BROWN UNIVERSITY

University Policy

Accepting Credit Cards to Conduct University Business

Purpose

Brown University requires all departments that are involved with credit card handling to do so in compliance with credit card industry standards, and in accordance with the procedure outlined in this document.

Scope

This policy applies to any department associated with the University that conducts business through credit card transactions or is responsible for developing and maintaining a University Website to conduct business transactions using credit cards. These policies apply to all employees, systems and networks involved with credit card handling which includes: transmission, storage, and/or processing of credit card numbers.

Authorization

Departments may accept credit cards with the prior approval of the Department Head and the Commerce Committee. See Brown University Policy for Accepting Credit Cards to Conduct University Business for details.

Policy Statement

A University department that sells goods or services may choose to accept credit cards from their customers as a payment method. Credit cards may only be accepted for goods, services, and gifts to the University. Credit cards are not accepted for tuition payments. The department should not accept credit cards unless there is a valid business need. **NOTE:** A department that sells goods and services, irrespective of the method of payment, must evaluate whether the sale requires the collection of sales tax and/or the reporting of unrelated business income (UBIT).

Policy

Acceptable Credit Cards: Brown currently has negotiated contracts and accepts Visa, MasterCard, Discover (and Discover network cards), and American Express. Departments may not negotiate their own contracts with credit card companies. For more information, contact Financial Services.

Authorized Vendors: Brown University has contracted with several vendors to assist in the engagement of credit cards activity. The authorized vendors meet the University's requirements for security compliance and centrally controlled financial settlement of credit card transactions, while at the same time acknowledging the diverse needs of the individual departments.

a. Banking Services: Brown has contracted with First Data Merchant Services (FDMS), a third party credit card payment processor to facilitate the financial authorization and settlement of all credit card transactions.

b. Internet Payment Gateway Services: Brown University has contracted with TouchNet Information Systems, Inc. to serve as the central link between a storefront and the banking services. The 'gateway' provides secure payment connectivity over the Internet between buyers, sellers, and the financial networks that move money between them. All storefronts must connect to the TouchNet Payment Gateway for processing of credit card information. TouchNet partners with software vendors to create a validated, PCI Compliant interface for payment processing. These partners meet the functional needs of University departments.
c. Storefront Services: Brown has contracted with TouchNet Information Systems, Inc. to provide Marketplace as the preferred storefront (shopping cart) option available for all e-commerce applications authorized by the University. Any other storefront services considered must be compatible with TouchNet's Payment Gateway, be SSL encryption enabled, and be able to adhere to applicable policies and procedures of the University.

NOTE: Departments engaging in credit card business must either use the authorized vendors or offer evidence to the Commerce Committee that such vendors cannot meet the business needs of the department and that an alternative vendor meets University requirements for security and for integrating transaction information into Brown's financial system. The Commerce Committee shall have the authority to decide whether or not to approve the department's request.

Credit Card Swipe Terminals: Purchase or rental of credit card terminals, including mobile applications, must be coordinated through Financial Services. All devices must meet PCI DSS standards. Financial Services personnel will provide on-site training at initial setup to authorized department. The department is responsible to ensure that only authorized staff have access to the terminal and are properly trained. Terminals must be inventoried with Financial Services and must be maintained in a secure location.

Engagement of Electronic Commerce: Departments or divisions of the University may engage in e-commerce only with the approval of the department head and the Commerce Committee. When engaging in e-commerce activities, the division or department must be able to meet the following standards:

a. Adhere to appropriate financial and accounting standards established by the University;
b. Transmit financial information electronically using a level of security that meets or exceeds common industry standards;
c. Use Brown University's authorized e-commerce vendors as described in this policy, or otherwise be approved by the Commerce Committee;
d. Satisfy security requirements defined by the University for secure connections and data management;
e. Adhere to generally accepted standards for electronic contracting;
f. Provide a link to the University's privacy statement from their site;
g. Keep abreast of University policies and procedures as they relate to e-commerce, as they may be periodically modified.

Security and Technical Standards: An individual's credit card information is confidential. Failure to maintain strict control over this information could result in unauthorized use of a credit card number, identity theft, and serious consequences for both the customer and the University.

Departments are responsible for safeguarding the confidentiality of e-commerce transactional data. All processes, procedures and technologies must follow the security standards dictated in the credit card industry's Payment Card Industry Data Security Standards (PCI DSS). Prior to implementation, third

party vendor securities, processes, and procedures will be evaluated as part of the review for new credit card merchants. Financial Services will work with each department to create and maintain a PCI-compliant environment for all systems involved in credit card processing.

Departments should adhere to Brown's e-commerce privacy guidelines and security procedures, linking directly to the guidelines/procedure at each point of sale. If a valid business reason dictates departure from privacy guidelines, departments should explicitly advise customers at the points of sale how their practice departs from University guidelines. Any such departures must be approved by the Commerce Committee.

PCI DSS Compliance: Payment Card Industry (PCI) security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. These standards are a set of mandated requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express, and JCB. The PCI Data Security Standards (PCI DSS) applies to all entities that store, process, and/or transmit cardholder data. The security controls and processes required by PCI DSS are vital to protecting cardholder account data (both electronic and paper handling), including the primary account number (PAN) printed on the front of a payment card. Merchants and any other service providers involved with payment card processing must never store sensitive authentication data after authorization. This includes sensitive data that is printed on a card, or stored on a card's magnetic stripe or chip – and personal identifications numbers entered by the cardholder. For details on PCI Compliance visit the PCI SSC website at www.pcisecuritystandards.org.

All users within the department authorized to process credit cards must have completed yearly PCI DSS training.

Financial Services will work with each Department directly to complete a yearly self-assessment questionnaire (SAQ). The SAQ is a validation tool for eligible organizations who self-assess their PCI DSS compliance. Each section of the questionnaire focuses on a specific area of security based on the PCI DSS requirements.

Settlement and Credit Card Fees: The University is charged a discount rate and other related fees for all credit card transactions. The rates may be different based on credit card type and/or transaction type. Note: Cards such as rewards cards fall outside of the standard discount rate.

A 'card present' transaction is a face to face interaction when the card is swiped in the terminal to capture the credit card transmittal data. The cardholder will be present to sign the sales receipt.

A 'card not present' transaction occurs when the credit card data is obtained by mail, telephone or fax and is manually keyed by an authorized operator of the credit card terminal. These transactions may be subject to additional fees.

Fees for each department's merchant account will be posted to the general ledger account designated on a monthly basis.

Each department is responsible to reconcile sales transactions to their general ledger.

Training and Guidance: All personnel who utilize or support the processing of credit cards must have completed "Protecting Brown's Information" security training and Payment Card Industry Data Security Standards (PCI DSS) training prior to receiving access. PCI DSS training is required on an annual basis. Training and guidance in the use of TouchNet services will be provided by Financial Services for those who are authorized access.

Reporting a Breach: In the event of a breach or suspected breach of security, the Department must immediately notify Financial Services at commerce@brown.edu and 401-863-2531. See procedural details in Brown University Credit Card Procedures.

Non-Compliance: Non-compliance with PCI DSS regulations may have severe consequences to the University. In the event of a data compromise, the University may incur large fines and/or be subject to a forensic examination. If a security breach occurs, the University is required to notify all customers whose data was compromised and pay restitution. In the event of a breach, the University may be suspended from processing until required remediation is met.

Failure to meet the requirements outlined in this policy will result in suspension of the physical, and if applicable, electronic payment capability with credit cards for the affected Department(s). Additionally, if applicable, any fines and assessments which may have been imposed by the affected credit card company will be the responsibility of the impacted Department.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges according to University Policy.

Commerce Committee: The Commerce Committee is a standing committee comprised of representatives from Financial and Administrative Services, Computer and Information Services, and Internal Audit.

The Committee will perform the following functions:

a. Establish registration requirements for e-commerce approval;
b. Review for approval request for establishment of e-commerce presence;
c. Provide advice to Senior Officers on the e-commerce policy, process, vendors, dissemination/publication of e-commerce information, and e-commerce matters in general; and
d. Evaluate and monitor vendor relationships.

Contact the Commerce Committee at commerce@brown.edu.

Implementation Guidelines: Further information on the registration and approval process, and how to set up and run a swipe terminal or create a TouchNet account, are available from Financial Services. Please contact via email at commerce@brown.edu.

Policy Review: The Commerce Committee will review this policy at least annually.

Definitions:

Credit Card Processor: Brown University has contracted with First Data Merchant Services (FDMS) for credit card processing. This third party provides processing services for credit and debit card financial authorization and settlement of all card transactions.

Department: A department includes all University units including all areas of the University, student groups, affiliate and quasi-Brown groups.

Personal Identification Number (PIN): A PIN is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. PINs are most commonly used for

automated teller machines (ATMs), but are increasingly used at the point of sale for debit and credit cards.

Primary Account Number (PAN): The primary account number, or PAN, is a number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.