BROWN UNIVERSITY

University Procedures

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, University Policy and in accordance with the procedures outlined in this document. Each merchant/department must also have written procedures in accordance with PCI DSS regulations. See Financial Services template for guidance.

Procedures

Authorization to Establish Credit Card Business: Complete a Credit 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 credit 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 credit cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within the department for credit card transactions. This individual must be designated as the primary contact on the Credit Card Merchant Request Form.

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 credit 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 credit 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 credit card processing areas to those individuals with authority to be there. Maintain a list of those with access to credit 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.

Settlement and Credit Card Fees:

a. 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.

   A CC Transmittal Form is to be completed for each batch and submitted to the Cashier's Office identifying the batch total and general ledger account distribution. A copy of the terminal Batch Total Settle Report which is printed from the credit card swipe terminal must be attached to each CC Transmittal Form. Forms should be completed electronically and then printed for submittal to the Cashier's Office, Campus Box 1911, on a daily basis. The credit for batch activity will appear on the department's designated general ledger within approximately 10 business days.

b. 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 will take approximately 10 business days to settle through the various processor and banks and post.

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

It is the responsibility of the department to ensure the general ledger reconciles to the original credit card activity 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 and Guidance: All users within the department authorized to process credit cards must have completed "Protecting Brown's Information" security training and Payment Card Industry Data Security Standards (PCI DSS) training. 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.
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.

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.

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, 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.