BROWN UNIVERSITY

University Policy
Accepting and Handling Payment Cards to Conduct University Business

Purpose

The purpose of this policy and related procedures is to ensure that all University departments that accept and process credit and debit card payments, hereafter referred to as payment cards, do so in compliance with payment card industry standards, and in accordance with the procedure outlined in this document.

This policy and University procedures are designed to be in compliance with PCI DSS and assist University departments/merchants in proactively protecting payment card information.

Scope

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

Authorization

Departments may accept payment cards with the prior approval of the Department Head and the Commerce Committee.

Authorization to Establish Payment Card Business: Complete a Payment Card Merchant Request Form online. This form will be submitted to Financial Services. If considering an e-commerce account, complete an E-Commerce Discovery Questionnaire online. The Commerce Committee will review this information and communicate with the department approval or denial and the next steps required. Any use of payment card business at Brown University must be consistent with the mission and business of the University and be in conformity with rules, policies, and procedures of the University relating to and regulating the conduct of commercial transactions by Brown University.

Any department accepting payment cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within the department for payment card transactions. This individual must be designated as the primary contact on the Payment Card Merchant Request Form.

Only departments that have established processes and appropriate controls will be approved to accept payment cards for goods and services.

Policy Statement

A University department that sells goods or services may choose to accept payment cards from their customers as a payment method. Payment cards may only be accepted for goods, services, and gifts to the University. Payment cards are not accepted for tuition payments. The department should not accept payment 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 Payment 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 payment card companies. For more information, contact Financial Services.

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

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

Payment Card Swipe Terminals: Purchase or rental of payment card terminals, including mobile applications, must be coordinated through Financial Services – only devices and locations that have been approved and tracked by Brown's Commerce Committee may be used in any way associated with payment card processing. All devices must meet PCI DSS standards. Effective July 1, 2018, all newly implemented card present devices must be PCI Council Validated Point-to Point Encrypted (P2PE) solutions. 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. Sharing or transfer of mobile swipe terminals between departments is not allowed without proper approval from Financial Services. It is the department's responsibility to coordinate efforts with Financial Services to ensure that swipe terminals are updated with the most recent software version to reduce processing errors.

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 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 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. Follow University PCI Network and Security Policies;
g. Provide a link to the University's privacy statement from their commerce site;
h. 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 payment card information is confidential. Failure to maintain strict control over this information could result in unauthorized use of a payment card number, identity theft, and serious consequences for both the customer and the University.

Departments are responsible for safeguarding the confidentiality of commerce transactional data. All processes, procedures and technologies must follow the security standards dictated in the payment 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 payment card merchants. Financial Services will work with each department to create and maintain a PCI-compliant environment for all systems involved in payment 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 must explicitly advise customers at the points of sale how their practice departs from University guidelines. Any such departures must be approved in advance by the Commerce Committee.

Standards for Business Processes, Paper and Electronic Processing: All departments must comply with these standards, based on PCI DSS, regardless of what method (i.e. swipe terminal, online processing, paper acceptance, etc.) is used for processing cards. It is the department's responsibility to develop departmental procedures and ensure that all staff are trained and apprised of University policy and procedures for handling cardholder data in accordance with industry standards. These include:

a. Never store the following payment card data:
    i. Full contents from a magnetic stripe
    ii. CAV2/CVC2/CVV2/CID
    iii. Personal Identification Number (PIN)
b. Paper documents containing credit card information should be securely collected, processed immediately, and then destroyed via proper authorized method (see item h below).
c. Keep storage of cardholder data to a minimum. Mask the primary account number (PAN) showing only the last four digits wherever it is stored.

d. The University does not accept or send cardholder data via insecure communication methods, i.e. e-mail, chat, instant messaging, text, etc. The payment received via insecure communication will not be processed and will be permanently deleted.

e. Restrict physical access to cardholder data when accepting payments via mail, fax, or phone.

f. Limit access of cardholder data only to those with a business need. Physically restrict payment card processing areas to those individuals with authority to be there. Maintain a list of those with access to payment card data.

g. Develop departmental procedures that capture internal controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected, in example - printed out or left on someone's desk. The University strictly prohibits the use of removable storage media (USB/CD/DVD/Floppy Drives) on all windows-based PCI endpoints as dictated in the University Information Security Policy.

i. Any identified security issues should be documented and communicated to University Financial Services. Media containing sensitive cardholder information should be easily identified so that the department has a method to protect the data.

ii. Distribution of media / cardholder data is strictly prohibited to internal and/or external users without prior written consent from Financial Services. A firm process is required to ensure media/data movement is authorized and tracked. Financial Services will evaluate the business need to transmit cardholder data and either approve or reject the request. Departmental policies and procedures should clearly address the impact of sharing cardholder data without proper approval. All media sent outside of the facility should be logged and tracked.

h. Destroy cardholder data (CHD) properly. CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices and payment card swipe terminals. Cross-shred, incinerate, or pulp paper documentation so that cardholder data cannot be reconstructed. Paper documentation may also be disposed of using one of the University's approved shredding services. Visit the Purchasing Department's Website for details. Disposal or repurposing of all electronic media should be done in compliance with Brown's Electronic Equipment Disposition Policy.

i. Assign access privileges based on job classifications and responsibilities. Separate duties to ensure proper controls (i.e. the individual responsible for card processing via swipe terminals should not be the individual responsible for reconciliation). Review at least quarterly all data access controls and make changes as appropriate.

j. Notify Financial Services of any significant changes to card processing environment (i.e. server changes, relocation or restructure, etc).

k. Processing transactions via WiFi is generally not allowed. Review and approval of this method must be approved in advance by Brown's Financial Services and CIS Network teams.

PCI DSS Compliance: Payment Card Industry Data Security Standards (PCI DSS) 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 payment 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 payment cards must have completed annual PCI DSS training. Part of the annual training includes acknowledgement of the University Policy on Accepting and Handling Payment Cards to Conduct University Business. Potential personnel should be vetted prior to hire to minimize the risk of attacks from internal sources. Employment eligibility verifications should be performed in accordance with the University Employment Eligibility Verifications Policy.

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 Payment Card Fees: Swipe terminals must be settled no less than daily. It may be prudent, given the level of activity, to settle batches on a more frequent basis. A transaction will not be processed and charged to the cardholder until the batch is settled. The department must maintain (for seven years) all signed receipts and credit card swipe terminal Batch Total Settlement Reports.

TouchNet Marketplace (uStore and uPay) settles each night automatically. At 12:00 EST (11:00 CST for TouchNet Systems, Inc.); a batch for each merchant is closed for the day's activity and sent to the credit card processor. Funds are posted to Workday based on the departments merchant account ID and worktags provided to Financial Services.

Departments will establish and maintain appropriate segregation of duties between credit card processing, processing of refunds, and the reconciliation of credit card transactions. Each department is responsible to reconcile sales transactions to their general ledger no less than monthly. The department should be prepared to provide documentation of reconciliation in an audit.

The University is charged a discount rate and other related fees for all payment card transactions. The rates may be different based on payment card type and/or transaction type. Note: Cards such as rewards cards fall outside of the standard discount rate. Fees for each department's merchant account will be posted to the general ledger account designated on a monthly basis.

Cardholder Disputes and Chargebacks: The bank will notify the University of a disputed charge. Financial Services is the primary contact. All disputes are reviewed by Financial Services, and then the department is contacted to receive written authorization/documentation of the transaction. Failure to respond to these requests will result in a chargeback to the department's account. Prompt attention to these matters is a priority. It is the department's responsibility to develop appropriate internal controls to mitigate risks related to chargebacks.

Training, Access and Guidance: Access to Brown University's cardholder system components and data is limited to only those individuals whose jobs require such access. Access to cardholder systems, including swipe terminals and TouchNet, will be restricted based on job responsibilities. All personnel

who utilize or support the processing of payment 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 an Incident: In the event of a security incident or suspected breach of security, the department must immediately notify Financial Services. In addition to the University Incident Response Plan, the Payment Card Security Incident Response Plan addresses PCI DSS requirements for payment card security incident response at Brown University. In the event of a suspected or confirmed incident, follow the instructions within the Incident Response Plans.

Compliance and Annual Certification: All University departments accepting payment cards for financial transactions must be compliant with PCI-DSS Security Standards. Financial Services will perform reviews of each department merchant. Non-compliance with PCI DSS 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 may result in suspension of the physical, and if applicable, electronic payment capability with payment cards for the affected Department(s). Additionally, if applicable, any fines and assessments which may have been imposed by the affected payment 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, Finance Division/Treasury, 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 e-commerce policy, process, vendors, dissemination/publication of e-commerce information, and e-commerce matters in general; and
d. Evaluate and exercise due diligence of vendor relationships, including monitoring service providers' PCI DSS compliance on an annual basis.

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.

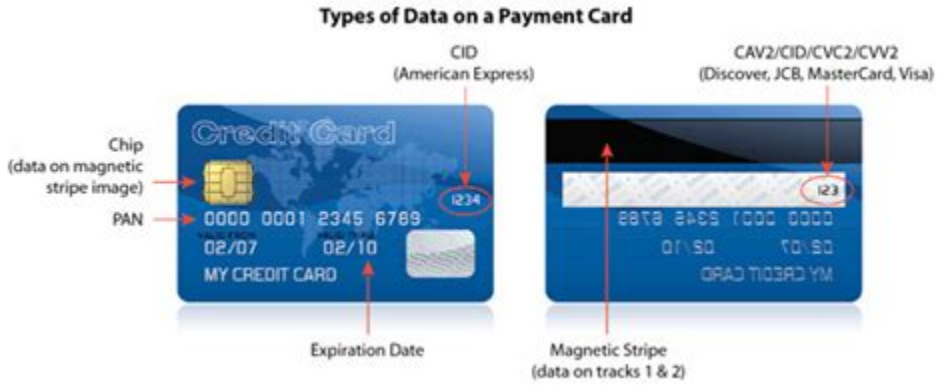
Policy Review: The Commerce Committee will review this policy at least annually.

Definitions:

Authentication: Process of verifying identity of an individual, device, or process.

Cardholder Data: Cardholder data (CHD) refers to any information printed, processed, transmitted or stored in any form on a payment card. Departments accepting payment cards are expected to protect cardholder data and to prevent its unauthorized use – whether the data is printed, stored locally, or distributed to an internal or external source.

CAV2/CVC2/CVV2/CID: The Card Security Code is the 3-digit security code on the *back* of the credit or debit card. Visa: CVV, MasterCard: CVC2JCB: CAV2. For American Express cards the CID or 4DBC and is 4-digits on the *front* of the AMEX card:



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

Media: Sources containing cardholder data including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes

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

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 payment cards.

Primary Account Number (PAN): The primary account number, or PAN, is a number code of 14 or 16 digits embossed on the front of the payment 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.