Responsible Office: Cash Management
Date First Effective: 11/24/2008
Revision Date: 6/30/2013

Accepting Credit Card Payments

Policy Statement

Harvard University accepts credit cards as payment from external parties for certain goods, services, or gifts. Harvard mandates that all credit card-accepting local units, called "merchants," do the following:

1. For one-time sales, use the University's approved credit card processing vendor.
2. For ongoing sales, request set up through the central Cash Management office and comply with the credit card industry standards, University guidelines and annual certifications as set forth in the University Credit Card Merchant Handbook.

Reason for Policy

Credit card data is high risk confidential information that is protected by state and federal law and Harvard has a legal obligation to protect it. Credit card associations require all merchants to follow protocols titled Payment Card Industry Data Security Standards ("PCI DSS"), designed to prevent cardholder fraud and identity theft. All merchants must comply with PCI DSS before accepting credit cards and must also certify their compliance annually. The risks of non-compliance include substantial fines and penalties imposed on the University by the card associations, University liability for all financial losses incurred as a result of a security failure, and damage to the University's reputation.

Who Must Comply

All Harvard University schools, tubs, local units, Affiliate Institutions, Allied Institutions and University-wide Initiatives that process, store or transmit cardholder data or plan to outsource the process, storage or transmission of cardholder data.

Procedures *(see links in Related Resources section)*

1. **Determine the scope of credit card needs**. While accepting credit cards is a convenience for customers, it also entails legal/financial risk for merchants and requires substantial compliance activities. Local units should consider the risks and responsibilities associated with accepting credit cards, as well as credit card payment alternatives, before requesting a merchant account.
    A. One-time events: Local units that want to accept credit cards for one-time events (such as a conference or seminar offered to the general public) **must** use the University's approved vendor for credit card processing service. This service provides units the convenience of accepting credit card payments without the extensive set up required and ongoing merchant account maintenance. Contact Campus Services Events for details.
    B. All other sales: prepare to consult with CMO about your needs.
        a. Review Appendix A, New Credit Card Merchant Account Request, to understand the types of information required for merchant set up.
        b. Review Appendix B, Summary of the Harvard University Credit Card Merchant Handbook, to understand the types of compliance activities required of merchants.
        c. Prepare a rough estimate of monthly dollar and transaction volumes.
        d. Ready a list of any questions.

2. **Contact the CMO at PCI_Compliance@harvard.edu.** The CMO will provide additional guidance to units considering merchant set up. CMO can also offer alternative payment suggestions to units for whom merchant set up and maintenance is not suitable.

3. **Read the full Harvard University Credit Card Merchant Handbook,** for a complete discussion of the requirements and procedures surrounding the acceptance of credit cards at the University before submitting a request for merchant set up.

4. **Request merchant set up.**
   A. Tub financial deans or equivalent must request merchant accounts on behalf of their departments.
   B. To establish a new merchant account, complete and submit the following forms to the CMO:
      a. New Merchant Request Form
      b. Harvard Credit Card Merchant Agreement
   C. Allow sufficient time for merchant set up. Depending on the complexity of the request, setting up a new credit card merchant account can take several weeks after the CMO has received and approved all of the appropriate documentation. Due to the time requirements for setup, departments should request credit card merchant accounts as soon as possible after determining one is needed.

5. **Plan for appropriate use.**
   A. Intercompany transactions: to minimize costs and also ensure accurate accounting, in most cases, Harvard merchants must not accept University purchasing cards (PCards) or University corporate cards for payment of University business purchases. See the Internal Billing and Purchasing Card policies.
   B. Acceptable cards: Harvard merchants may accept VISA, MasterCard, Discover and American Express.

6. **Perform annual PCI compliance activities.** These include annual certifications, reconciliations, and audits where appropriate. See Appendix C for details.

7. **Annually, review existing merchant accounts and close unnecessary ones.**

Responsibilities and Contacts

Financial deans or equivalent tub financial officers are responsible for ensuring that local units abide by this policy and the accompanying procedures.

Cash Management Office (CMO) within the Office of Treasury Management, is responsible for maintaining this policy and the Credit Card Merchant Handbook, answering related questions, and managing and reporting the University's compliance status. ***Contact:*** ***http://vpf-web.harvard.edu/otm/home/hom_contact.shtml***

Harvard University Information Technology IT Security (HUIT IT Security) provides technical assistance to the Cash Management Office and schools/units and ensures that all merchants are in compliance with University high risk confidential information (HRCI) policies and PCI DSS requirement. ***Contact:*** ***http://www.security.harvard.edu/***

Campus Services Events is responsible for setting up Harvard units with credit card processing services for one-time events. Contact: ***events@harvard.edu***

Risk Management & Audit Services (RMAS) performs periodic merchant audits and evaluates the security levels of credit card server locations. ***Contact:*** ***http://rmas.fad.harvard.edu/people***

Related Resources

New Merchant Request Form: http://vpf-web.harvard.edu/otm/protected/NewMerchantRequestForm.pdf
Harvard Credit Card Merchant Agreement: http://vpf-web.harvard.edu/ofs/policies/documents/credit_card_merch_handb.pdf
Full Harvard University Credit Card Merchant Handbook
PCI self-assessment questionnaire: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php
PCI Security Standards Counsel, for information on data security standards: https://www.pcisecuritystandards.org/
Cash Management credit card security breach procedures: http://vpf-web.harvard.edu/otm/protected/pci_security_breach_business_process.pdf
Internal Billing policy http://vpf-web.harvard.edu/ofs/policies/documents/inter_billi_trans.pdf
Purchasing Card policy: http://vpf-web.harvard.edu/ofs/policies/documents/purch_card.pdf

Definitions

Customer: An individual or other external entity that makes a payment to the University for goods, services or gifts.
Merchant: A local unit that accepts credit and/or debit cards as a method of payment for goods, services or gifts.
Merchant account: An account established with the University's credit card processor to uniquely identify the local units credit/debit cards sales and processing fees.

Revision History

6/1/2013: updated format, added appendices

Appendices

Appendix A: New Credit Card Merchant Account Request
Appendix B: Summary of the University Credit Card Merchant Handbook

APPENDIX A

Harvard University

New Credit Card Merchant Account Request

Purpose of the credit card merchant account *Brief description of the goods or services for which you want to accept credit cards*	
Estimated annual activity volume *Include both numbers of transactions and total dollar value*	
Business Case *A business case for why you need to accept credit cards. Please include who your customers are and the impact to your organization if you can't accept credit cards. Also describe any challenges you have with your current method of accepting payments.*	
The target date for setup	
The name of the new account *This is the name that will appear on the customers credit card statement*	
The Tub and Org *where credit card transactions should be posted in the general ledger*	
Clientele, who will be the customers? *E.g., students, General population, Alumni etc*	.
What type of credit cards do you wish to process? *E.g. MC/Visa, Amex, Discover*	
How will credit cards be accepted? *Please check all methods of acceptance.*	☐ Card Present ☐ Phone ☐ Fax ☐ Web
FOR THE FOLLOWING SECTIONS ONLY FILL OUT THOSE THAT APPLY TO YOUR METHOD OF ACCEPTANCE	
If web based, what software will be used to accept the credit cards?	☐ Locally Developed application using HOP ☐ Off the shelf software ☐ Solution hosted by Certified PCI compliant Service Provider
If terminals will be used, enter equipment information *Contact Cash Management for additional information on options available.*	Terminal type and quantity Printer type and quantity Pin pad type and quantity Whether Lease, rent or purchase (Leasing recommended) Address where equipment is to be shipped:

If Point of Sale System (POS) to be used:	Name of POS application Name and version of POS Software Whether authorizations will be done via Dial-up or Internet Where the POS application will be hosted Whether Wireless technology will be used.
ALL MERCHANTS MUST PROVIDE CONTACT INFORMATION	
Contact Information	(Name, address, Phone and Email) for:
Business owner *(This is generally the head of a department or unit. All communications regarding compliance will go to this individual.*)	
Primary Business Contact *(This is the contact for day to day operational issues).*	
Alternate Business Contact *(Used when the Primary Contact is unavailable)*	
Person responsible for posting the credit card activities and resolving **reconciliation** issues.	
If applicable, IT person responsible for compliance testing or **technical support**.	

Merchant:
My signature below indicates that I have reviewed the Harvard Credit Card Merchant Handbook and the PCI Data Security Standard. I understand the responsibilities of a credit card merchant

Requested (Business Owner) _____

CIO:
*[The School CIO of school units or the University Chief Information Officer for Central Administration and Affiliate Organizations must sign all request except for merchants **only** using dial-up terminals)*

- ☐ My signature below indicates that I have reviewed the Harvard Credit Card Merchant Handbook and the PCI Data Security Standard. I understand the technical responsibilities for maintaining a secure credit card environment.
- ☐ My signature below indicates I am aware of the application but it is being hosted by an external service provider.

.

(Chief Information Officer) _____

Financial Dean:
My Signature bellows indicates that I approve this request and understand the obligations of adding an additional credit card merchant.

(Financial Dean)_____

APPENDIX B:

Summary of the Harvard University Credit Card Merchant Handbook

The following is a high level summary of the Harvard University Credit Card Merchant Handbook. This summary is intended to provide interested units with an overview of the compliance activities required of University merchants. It is not intended to supplant the more extensive full Harvard University Credit Card Merchant Handbook.

Required Local Policies

Harvard University credit card merchants must have local policies and procedures for the handling of credit cards. Local policies and procedures should supplement this policy, the Harvard University Credit Card Merchant Handbook, and security policies found on the University's Information Security and Privacy website (www.security.harvard.edu).

Employees involved in credit card processing must read and understand both local credit card policies and the University's credit card policies published on the Cash Management website. Employees must annually sign the Credit Card Merchant Agreement to acknowledge that they have read and understood the policies and that they will comply with them. Additionally, employees must complete annually online training via Eureka and obtain the Certificate of Completion relating to PCI DSS.

Security

In order to accept credit cards over the Internet, a merchant must have a secure website. In addition, RMAS must evaluate all physical locations that will house credit card servers and will bring control weaknesses to the attention of tub management, CMO and HUIT IT Security. Individual credit card information is confidential; failure to maintain strict controls over this information could result in unauthorized use of a credit card number and serious problems for both the customer and the merchant. The risks of non-compliance by the University include substantial fines and penalties imposed by the card associations, reputational damage to the University, and merchant liability for all losses incurred as a result of a security failure. In the event of a security breach, all penalties, fines and costs imposed by the credit card associations and the banks are the responsibilities of the local units.

Background Checks

Background checks must be performed on employees who have access to credit card account numbers. Local units must have local policies defining which positions require account-number access and attendant background checks. Background checks should be carried out by local Human Resources departments, and evaluated in conjunction with the Office of the General Counsel. For details, refer to the Harvard HR policy on pre-employment screening (available only to HR administrators, at http://hr.harvard.edu).

Compliance and Annual Certification Requirements

Due to widespread identity theft, fraudulent credit card activity, and other security threats, the credit card associations (Visa, MasterCard, etc.) have mandated compliance with PCI data security standards for any merchant or service provider that "transmits, stores, or processes" cardholder information. In order to accept credit cards, each merchant must be certified annually to be in compliance with PCI data security

standards. Merchants will receive a compliance certificate once they have completed and passed the requirements.

New merchants must be certified before they can begin accepting credit cards. Cash Management will deactivate any merchant account if the local unit does not receive or maintain PCI certification. Any merchant who fails a monthly scan must communicate a corrective action plan within five days and correct all failing vulnerabilities within 30 days. Cash Management will deactivate the merchant if these vulnerabilities are not corrected within 30 days. Exceptions can only be approved by the PCI Committee. Cash Management will notify the financial dean or equivalent, RMAS and the PCI Committee of any PCI-related failures and merchant deactivations.

Audits

Merchants are subject to periodic audits by RMAS. RMAS will either conduct these audits themselves, or contract with a third party to conduct them. Cash Management will receive a letter indicating any non-compliance with PCI requirements. Merchants will be required to correct any deficiencies as agreed to in the audit report and as mandated by PCI standards. If deficiencies are not corrected within 30 days, Cash Management will deactivate the merchant. Cash Management will notify the merchant's financial dean or equivalent, RMAS and the PCI Committee of any deactivation.

Monitoring and Security Incident Handling

Merchants and system operators must notify Cash Management immediately in the event of a breach or suspected breach of credit card data security.

Cash Management has established procedures to use after being notified of a security breach (http://fad.harvard.edu/otm/protected/pci_security_breach_business_process.pdf). Schools and local units must establish and document local procedures for ongoing system security monitoring, and for what to do in the event of a security breach.

Reconciliation Procedures

1. The merchant is responsible for posting all credit card transactions and associated fees via journal voucher on a monthly basis.
2. The Cash Management Office is responsible for performing monthly reconciliations of the bank accounts that receive credit card funds.
3. The merchant is responsible for researching and resolving an unreconciled transaction within three months of the transaction date.
4. On a monthly basis all transactions 90 days or older that have not been posted to the general ledger by local units will be posted by Cash Management to the appropriate local-unit default coding.

Data Access and Record Retention

Customer credit card records located within local units must be stored in locked cabinets, and access must be limited to those employees who need this information to accomplish their work. All paper and electronic records must be destroyed in accordance with the University's general record retention schedule (http://www.grs.harvard.edu/).