly external vulnerability scans on its data centers' Internet facing infrastructure.
 - Shift4 performs its own internal and external vulnerability scans and security reviews of its data centers on a monthly basis.
 - PCI DSS compliance at Shift4 is managed by the Security and Compliance team.
 - Shift4's PCI DSS assessment cycle is approximately June to May, but always within compliance period guidelines.
 - Shift4's compliance certificate and executive summary of its Report on Compliance (ROC) are available for download at <http://www.shift4.com>. Due to the nature of Shift4's business and the proprietary aspects of the information in such documents, ROCs will not be provided in their entirety.
 - Shift4 does not share cardholder data with any third party service providers as defined in PCI DSS Requirement 12.8.

- Does Shift4 have a dedicated security team responsible for security and compliance? **YES**
 - The director of Security and Compliance reports to the chief technology officer.
 - The Security Compliance and Security Process managers each report to the director.
 - The PCI DSS compliance and PA-DSS validation programs are managed by the Security and Compliance team.

- Does Shift4 have written security policies, standards, and procedures along with a process to manage them? **YES**
 - Shift4 has documented policies in place for each and every PCI requirement without exception.
 - They are reviewed and updated at least annually.
 - As a Nevada Corporation, Shift4 also has strict policies governing Personally Identifiable Information over and above what is required by the PCI DSS.
 - Shift4 has also adopted other security frameworks and enforces security policies that are far more restrictive, preventative, and/or protective than the PCI DSS.

- Does Shift4 have SAS 70 Level II audits performed on its data centers? **NO**
 - Shift4 is not a publicly held company, and as such is not required to have independent SAS 70 Level II audits, Shift4 has chosen not to do so at this time. There is however, nothing in any Shift4 policy or procedures that would interfere with any public company's compliance or adherence to any known Local, State, or Federal statute or guideline, such as GLBA, HIPPA, and SOX.

Financial and Corporate Governance:

- Is Shift4's corporate structure publicly available? **YES**
 - All company Founder and Executive Team member information is available on Shift4's corporate website at: http://www.shift4.com/About_Us.htm#overview. This website also provides a description and history of Shift4 Corporation.

- Is Shift4 a publicly held company and/or subsidiary of a parent company? **NO**
 - Shift4 is a Nevada Corporation and is a privately held, independent organization.
 - Shift4 is not wholly or partially owned by another entity.
 - Shift4 has no venture capitalists, independent, or institutional investors funding Shift4 Corporation.
 - Shift4 is self-funded and profitable, and as such is very stable.

- Does Shift4 partially own other business entities? **NO**

- Does Shift4 have an internal audit department? **NO**

- What mechanism does Shift4 have in place to show its financial stability?
 - Since 2003 an independent financial auditor has been retained to audit Shift4 financials and issue annual reports to the executive leadership.

- All financial audit reports have been issued with an unqualified opinion.
- Since Shift4 is not publicly held, it has no legal requirement to disclose any sort of financial information. If necessary however, Shift4's accounting office may provide a packet consisting of "ratio" documents based on fully audited financials.
- Does Shift4 have and maintain insurance? **YES**
 - Shift4 maintains Errors and omissions (E&O) coverage for up to \$5,000,000.
 - In addition, Shift4 has "umbrella" coverage for up to \$10,000,000.
- Does Shift4 have a pre-employment screening process? **YES**
 - Shift4 has a very involved employee vetting and boarding process where all employees (no matter the position applied for) must submit to a minimum of a:
 - Three agency financial background checks.
 - Local, State, and Federal criminal background checks
 - Full drug & alcohol screening via hair and urine samples.

Security and Information Technology (IT) Governance Overview:

- Does Shift4 have disaster recovery and business continuance plans in place? **YES**
 - Disaster recovery and business continuance plans are in place and are reviewed and tested at least annually.
 - Periodic risk assessments are performed and the plans are adjusted and retested as necessary.
 - The plans include detailed procedures to contact all affected customers, partners, and upstream and downstream processors and service providers.
 - Specific Service Level Agreement commitments are based on contractual agreement with each Shift4 customer.
- Does Shift4 have change control and backup procedures? **YES**
 - Shift4's 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 internal personnel and kept off-site from all data centers. No service providers are involved.
 - Cardholder data is encrypted on all media.

- Does Shift4 use third party service providers to handle backup media storage? **NO**
 - Shift4 does not use *any* third party service providers in the cardholder data environment.
- Does Shift4 have redundant systems and connectivity to ensure survivability? **YES**
 - All of Shift4's data centers include redundancy in all aspects of IT operations, including telecommunications providers, power grid, UPS, backup power generator, and HVAC systems according to industry best practices.

Logical Security Processes:

- Does Shift4 have written security policies and procedures? **YES**
 - New employees receive initial security orientation on all security policies and are required to read and acknowledge receipt and understanding of Shift4's end-user security statutes. Quarterly security awareness training is performed at all-hands meetings and security policy themed email reminders are sent to all employees on a bi-weekly basis. Finally, all employees are required to re-acknowledge their understanding of the end-user security statutes on an annual basis.
- Does Shift4 have a documented process for cardholder data, access control, encryption, and key management? **YES**
- Does Shift4 have systems security vulnerability and patch management policies? **YES**
 - Shift4's 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 applicable to Shift4 business operations and applicable to each particular system component are applied, and fully tested prior to full implementation.
- Does Shift4 have a data retention policy? **YES**
 - Cardholder data is retained for up to 24 months, based on the transaction type and customer requirement. Sensitive authentication data is automatically purged, post authorization, and is never retained. All other media follows explicit handling and destruction processes from shredding or pulping, to degaussing, software wiping, or actual physical destruction.
- Does Shift4 have layers of security such as firewalls, intrusion detection systems, intrusion prevention systems, file integrity monitoring, anti-malware, and access control systems?
YES

- Are Shift4's security systems monitored and updated on a regular basis? **YES**

Physical Security Processes:

- Do Shift4 data centers have fire detection and suppression systems? **YES**
- Do Shift4 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.
 - High security controlled areas, such as Shift4 data centers require a minimum of two phase authentication to gain entry.
- Are Shift4 premises under video surveillance? **YES**
 - Videos are retained on DVRs and then backed up and retained per industry guidelines.
- Are sensitive controlled areas alarmed and monitored by an armed response alarm monitoring company? **YES**
 - Employees of the alarm company are not authorized unescorted access to the data centers.