# Brandeis University Credit Card Processing Policy and Procedures

## Policy

Brandeis University currently accepts credit cards at several locations on campus as well as on the telephone and web. The University is responsible for safeguarding and protecting all consumer data received with credit card transactions in accordance with applicable laws and regulations such as PCI-DSS and MA 201 CMR 17.00.

- Card Swipe and POS (Point of Sale) terminals that retain credit card information are not permitted at Brandeis.
- The use of Virtual Terminals that employ a Card-Not-Present method is the only approved way of accepting credit cards.
- It is not permitted to retain full credit card information on campus in any form once the transaction is complete.

## Procedures for Credit Card Processing

- All merchant ID accounts must be set up by the Treasury Services Department. Please forward all documentation to Carol DePasquale at cdepasqu@brandeis.edu.
- Any unauthorized merchant accounts will be closed upon discovery.
- Draft business practices and procedures must be submitted to Treasury Services for approval.
- You must use the University approved vendors.

## Merchant Account Authorization

- Schools and departments that have business requirements to accept credit cards must contact Treasury Services at extension 6-4437 before setting up a merchant account. Treasury Services will assist you in the set up of both the credit card merchant account and the bank account. Treasury Services will provide the tools and resources for you to effectively manage credit card processing.
- Recommended procedures can be found on the Visa website (www.visa.com) or obtained from Treasury Services.
- Compliance with these procedures will prevent Brandeis University from retaining credit card information and which reduces the burden on the university having to provide security of credit card data. Charge backs to customer accounts also may be processed in the same manner.

## Departmental Policies and Procedures

Treasury Services will assist the schools and departments to develop policies based on the business needs of the school or department on the following issues:

- **Chargebacks:**
    - Who will have authority to process? Who will do the monitoring?
- **Data Access:** The account owner and one other individual should have access to credit card data until authorization has been obtained. Other individuals should see the last 4 digits of a credit card number as required by law since November 2005.
- **Transaction Processing Security:** Individuals who handle credit cards should have separation of duties and authority. One person should not be able to authorize, settle, and do returns/chargebacks. The person entering transactions should not have the authority to perform the daily settlement.
- **Passwords:** Passwords must be changed regularly. Use caution when selecting a password as it should not be easily guessed or be the same as any other password.
- **Retention:** Each school or department should have a data retention policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy.
    - **Electronic** - Credit card numbers will not be stored on campus in electronic form. It is permissible to retain the last four digits of the credit card number.
    - **Paper** – According to the credit card issuers and Federal regulation merchants are required to retain the original copies of charge slips for 2 years. The slips should be in a secure location with limited access for a brief time (as defined by the department's business practices) and then placed in storage for the rest of the 2 year period. Immediately following the 2 year period, all records must be destroyed.
- **Changes:** Before making any changes to your account administrator and business practices please contact Treasury Services. Any changes to your website must be tested to ensure it is in compliance with PCI data security standards. Your change control process should include the same requirements for testing as the initial credit card authorization verification process.

**Transaction Monitoring**

- You should perform the following monitoring on credit card transactions
    - Review all returns and charge backs. A chargeback occurs when a cardholder disputes a charge, processing errors, authorization issues, or with fraud. Procedures for reducing charge backs can be obtained through Treasury Services. Brandeis University can lose both the dollar amount of the sale as well the related merchandise. There are various costs involved in a chargeback including additional bank fees and can be a significant loss to the university. You should monitor card-present and card-not-present transactions separately. A large number of chargebacks might indicate that your site is being used for fraudulent activities.
    - Perform daily reconciliations between what your local system is recording and the bank is posting. Treasury Services can provide online tools that will help you do this.

**Card-Not-Present Transactions**

- Use of a card swipe or point of sale terminal is not allowed. Please contact Treasury Services to transition to Virtual Terminal, a web based payment form which enables merchants to accept telephone, fax, and mail payments for all major credit cards. The functionality is the same as a stand-alone credit card processing terminal. Virtual Terminal has more advanced security as it allows for different levels of access.

- If you accept credit cards over the telephone, mail or via fax, you will need to do the following:
    - If you have a Paymentech business account for use on a website you may contact the vendor to use their virtual terminal. Please submit the application and supporting documentation to Treasury Services.
    - Contact Treasury Services with the necessary information and they will set up virtual terminal for you.

**Compliance Validation**

- Third party service providers we are using in whole or in part to accomplish on line acceptance of credit cards must provide to Brandeis a copy of their compliance certificate. Treasury Services will be responsible for maintaining a current certificate on file for Paymentech.

**Disclosure Requirements for Potential Breaches**

- If you suspect or have a known security breach, immediate action must taken to prevent further loss of cardholder data.
- Report all incidents to Treasury Services and the Chief Information Security immediately. The credit card issuers require merchants to have an incident response team to react to potential breaches of credit card data. Treasury Services will involve a credit card incident response team comprised of representatives from Treasury Services, the Chief Information Security Officer, and Office of the General Counsel. This team will assist you with the investigation. Treasury Services will be responsible for notifying our acquiring bank of any breaches. Local units will be responsible for any fines or penalties resulting from breaches of their data.

For further clarification of this policy, please contact Treasury Services at 6-4437.