BROWN UNIVERSITY

University Policy

Accepting and Handling Payment Cards to Conduct University Business

Table of Contents

Purpose

This policy defines the responsibility and accountability for all steps related to processing credit and debit card payments, hereafter referred to as payment cards, including the transmission, storage and processing of cardholder data.

Brown University, hereafter referred to as "the University", will undertake steps to ensure the University is compliant with the Payment Card Industry Data Security Standards (PCI DSS) by developing and implementing a service offering that includes the technology, training, policies, procedures, and support to achieve compliance and mitigate risks, as outlined in the PCI DSS Policy and Standards.

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 (full-time, part-time, student and temporary), systems and networks involved with payment card handling which includes: transmission, storage, and/or processing of payment cards.

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 as payment 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). Further information can be provided by the Tax Manager in the Controller's Office.

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 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 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: Use, purchase or rental of payment 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 the authorized department. The department is responsible to ensure that only authorized staff have access to the terminal and are properly trained.

Terminal Security: Devices that capture payment card data via direct physical interaction with the card, such as swipe readers, must be protected. This protection must include preventing the devices from being tampered with or substituted. Terminals will be inventoried with Financial Services and must be maintained in a secure location by the department. The department must maintain the details on the make, model and serial number of all devices under their merchant ID within their written policies and procedures. The devices must be inspected periodically. This inspection includes checking the surfaces for tampering or substitution. (PCI Requirement 9.9 – 9.9.3).

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 University financial and accounting policies and procedures;
b. Transmit financial information electronically using a level of security that meets or exceeds University 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 University 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 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 must 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 any 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 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 ensure that all staff are trained and apprised of the proper policy and procedures for handling cardholder data.

a. Keep storage of cardholder data to a minimum. This means only information necessary for processing should be retained. The maximum storage time for this information is six-months. Mask the primary account number (PAN) showing only the last four digits wherever it is stored.
b. Never store the following payment card data: i. Full contents from a magnetic stripe
ii. CAV2/CVC2/CVV2/CID
iii. Personal Identification Number (PIN)
c. When absolutely necessary that cardholder information is to be collected on a form, locate that information on the bottom so that it may be cut off and destroyed properly.
d. Develop a departmental disposal policy (based on requirements in section e below) and adhere to it. Verify on a regular basis that the proper procedures are being followed.
e. 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.

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. 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.

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 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.

All users within the department authorized to process payment cards must complete 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.

An annual self-assessment questionnaire (SAQ) must be completed by each campus merchant. 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. Financial Services will work with each Department directly to complete the SAQ.

For details on PCI Compliance visit the PCI SSC website at www.pcisecuritystandards.org.

Settlement and Payment Card Fees: 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.

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

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

Fees (e.g., credit and debit card fees) for each department's merchant account will be posted to the general ledger account designated on a monthly basis.

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 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. The Cashier's Office will post funds to the departments designated general ledger account when funds are received from the bank. Activity may take up to 10 business days to settle through the various processors and banks.

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.

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.

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. Departments authorized to accept payment cards must have written policies and procedures. Security polices and operational procedures for restricting access to cardholder data must be documented, in use, and known to and signed by all affected parties. 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. Follow the instructions below to document the issue:

a. Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation the date and time, action taken, location, person performing action, person performing documentation, and all personnel involved.

b. Contact Brown University Information Security Group (ISG) for proper direction of preservation of electronic data.

c. Notify Financial Services and the Dean/Director/Department Head of the unit experiencing the breach. No one should communicate with anyone outside of their supervisor(s), ISG, or Financial Services about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated with the Executive VP for Finance & Administration.

d. Prevent any further access to or alteration of the compromised system. Disconnect from the network and wait to hear from a security consultant.

e. If a suspected or confirmed intrusion/breach of a system has occurred, the Director of Financial Services, along with the commerce committee, will alert the merchant bank, credit card processor, Internal Audit, Office of General Counsel, and other respective authorities as required.

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 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, Computer and Information Services, and Internal Audit.

The Committee will perform the following functions:

a. Establish registration requirements for commerce approval;
b. Review for approval requests for establishment of commerce presence;
c. Monitor, support, and follow-up with merchant areas to ensure any and all corrective actions are applied in cases of non-compliance;
d. Provide advice to Senior Officers on the commerce policy, process, vendors, dissemination/publication of commerce information, and e-commerce matters in general;
e. Assist the University in compliance with PCI DSS and reduce the scope of items that will need to be compliant; and
f. 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:

CAV2/CVC2/CVV2/CID: The Card Security Code is the 3-digit security code on *the back* of your credit or debit card. Visa calls it CVV2, MasterCard calls it CVC2. JCB call it the CAV2:

For American Express cards it is called 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, and affiliate and quasi-Brown groups.

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 a bank or 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.