# Third-Party Service Provider Guidance

**Finance Area:**

Vice President for Finance

**Responsible or Contact Office/Role:**

Financial Reporting & Operations (Payment Card Services)

**PCI SCOPE :**

PCI DSS applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to ***all*** other entities that store, process, or transmit cardholder data and/or sensitive authentication data and may have an impact on the security of the cardholder data environment. (those entities

PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE.1 Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

All applications that store, process, or transmit cardholder data or may have an impact on the security of the cardholder data environment are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements.

**Definitions:**

**CDE-Cardholder Data Environment –** The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

**Eventbrite –** A University vetted and approved Third-Party vendor who specialize in event management and ticketing. The service allows users to browse, create and promote local paid or free events. The Eventbrite contract and interface is managed by ITS in partnership with Payment Card Services for UVa Academic departments. .

> www.its.virginia.edu/hosting/websites/ **Click** "SOFTWARE" on the ribbon the **Scroll** to – EVENTS, Video Conferencing and Web then **Click** Eventbrite

**Hosting Provider** – Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options. From payment applications to connections to payment gateways and processors: and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.

**Nested or Chained Third-Party Service Providers** – Any entity that is contracted for its services by another third-party service provider for the purpose of providing a service.

**PA-DSS** – Payment Application Data Security Standard and the Security

**Payment Application** – **Data Security Standards** In the context of a PA-DSS, a software application that stores, processes or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties. Refer to PA-DSS Program Guide for details.

**PCI-DSS – Payment Card Industry Data Security Standards** Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa. The Council is a global organization that maintains, evolves and promotes the Payment Card Industry Standards for the safety of cardholder data across the globe and includes merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

**PCI-DSS – Payment Card Industry Data Security Standards Council** was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa. The Council is a global organization that maintains, evolves and promotes the Payment Card Industry Standards for the safety of cardholder data across the globe and includes merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

**Service Provider** - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data (the Pay Now button). Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access-such as a telecommunications company providing just the communications link-the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

## Procedure:

Contact Payment Card Services for a new or pre-existing vendor agreement.

- Eventbrite – See ITS link www.its.virginia.edu/hosting/websites/ **Click** "SOFTWARE" on the ribbon the **Scroll** to – EVENTS, Video Conferencing and Web then **Click** Eventbrite
- Plan to meet with the PCS to discuss the way you will be implementing the contract with regard to payment card processing;
- Engage Procurement to assure that the vendor has agreed to the most recent Data and Intellectual Property Protection addendum;
- Provide an explanation of the services the vendor will provide, see application;
- Provide a list of third-parties the vendor deals with who are involved in the payment card process, *an annual requirement*;
- Provide a payment card flow diagram, ( PCI SAQ D for Service Providers Requirement 1.1.2 and 1.1.3 below), *an annual requirement*; (Processing e-commerce payments)
- Provide the last ASV Scan Report Attestation of Scan Compliance
- Provide an AOC and SAQ D for vendors processing <300,000 transactions annually or ROC from a QSA (Qualified Security Assessment firm) for >300,000 transaction processed annually for each nested vendor in the payment card flow process, *an annual requirement*.

See PCI SAQ D for Service Providers and specific standards (12.8 and 12.9) for validating compliance of Service Providers.

For the complete guidance document on choosing a Third-Party Services Provided see the following document from the PCI Council:

https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf

https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

**In the "Before You Begin" section of each SAQ is the following statement:**

*If there are PCI DSS requirements applicable to your environment that are not covered in the SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI compliant.*

**Whether your department completes an SAQ or not because you do not own the merchant number and do not have to attest to compliance, you are still obligated to comply with the standards regarding service providers and annually verify their compliance to University Payment Card Services.**

## PCI Guidance from the Standards

**Use of Third-Party Service Providers / Outsourcing from the Standards document.**

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are their customer's responsibility to include in their own quarterly scans.

Service providers are responsible for demonstrating their PCI DSS compliance, and may be required to do so by the payment brands. Service providers should contact their acquirer and/or payment brand to determine the appropriate compliance validation.
There are two options for third-party service providers to validate compliance:

1) **Annual assessment**: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or
2) **Multiple, on-demand assessments**: If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s)

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and/or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 below.*

| PCI DSS Requirements | Testing Procedures | Guidance |
|---|---|---|
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:<br><br>**12.8.1** Maintain a list of service providers including a description of the service provided. | **12.8** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows: | If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers.<br><br>Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, |

| | | |
|---|---|---|
| | **12.8.1** Verify that a list of service providers is maintained and includes a description of the service provided. | entities that receive data for fraud-modeling purposes, etc.<br><br>Keeping track of all service providers identifies where potential risk extends to outside of the organization. |
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.<br><br>**Note:** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | **12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. | The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity.<br><br>In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service. |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider. Specific due-diligence processes and goals will vary for each organization.<br>Examples of considerations may include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they will provide, etc. |
| **12.8.4** Maintain a program to monitor service providers' PCI DSS compliance status at least annually. | **12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually. | Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and those services in scope for the client's PCI DSS assessment. |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet. |

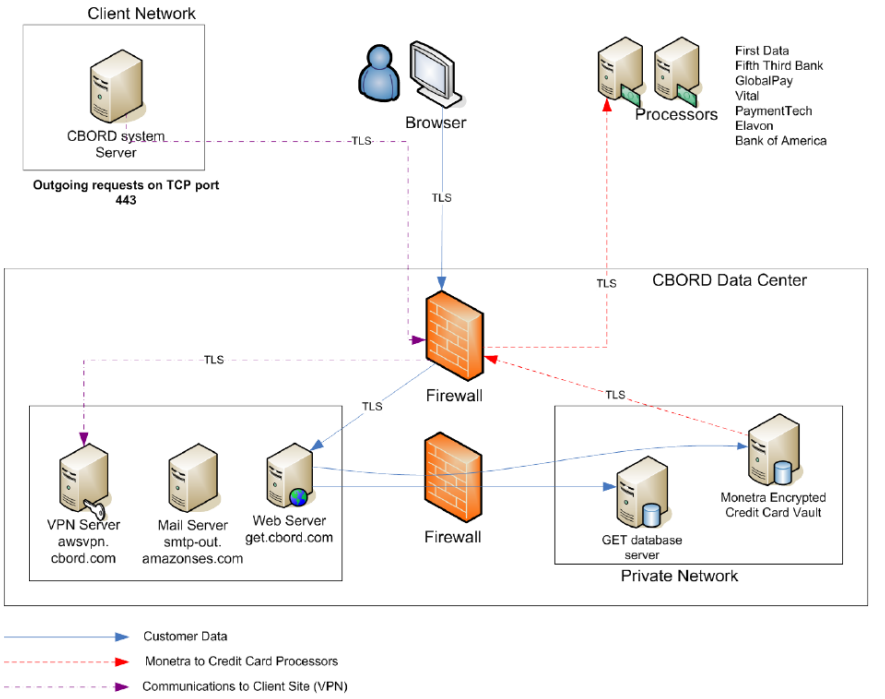
## Additional Supplemental Information:

| PCI DSS Requirements | Testing Procedures | Guidance |
|---|---|---|
| **1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks | **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks. | Network diagrams describe how networks are configured, and identify the location of all network devices. |

| | | |
|---|---|---|
| | **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. | Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise. |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks | **1.1.3** Examine data-flow diagram and interview personnel to verify the diagram:<br>• Shows all cardholder data flows across systems and networks.<br>• Is kept current and updated as needed upon changes to the environment. | Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network.<br><br>Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices. |

### Sample Card Flow Diagram

Diagram 1




**Resources:**

FIN-049: Revenue Generating Activities

Before a unit can engage in collecting revenue directly or indirectly or change a current a fee; the activities must be approved centrally and at the department level, conform to all University policies and procedures, Sales Tax implications must be addressed and the activity must not compete with private business enterprises.

**Revision History:**

December 4, 2018