New Merchant Request Companion Document

This document outlines the details of requirements in order to accept credit card payments. It is to be used to assist departments with gathering information to make the request to Financial Services and the Commerce Committee for new merchants. As each situation is different, this is a guide only. Financial Services will assist departments in coordinating with vendors on the requirements. It is important for the department to review the [University Policy on Accepting and Handling Payment Cards to Conduct University Business](#) before beginning this process.

Requestor (Department) must gather documentation to provide to the Commerce Committee. This documentation includes:

- Copy of Contract/Agreement with Vendor
- PCI DSS Attestation of Compliance (AOC)
- Complete Network Diagram, to include card payment process flow(s)

Brown University has contracted with several vendors to assist in the engagement of payment cards activity. These authorized vendors meet the University's requirements for security compliance and centrally controlled financial settlement of payment card transactions, while at the same time meeting the diverse needs of individual departments. The following questions identify if your request falls within the preferred authorized vendors. Requests that do not must offer evidence that the preferred vendors do not meet the business needs of the department, and the alternative vendor must meet the University requirements for security and integrating transaction information into Brown's financial systems. The Commerce Committee shall have the authority to decide whether or not to approve the department request for exception.

Does the Vendor Process to Heartland Payment Systems?

- Heartland is the preferred credit card merchant for processing card payments
- If the vendor does not process credit card payments via Heartland, Financial Services requires additional information and documentation:
    - Which acquirer/card processor does the vendor work with?
    - Contact information for the card processor
    - Is a contract required? Note: Contracts for acquirers/card processors are held by Financial Services.
    - PCI DSS Attestation of Compliance (AOC) for the credit card processor.
    - What fees will be charged?
    - Document detailing how the requestor will support this from a systems and implementation perspective, in addition to financial transactions and reconciliation.
      NOTE: All acquirers/card processors are considered a [level 3 security risk](#). If the preferred vendor, Heartland, is not being used, and any additional contract is required, the department should be aware of the additional time necessary for security and contract review.

Payment Processing Information

- For in-person payments, devices must be PCI Council Validated Point-to-Piont Encrypted (Validated P2PE)
    - Please provide the detail on the devices recommended by the vendor for in person payments. Financial Services will review and confirm if the devices are Validated P2PE.

- ○ If the devices are not Validated P2PE, approval for this exception will be required by the Commerce Committee. Also, additional detail regarding the scope of the Cardholder Data Environment (CDE) will be required, which includes a full network diagram. This is to minimize risk and to ensure that Brown remains in PCI DSS Compliance.
- For online payments:
  - ○ Is the vendor a TouchNet Ready Partner? https://www.touchnet.com/en/partners/touchnet-ready-partners
    - ■ Yes - If the vendor is a TouchNet Ready Partner, Financial Services will initiate a contract addendum (as part of the project) with TouchNet to add this partner. Please note that there will be an implementation fee (@$1250) and an annual hosting/access fee (@$1500) charged to the department for this service.
    - ■ No - additional information is required.
      - Which gateway services does the vendor work with?
      - Contact information for the gateway service
      - Is a contract required? Note: Contracts for card gateway services are held by Financial Services.
      - What fees will be charged?
      - PCI DSS Attestation of Compliance (AOC) for the gateway service provider.
      - Document detailing how the requestor will support this from a systems and implementation perspective, in addition to financial transactions and reconciliation.
      NOTE: All credit card gateways are considered a level 3 security risk. If the preferred vendor, Heartland, is not being used, and any additional contract is required, the department should be aware of the additional time necessary for security and contract review.

Commerce Committee Review

Once all information has been received by Financial Services, the Senior Director of University Receivables will bring the request to the Commerce Committee for review. The Commerce Committee may have follow-up questions or request additional information. The Commerce Committee has the authority to decide whether or not to approve the department's request.

Contract and Security Review

Financial Services and Commerce Committee review must be completed prior to the contract and security review processes.

Project Checklist

Once a project is approved, Financial Services will coordinate with the department, and the project manager (if applicable). Below is an example of a project checklist:

Initial Project Tasks		
Task	**Task Owner**	**Notes**
Data Gathering		Complete Network Diagram Attestation of Compliance Contract from Vendor

Commerce Committee Approval		
Provide project and vendor contact list	Department/Project Manager	
Project Manager	Department/Project Manager	
Departmental Contacts	Department/Project Manager	
Project Timeline	Department/Project Manager	
Project Milestones	Department/Project Manager	
Testing Schedule	Department/Project Manager	
Anticipated Go-Live Date	Department/Project Manager	
Merchant Setup		
Task	**Task Owner**	**Notes**
TouchNet Ready Partner Addendum (if applicable)	Financial Services	**Approx 4 weeks**
Submit New Merchant Request Form	Department Project Owner	COMPLETE
Update Master Merchant Listing with Contacts, etc.	Financial Services	
Request new AMEX Merchant (if applicable)	Financial Services	COMPLETE
Request new Heartland Merchant (if applicable)	Financial Services	COMPLETE
Update Master Merchant Listing with Heartland and AMEX #'s	Financial Services	COMPLETE
Information Guide on Devices (for in-person payments)		NA
Order devices	Financial Services	NA
Device Log		NA
Tamper Resistance Training		NA
Device Training		NA
Implementation Calendar for devices		NA
Payment Testing		Preferably 1 month prior to go-live
Department Refund Policy Updates		
Validate visibility of Refund Policy		

First Notice Rules Accounting Information	Department Project Owner	Worktags where revenue will post. We will need a Cost Center, Ledger Account, and Sales Code
First Notice Rules Update	Financial Services	FS will submit ticket to Workday team to setup/update First Notice Rules
Policies and Procedures	Department Project Owner	
PCI Compliance Training for departmental staff utilizing new system or terminals		Must be completed before individuals access the system or terminals.
Go-Live		
Post Go-Live		
Additional Training	Financial Services	FS to provide additional training to department on TouchNet or devices as needed
Ongoing Support	Financial Services	Provide contact information to department for ongoing support
Annual PCI Compliance Review	Department Primary Contact	Participate in annual PCI Compliance Review as requested to Financial Services

if accepting in-person payments

Appendix / Definitions

- Attestation of Compliance
  - This document is used by merchants and service providers to acknowledge that the company, their systems and devices are PCI DSS Compliant.
- Cardholder Data Environment (CDE)
  - This is the network environment that includes the people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
- Network Diagram
  - This document should depict the connections of system components and devices.
- Payment Card Payment Processor - Heartland Payment Systems
  - Brown University's preferred credit card processor. This third party provides processing services for credit and debit card financial authorization and settlement of all card transactions.
- PCI DSS
  - Payment Card Industry Data Security Standards
  - These standards ensure that Brown remains in compliance in payment card processing.
- Validated P2PE
  - Validated Point-to-Point Encryption
  - This is the most secure form of encryption for payment card processing devices and is validated by the PCI SSC (Security Standards Council)