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/).