Credit Card Merchant Identification/ID (MID) Setup and Maintenance Policy

Effective Date: August 31, 2009

Policy Statement
This policy sets requirements for the establishment and maintenance of a Merchant Identification/ID (MID) for the acceptance of credit card payments for the sale of approved goods, services, information or gifts.

Reasons for the Policy
The purpose of this policy is to document control procedures and requirements prior to the acceptance of credit card payments to prevent loss of confidential data and ensure compliance with University Policies and industry security standards and regulations.

Primary Guidance to Which This Policy Responds
E-Commerce: Electronic Protection of Credit Card Holder Information Policy and to the Payment Card Industry Data Security Standard (PCI DSS).

Responsible University Office
The Office of the Treasurer

Revision History
This policy was established in August 2009.

Who is Governed by this Policy
This policy applies to individuals, schools, departments, centers, institutes, and programs ("University Departments") that sell goods, services, information, or gifts and accept credit cards as a form of payment.

Who Should Know This Policy
All senior business officers, department administrators and financial and administrative staff whose business accepts credit cards as a form of payment should know this policy.

Exclusions and Special Situations
None

Policy Text
A University Department accepting credit card payments for the sale of goods, services, information or gifts is a merchant. In order to accept credit card payments, the merchant must obtain a MID which is a unique number that identifies the merchant for reference and billing purposes.

There are four methods for processing merchant transactions that require a MID:

1. Mail order (ex. Lockbox, card not present);
2. Telephone Order (card not present); } together MO/TO
3. Retail face to face (Point of Sale (POS), card present);
4. E-commerce (internet/computer network, card not present).

Regardless of the method chosen, credit card information and transaction receipts must be captured and stored in a secure manner.

E-commerce transactions

University Departments must adhere to the criteria in the *E-Commerce: Electronic Protection of Credit Card Holder Information Policy and its Appendices* which states that University Departments must not capture, store or transmit credit card information of on CU servers or network.

MO/TO and Retail transactions

Credit card information should be captured securely. The Card Verification ID (CVV/CID/CVN) printed on the signature panel of the card must not be written or stored at any time.

Data Retention

Transaction receipts (paper or electronic records of the purchase) must be retained for a minimum of two (2) years (or such period as the Card Rules or the Laws may require or your specific department guidelines mandate) to dispute a chargeback from a cardholder if necessary. The receipts should be stored in a safe, secure area and organized in chronological order by transaction date and kept locked on site for 2-3 months and then placed in archives for the remainder of the two years. They should be securely destroyed directly from archives.

Responsibilities

A Columbia University (CU) MID will only be issued to University Departments that comply with this policy, all related policies and acknowledge technical and operational responsibilities associated with credit card acceptance.

University Departments may ONLY obtain a CU MID by contacting the Office of the Treasurer creditcards@columbia.edu and outlining specific requirements.

All University Department merchants must comply with University policies to safeguard credit card and other personally identifiable or sensitive information.

UNIVERSITY DEPARTMENTS

Initial Setup Requirements

- Determine the need for a merchant account. Consider the following:
  1. Purpose of the account
  2. Anticipated dollar and transaction volume
  3. Average transaction amount

4. Frequency of transactions (year-round, seasonal, limited)
5. Type of processing required (MO/TO, POS, e-commerce).
6. Transaction and service fees associated with processing credit cards as well as setup and monthly fees for online merchant accounts.

- Contact the Office of the Treasurer creditcards@columbia.edu for a MID.
- Complete and submit the authorized Acknowledgement and Approval Form (*Appendix A*).
    - Request new or update to an existing MID approved by the Senior Business Officer.
    - Acknowledge review and compliance with CU policies and procedures.
- Complete and submit required forms provided by the Treasurer's office, including New Merchant Account Application and FAS account numbers for revenue and expenses.
- Request MID Users be setup to process and view credit card transactions.
    - Acknowledge understanding of responsibilities of MID User access rights.
- Ensure that cardholder data is treated as confidential and access is restricted to a need to know basis.
- Ensure functional segregation of duties between employees who process credit card transactions and chargebacks with those who balance and reconcile the transactions.
- Ensure departmental personnel are trained not only on CU policies and procedures but also local departmental procedures related to authorization of transactions, segregation of duties, reconciliations, chargebacks, record retention, data access, training, and physical security.
- *If processing credit card data via e-commerce*,
    - Select an approved third party e-commerce vendor (*Appendix B*).
    - If an approved vendor cannot support the business objective, a new vendor may be recommended, but must first be reviewed and approved by Procurement Services.
    - Provide the URL (web link) of your privacy and refund policy disclosures.
    - Provide the URL to the website's checkout page that redirects the customer to an approved third party PCI DSS compliant vendor.
    - Coordinate a CU e-commerce technical security review. Refer to the *E-Commerce: Electronic Protection of Credit Card Holder Information Policy and its Appendices* for requirements which will include compliance with PCI DSS technical requirements and related CU policies.

Ongoing Maintenance Requirements

- Reconcile credit card receipts total (from POS device or online terminal) to credit card cash deposits total (cash deposited into CU bank account) daily. This will validate that transactions are correct, that there has not been a keying error and/or any malicious activity.
- Reconcile account activity monthly. It is important to record sales revenue and expense timely and accurately. It is incumbent on the University Departments to reconcile FAS accounts to ensure that revenue and related expenses are posted accurately. Any discrepancies must be addressed timely.
- Contact the Office of the Treasurer at creditcards@columbia.edu to update a MID. Reasons to update a MID include the addition of new website associated with an existing MID or a change to a website associated with a current MID (complete and submit the authorized Acknowledgement and Approval Form (*Appendix A*)), a change in MID Users or contact

person, a change in FAS account numbers, or a change in business purpose for which the MID was established.

- Contact the Office of the Treasurer at creditcards@columbia.edu to close a MID. Reasons to close a MID include unauthorized activity, no activity/dormant or a change in business purpose for which the MID was established.
- Certify compliance with PCI DSS technical and operational requirements as requested by the Office of the Treasurer on an annual basis**.**

OFFICE OF THE TREASURER

Initial Setup Requirements

- Obtain authorized Acknowledgement and Approval Form (*Appendix A*) to verify approval by the Senior Business Officer of the MID and acknowledgement of adherence to CU Policies.
- Process required forms and establish MIDs with only a*pproved Cr*edit Card Payment Gateways and Processors that are contractually obligated to comply with PCI DSS standards. Third party gateways are the infrastructure that allows a merchant to accept credit cards. Third party processors handle many aspects of the transaction such as authorization, billing, reporting and settlement. Some third party vendors provide both functions.
- Confirm FAS account numbers for credit card revenue and expenses.
- Setup MID Users which will be entitled to process and view credit card payments.
    - Receive email acknowledgement from each MID User confirming their understanding of the responsibilities of their access rights.
- If the University Department processes credit card transactions via e-commerce:
    - Confirm that a CU e-commerce technical security review was completed.
    - Confirm URL for privacy and refund policy disclosures.
- Update University data files of authorized MIDs.

Ongoing Maintenance Requirements

- Review as necessary University MIDs and transactions for compliance with University policies and industry standards and regulations.
- Recommend MIDs for update or closure. Reasons include changes in the original purpose of the MID, addition of new websites associated with the MID, unauthorized activity, no activity/dormant, the FAS accounts are not reconciled timely or there are significant unresolved open items, and violation of University policies or industry standards and regulations.
- Review MID Users access for activity and validity of accounts.
- Coordinate University Department's certification of compliance with PCI DSS technical and CU operational requirements on an annual basis**.**

Consequences for Non-Compliance with this Policy

Failure to comply with this policy can result in the termination of merchant services privileges and individuals may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance to Columbia University policy and procedures.

Additionally, intentional negligence that results in breach of confidentiality of personal information that is protected by law, acts, or regulations, can also result in criminal prosecution. Penalties for non-compliance of PCI DSS requirements include fines up to $500,000 per incident if data is compromised.

Respond to a Credit Card Security Breach

If you have knowledge of or suspect a security breach of credit card data, report the incident to:

1. Office of the Treasurer - creditcards@columbia.edu or Associate Treasurer-Cash Management and Operations 212-854-9685.
2. CUIT Security - security@columbia.edu or 212-854-1919.

You must also take immediate steps to preserve all business records, logs and electronic evidence.

Contacts

For questions or comments

Office of the Treasurer
Email: creditcards@columbia.edu
Telephone: 212-851-0417

Cross References to Related Policies

The University Administrative Policy Library, CU Information Technology section:

http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html

See the "E-Commerce: Electronic Protection of Credit Card Holder Information Policy" and "Electronic Information Resources Security policy" for related information.

For more information on PCI, refer to https://www.pcisecuritystandards.org/. All processes for accepting credit cards must comply with Payment Card Industry Data Security Standards (PCI DSS). The standards globally govern all merchants and organizations that store, process or transmit credit card data.