Harvard Credit Card Merchant Agreement (HCCMA)

I. Introduction

The Harvard credit card merchant agreement represents the terms and conditions for Harvard University departments obtaining a credit card merchant account.

1. Purpose of this document

This agreement provides the basis for a partnership between Cash Management (CM), Harvard University Information Technology IT Security (HUIT IT Security) and _____ (merchant/local unit). It details the services provided by CM and HUIT IT SECURITY and outlines the basic responsibilities of each party involved. Throughout this document the term ***Merchant*** refers to the local unit named above.

2. Dispute resolution

The primary point of contact is the CM credit card accountants at 617-495-4397 or 496-0853. If a satisfactory resolution has not, or cannot be reached, the problem will be brought to the attention of the Manager of Cash Management. For current contacts, please refer to the list of contacts provided on Cash Management's web site. CM and HUIT IT SECURITY play a primary role in interpreting the policies and procedures outlined in this document and other University communications pertaining to credit card processing. CM is the only area with employees authorized to contact our credit card processor. Bank of America Merchant Services (BAMS), Harvard's preferred merchant services provider, provides equipment and other operational assistance to our merchants.

II. General Responsibilities

CM agrees to:

- Set up and maintain merchant account(s) with the credit card processor.
- Notify merchants on a regular and timely basis about service availability, product features and upgrades and changes to University and credit card association policies.
- Provide customer support via telephone and e-mail during normal business hours (Monday thru Friday, 9 AM – 5 PM).

Merchant agrees to:

- Read, understand and carryout all responsibilities outlined in the Harvard Credit Card Merchant Handbook.
- Attend annual campus credit card training meetings and implement any changes expected by the card processor. Information about these will be provided by CM.
- Meet connectivity and security requirements as provided herein.
- Follow University policies and procedures for ensuring data security and comply with guidelines for credit card acceptance.

III. Account Setup, Testing, & Maintenance

Account Setup

Upon receipt of signed, completed Credit Card Merchant Account (CCMA) Merchant Request Form, CM will do the following:

Present request to eCommerce Manager for approval.
If Approved:

- Create a merchant account with a credit card processor contracted by Cash Management.
- Create an account in the TrustKeeper portal used for compliance certification for the merchant account.
- When required, initiate requests for:
  1. TouchNet or CyberSource account (preferred Internet Gateway)
  2. ClientLine – access to Bank of America Merchant Services web base platform

Before the user can create transactions, the merchant must be certified to be in compliance with Payment Card Industry (PCI) Standards. Compliance is certified through the completion of a self-assessment questionnaire in the TrustKeeper compliance portal and if required, a successful scan of any website that either hosts ecommerce activity or redirect to another site.

Account Set up Process Time

Depending on the complexity of the set-up process, establishment of a new account can take a number of weeks. This period of time may be necessary because of the number of third parties involved in the process, particularly for web-based merchants, which Cash Management cannot completely control. Request should be made early enough to allow for enough time. (Recommendation is 4-6 weeks.)

User Training

Cash Management will provide basic training and documentation to outline the transaction authorization and settlement process. Participation is required before the credit cards can be accepted, and the account activated.

Account Maintenance

Cash Management will act as a liaison to the bank, gateway and processor.

Refunds/credits to an account must be processed by a different user authorized to access that account. The user who creates a transaction cannot process a refund/credit.

Requests to activate, deactivate, or suspend a merchant account must be received in writing from an authorized signer(s).

IV. Security

Security is a top priority for credit card transactions. In order to accept credit cards over the

Internet, a merchant must have a secure web site to protect the safekeeping of cardholder information. 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, as well as reputational risk and 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 responsibility of the local units.

Merchant-level Security

It is the merchant's responsibility to maintain a secure environment for credit card processing. Merchant agrees to take sufficient measures to ensure security of a cardholder's information and to comply with all state and federal data privacy and security laws.

Restrict access to authorized administrative users.

Merchant must *never*:

- Transmit credit card information via unencrypted e-mail.
- Store card information in an unsecured database or other electronic medium.

CM reserves the right to suspend or terminate service at any time if sufficient security measures are not employed by the merchant.

V. Third Party Vendors

Merchants are responsible for third party processors that they grant access to cardholder data. Merchants must only use Level 1 PCI validated service providers to handle or process cardholder account numbers.

All vendors with access to cardholder account numbers must be contractually obligated to comply with the PCI requirements. Merchants must notify Cash Management of service providers being used and obtain prior approval.

All third party vendors must include the University PCI Rider in contracts with merchants.

VI. Support

Technical

- TouchNet and CyberSource provides support to Merchants using uStore, uPay or Secure Acceptance.
- Merchant is responsible for establishing and maintaining local website.
- CM does not provide any technical assistance to the Merchant.
- Technical Support beyond HUIT IT SECURITY Security's guidance must be separately contracted with HUIT IT SECURITY

Administrative

- Cash Management
    - Manage bank relationship

    - Be primary liaison between bank and local unit on issues related to the bank
    - Reconcile bank account to the general ledger
    - Notify the Merchant about any reconciliation or deposit problems
    - Post any unreconciled items over 90 days old to default coding provided by merchant
- Merchant
    - Ensure that a mandatory reviewer is set up for each account used
    - Post revenue (credit card deposits) and expenses (credit card fees) in a timely manner to the General Ledger
    - Research and resolve any un-reconciled items in a timely manner
    - Ensure that any refunds/credits are processed by a user other than the one who created the original transaction.

- The CM Support Team is the Merchant's first line of contact for support. Support Team members can answer questions about:
    - Merchant setup and maintenance
    - Billing questions
    - General processing questions

VII. Reporting

Bank of America Merchant Services (BAMS) provides online access to your credit card transactions. Cash Management will set up merchant user responsibilities in the system as well as merchant user access to TouchNet or CyberSource. If a local unit uses TouchNet or CyberSource, then Cash Management will provide authorized users with access to review reports from the gateway. Merchants must notify Cash Management if the authorized users need to change.

VIII. Cost and Billing

Bank Fees

Processor fees are negotiated by CM and are subject to change without notice.

- Bank fees are billed directly to the merchant in the form of interchange and assessment fees. It is the responsibility of the merchant to post these fees to the general ledger. The actual payment is deducted directly out of the bank account.
- Visa and MasterCard have a complex fee structure based on the type of card used, payment channel used (card present or card not present) and prior electronic authorization. A detailed description can be found at these sites.

  http://www.mastercard.com/us/merchant/how_works/interchange_rates.html
  http://usa.visa.com/merchants/operations/interchange_rates.html

IX. Signatures

The parties listed below agree to the terms and conditions listed in the HCCMA. Any updates to the original agreement shall be considered part of the original agreement entered into unless written notification within 30 days is provided by party, thereby nullifying said agreement.

Department Name: _____
Department Default Coding: _____
Merchant Name: _____

_____ _____
Department Representative/Business Owner Date

School CIO's or the CISDPO are responsible for security of electronic storage and processing of credit card data.

_____ _____
School or Unit CIO or the CISDPO Date

Not Required by Merchants using only Dial-up terminals

_____ _____
Financial Dean/Financial Director Date