

University of Massachusetts Standards for Acceptance of Debit and Credit Cards

Many University departments (also referred to as merchants) are accepting debit and credit cards (i.e., Card) either over the web, via fax, telephone or point of sale terminal/device. This exposes the University to become a target for bankcard fraud. Many of the card features that prevent fraud when a physical card is required to process a transaction do not apply in the “card-not-present” environment. Therefore, there is a greater need to protect against fraud and possible losses especially since “card-not-present” merchants can be held financially responsible for fraudulent transactions, even if the Card Issuers (i.e., Visa, MasterCard, etc.) have approved the transactions.

Purpose

To reduce the risk of debit and credit card fraud, protect University resources and to ensure card holder data is private and secure, the University has established standards for protecting debit and credit card data and transactions.

Scope

These standards apply to all debit and credit card transactions/ecommerce activity where the University or its departments is considered the merchant

General

The required handling, storage and security of personally identifiable (e.g., Card information) and protected information is detailed in the [University Data and Computing Standards](#).

Debit and Credit Card Use, Authorization and Monitoring

Schools and departments that are planning to accept debit and credit cards must contact their Campus E-Commerce Representative. Campus E-Commerce representatives must approve any decisions to accept debit and credit cards or other electronic form of cash receipts.

The Campus E-Commerce representative and Campus Bursar will work with departments and provide the necessary guidance in the areas of [Payment Card Industry Data Security Standards \(i.e., PCI DSS\)](#) compliance, internal controls, deposit techniques and reconciliation. All new e-commerce sites must be approved by the Campus E-Commerce Representative.

Bank accounts and debit and credit card accounts may only be opened by the University Treasurer’s Office. Any bank account that has been opened with University/Campus funds and has not been authorized by the University Treasurer’s Office must be closed immediately.

Each campus must maintain a complete and accurate inventory of all debit and credit card processing locations; this should include documentation regarding third party vendors contracted to process debit and credit cards. Process flows and technology configuration should be documented and updated as needed.

CyberSource has been identified as the third party vendor of choice for all e-commerce activity. Any deviation from the use of CyberSource must be approved by your campus Vice Chancellor for A&F as well as the E-Commerce Committee. Proof of PCI DSS compliance must be provided on an ongoing basis.

Approved: 08/11/08

The University has approved scanning vendors and third party credit card processors, contact your campus E-commerce representative or the University Treasurer's Office for a list of accepted vendors.

All new contracts with third party or outside vendors must contain language requiring that the vendor be PCI DSS Compliant and they will remain PCI DSS Compliant. Failure to do so should result in the termination of the contract at no penalty to the University of Massachusetts.

Security

All University and Campus debit and credit card applications must comply with these standards and the PCI DSS. All third party vendors are subject to the same standards for data compliance and security.

All new Card processing computer applications that use Internet connections must be tested, scanned and compliant prior to their being moved into production/"going live".

System patches shall be made within one month of the patch becoming available for any part of the system which helps process or store credit card transactions.

Card information should not be communicated via unencrypted electronic communications (e.g., email, instant messaging). Merchants shall not email/instant message Card information. If a merchant contacts a customer via email/instant message all card information must be deleted prior to the message being sent.

Under no circumstances should Campus merchants take a photocopy of a customer's debit or credit card.

After a transaction has been authorized access to card data should be limited to staff with a business need to access this information. All hardcopy Cardholder information shall be securely stored and properly destroyed in compliance with [University Data and Computing Standards](#).

Campus merchants may not store in any manner the magnetic stripe data, card verification value (i.e., CVV2 – the 3 or 4 digit security code printed on the back of a credit card) or personal identification number (i.e., PIN) of the customer. If the credit card processing system automatically generates a receipt which displays the card number, the first 12 digit must be defaced with permanent marker. If the electronic Card processing system is storing the debit card number or full 16 digits of the credit card, the system must be modified to only print the last four digits of the credit card number. If there is a business requirement to store the full 16 digit debit or credit card number it greatly increases the compliance burden for safeguarding this information. Any of these exceptions must be documented and approved by the campus Controller and the E-commerce representative.

The University Records Retention and Disposition Schedule require merchants to retain the original signed debit or credit card merchant slip for 3 years. This complies with current credit card association requirements. Signed debit and credit card merchant slips shall be kept locked and secure. They should be securely destroyed directly from archives in compliance with [University Data and Computing Standards](#) and [Massachusetts Law 93I](#) which addresses the destruction of records containing personal information. Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than \$100 **per data subject affected**, provided said fine shall not exceed \$50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Campuses should use network segmentation and firewalls that isolate systems that store, process, or transmit cardholder data from the rest of the network, to reduce the scope of the cardholder data environment

Approved: 08/11/08

Very few authorized users should have access to Card data after the transaction has been authorized. Other authorized users should either not see any data or see a masked number with only the last 4 digits visible.

Campuses shall:

- Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files, including logs; and configure the software to perform critical file comparisons at least weekly. Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise.
- Perform penetration testing including network and application layer penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such upgrade, a sub-net environment, or an environment).
- Use network intrusion detection systems, host-based intrusion detection systems, or intrusion prevention systems to monitor all network traffic transmitting cardholder data and alert personnel to suspected compromises.

Computer logs of card transaction activity should be maintained for one year in compliance with the [University Computer Network And System Records, Logs And Structures Policy](#). Additionally, a minimum of 3 months of credit card transaction log activity will be available online.

Payment Card Industry Data Security Standard (i.e., PCI DSS)

The PCI DSS applies to:

- The security of transactions related to all credit card brands (e.g., Visa, MasterCard, Discover, American Express, Diners Club, etc.)
- All “system components.” The PCI Data Security Standard defines a system component as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

The PCI DSS contains two main requirements:

- The requirement to comply with the PCI Data Security Standards which are comprised of 12 broad requirements within 6 categories of security safeguards/controls.
- The validation of compliance whereby entities verify and demonstrate their compliance status. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained.

Approved: 08/11/08

Compliance to all PCI DSS standards is mandatory. Each merchant shall complete and submit an Annual Self-Assessment Questionnaire and run quarterly security scans on all outward facing IP addresses handling cardholder data. All documents should be forwarded to the appropriate E-commerce Representative.

A current PCI DSS and Self Assessment Questionnaire can be found at: www.pcisecuritystandards.org.

All outward-facing IP addresses as well as URL's on network segments that have servers that accept, store or transmit credit card numbers must be tested/scanned and certified.

The University outsources storage, processing, and transmission of cardholder data to third party providers such as CyberSource. PCI DSS requires that the University document the role of each service provider on the Report on Compliance. Additionally, the third party provider is responsible for validating their own compliance with the PCI DSS requirements, independent of their University scans/audits. Campuses shall have all PCI DSS compliance certificates on file for non-CyberSource contracted third party providers. The Treasurer's Office shall have CyberSource's PCI DSS compliance certificate on file.

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (LAN) is connected to or part of the cardholder environment (for example, not clearly separated by a firewall), the Requirements and Testing Procedures for wireless environments apply and must be performed as well.

Physical Card Processing

Campus merchants should use point of sale terminals that allow them to enter debit or credit card account numbers and expiration dates. The terminal uses the phone line or encrypted Internet connections to contact a service provider. These devices must be purchased or approved through the University Treasurer's Office.

Campus merchants must receive authorization from the IT department prior to the purchase, lease, or on-line evaluation of any point of sale device if the device will be connected to the Campus network.

Phone, Mail, And Fax Card Transactions

If debit or credit cards are accepted either over the phone, mail or via fax, they should be processed using one of the following:

- Point of sale terminals.
- CyberSource's virtual terminal if you have an authorized account.

Chargebacks and Requests for Copy

A request from one of the charge card brands or our merchant bank must be processed in accordance with the Payment Brands (i.e. Visa, MasterCard) rules and regulations. Failure to respond to the request within the requested time frame results in a chargeback and loss of the funds for the campus or department.

Breach or Unauthorized Disclosure of Card Information

In 2007, a Massachusetts State Law ([Chapter 93H](#)) went into effect that requires disclosure in the event of:

- Unauthorized acquisition or unauthorized use of unencrypted personal data or,
- Encrypted electronic personal data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information,

Approved: 08/11/08

maintained by an agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. This law applies to and defines personal information as a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

- (a) Social Security number;
- (b) driver's license number or state-issued identification card number; or
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

In the event of a security breach of Card numbers, merchants should follow the [University Personally Identifiable or Protected Information Comprise Incident and Notice Procedures](#).

Additionally, the Payment Card Industry has defined Cardholder Data compromise procedures that work with the requirements under M.G.L. 93H. Both M.G.L. 93H and the PCI cardholder data compromise procedures shall be complied with when a data security breach has occurred.

Compliance

Ecommerce representatives, in coordination with the Treasurer's Office, have the authority to shut down a merchant who is not in compliance with University of Massachusetts PCI DSS Standards.

If merchant or service provider does not comply with the PCI DSS or fails to rectify a security issue, they may be fined or their use of Card processing restricted. Fines and penalties arising from a merchant's failure to follow/comply with the PCI DSS are responsibility of the violating campus. Campuses may assign responsibility for the fines to the responsible department.