Responsible Office: Cash Management
Date First Effective: 11/24/2008
Revision Date: 6/30/2013.01M

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," investigate the following options before requesting a new merchant account:

- Central Accounts Receivable, web-based billing and collection system for local units wishing to invoice "external" customers
- TouchNet uStores, ecommerce storefront for event tickets, conference registrations, subscriptions, merchandise, and fees.
- Review eCommerce Payment Decision Tool to determine which payment product matches your needs.

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 because 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 well-accepted method of payment for customers, it 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. Review eCommerce Payment Decision Tool to determine which payment product matches your needs.
    B. PrepareP to consult with CMO about your needs.
        a. Review TouchNet Marketplace eCommerce Tool for detailed information about online payment acceptance options. When using TouchNet uStores, an ecommerce storefront, departments can leverage the tub's central finance merchant account to minimize PCI Compliance responsibilities.
        b. Review Appendix A, New Credit Card Merchant Account Request, to understand the types of information required for merchant set up.
        c. **Review Appendix B, Summary of the Harvard University Credit Card Merchant**

Handbook, to understand the types of compliance activities required of merchants.

d. Prepare a rough estimate of monthly dollar and transaction volumes.
e. 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 3-4 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 Harvard Credit Card Merchant Handbook 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: pci_compliance@harvard.edu***

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: https://security.harvard.edu/report-incident***

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

Credit Cards – Office of Treasury Management
Credit Card Security Breach Procedures
eCommerce Payment Decision Tool
Harvard Credit Card Merchant Agreement
Harvard University Credit Card Merchant Handbook
Internal Billing Policy
New Merchant Request Form
PCI Self-Assessment Questionnaire
PCI Security Standards Counsel Data Security Standards
University-Issued Card Policy

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

6/1/2013.01M: revised 04/22/2024 corrections to dated information links and contact information

Appendices

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

Appendix A
Credit Card Merchant Request Form

New Credit Card Merchant Request Form

Purpose of the credit card merchant account

_____

Clientele, who will be the customers? ☐ Students ☐ Alumni ☐ Public

Estimated annual activity volume # _____ $ _____

The name of the new account _____

Target date of setup _____ **Tub** _____ **Org** _____

What types of card will be accepted?

☐ Visa / Mastercard ☐ Amex ☐ Discover

How will cards be accepted?

☐ Credit card present ☐ ecommerce ☐ Virtual Terminal ☐ Phone/mail order

If ecommerce, what software will be used to accept cards?

☐ Locally developed application ☐ Third Party software ☐ Off the shelf software

If ecommerce, where will website be hosted?

☐ @Harvard ☐ @Third Party ☐ @Hosting site (vendor name) _____

If terminals will be used, where will the equipment be shipped?

Address _____

City _____ State _____ Zip _____

If Point of Sale (POS) is to be used:

Name of POS _____

Name and Version of POS software _____

Authorizations will be done by ☐ Dial-up ☐ Internet

Where will POS be hosted? _____

Business owner (department or unit head)

Name _____ Phone _____ Email _____

Address _____

Reconciliation contact

Name _____ Phone _____ Email _____

Address _____

IT contact (responsible for technical support)

Name _____ Phone _____ Email _____

Address _____

Primary business contact (operational contact)

Name _____ Phone _____ Email _____

Address _____

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) _____ **Date** _____

Financial Dean

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

(Financial Dean) _____ **Date** _____

Chief Information Officer

[The School CIO for school units or the University Chief Information Officer for Central Administration and Affiliates 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.

(CIO) _____ **Date** _____

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 Harvard Training Portal 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. Individual credit card information is confidential and is never collected or stored electronically; 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. Merchants are still responsible for complying with PCI data security standards regardless if they outsource the processing of credit card data to a third party service provider/payment processor. 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 ((https://otm.finance.harvard.edu/how-to/credit-cards/credit-card-security). 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. Merchants using TouchNet uStores and/or uPay may have TouchNet generate a nightly update of revenue to their department coding. All other merchants using other payment gateways (such as CyberSource) are responsible for posting all credit card transactions. All merchants are responsible for posting 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 records must be destroyed in accordance with the University's general record retention schedule (https://library.harvard.edu/services-tools/general-records-schedule).