Accepting Credit Cards to Conduct University Business

POLICY STATEMENT

Cornell University requires all units that accept credit cards to do so only in compliance with credit card industry standards, and in accordance with the procedures outlined in this document.

REASON FOR POLICY

The university supports the acceptance of credit cards as payment for goods and services to improve customer service, bring efficiencies to Cornell’s cash collection process, and increase the sales volume of certain types of transactions. In addition, the university must support unit compliance with industry standards governing credit card transaction processing, specifically Payment Card Industry Data Security Standards (PCI DSS).

ENTITIES AFFECTED BY THIS POLICY

– All units of the university

WHO SHOULD READ THIS POLICY

– Any unit that conducts university business using credit cards
– Any unit responsible for developing and maintaining a university website to conduct business transactions using credit cards
– Any unit utilizing third-party software to process credit card transactions
– Unit managers

WEB ADDRESS FOR THIS POLICY

– This policy: www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/finance/creditcards.cfm
– University Policy Office: www.policy.cornell.edu
POLICY 3.17

Accepting Credit Cards to Conduct University Business

CONTENTS

Policy Statement .................................................................................. 1
Reason for Policy .................................................................................. 1
Entities Affected by this Policy ............................................................. 1
Who Should Read this Policy ............................................................... 1
Web Site Address for this Policy ........................................................... 1
Related Resources ................................................................................ 4
Contacts ................................................................................................ 5
Contacts, Weill Cornell Campus Units ............................................... 6
Definitions ............................................................................................. 7
Responsibilities, Ithaca Campus Units ............................................... 9
Responsibilities, Weill Cornell Campus Units .................................. 11
Principles .............................................................................................. 12
   Introduction ...................................................................................... 12
   PCI DSS Compliance ...................................................................... 12
   Acceptable Credit Cards ................................................................. 12
   Credit Card Fees ............................................................................. 13
   Security and Technical Standards .................................................. 13
   Standards for Business Processes, Paper and Electronic Processing ..... 14
   Prohibited Credit Card Activities .................................................. 16
   Methods of Processing Transactions ............................................ 16
   Non-Compliance .............................................................................. 18
   Procedures, Ithaca Campus Units ................................................. 19
      Requirements for Any Individuals Involved with Credit Card Processing 19
      Credit Card Information and E-mail ........................................... 19
      Establishing a Merchant Account .............................................. 19
      Decommissioning of Computer Systems and Electronic Media Devices 19
      Protecting Sensitive Information ............................................... 20
      Third-Party Outsourcing ............................................................. 20
      Accepting University Procurement Cards ................................ 20
      Transaction Reconciliation ......................................................... 20
      Refunds ....................................................................................... 21
      Handling a Customer Disputed Charge ................................... 21
      Posting and Reconciling Transactions .................................... 21
      Canceling a Merchant ID .............................................................. 21
      Reporting a Breach ..................................................................... 22
   Procedures, Weill Cornell Campus Units ..................................... 23
      PCI DSS Compliance Certification ............................................. 23
      Credit Card Information and E-mail ........................................... 23
      Establishing a Merchant Account .............................................. 23
      Decommissioning of Computer Systems and Electronic Media Devices 23
      Protecting Sensitive Information .............................................. 23
## CONTENTS, continued

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Outsourcing</td>
<td>24</td>
</tr>
<tr>
<td>Transaction Reconciliation</td>
<td>24</td>
</tr>
<tr>
<td>Refunds</td>
<td>24</td>
</tr>
<tr>
<td>Handling a Customer Disputed Charge</td>
<td>24</td>
</tr>
<tr>
<td>Posting and Reconciling Transactions</td>
<td>25</td>
</tr>
<tr>
<td>Canceling a Merchant ID</td>
<td>25</td>
</tr>
<tr>
<td>Reporting a Breach</td>
<td>25</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>
POLICY 3.17

Accepting Credit Cards to Conduct University Business

RELATED RESOURCES

University Policies and Documents Applicable to All Units of the University

University Policy 3.1, Accepting University Gifts
University Policy 3.6, Financial Irregularities
University Policy 3.20, Cost Transfers on Sponsored Agreements
University Policy 3.22, Accepting Cash and Checks
University Policy 3.25, Procurement of Goods and Services
University Policy 4.2, Transaction Authority and Payment Approval
University Policy 4.7, Retention of University Records
University Policy 5.1, Responsible Use of Information Technology Resources
University Policy 5.10, Information Security

University Policies and Documents Applicable to Only Ithaca Campus Units

University Policy 3.2, University Travel
University Policy 4.3, Sales Activities on Campus
University Policy 4.12, Data Stewardship and Custodianship
University Policy 5.3, Use of Escrowed Encryption Keys
University Policy 5.4.1, Security of Information Technology Resources
University Policy 5.4.2, Reporting Electronic Security Incidents

Policies and Documents Applicable to Only Weill Cornell Campus Units

University Policy 3.2.1, Travel
University Policy 3.2.2, Travel, WCMC-Qatar
WCMC Policy 11.1, Responsible Use of Information Technology Resources
WCMC Policy 11.3, Data Classification
WCMC Policy 11.6, Laptop Encryption
WCMC Policy 12.2, Physical Security

External Documentation

PCI Security Standards Council
PCI Security Standards Council List of Validated Payment Applications

University Forms and Systems

<table>
<thead>
<tr>
<th>Ithaca Campus Units</th>
<th>Weill Cornell Campus Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application for Credit Card Merchant Accounts</td>
<td>myCertificates (Security Awareness Training)</td>
</tr>
<tr>
<td>Cornell University DropBox</td>
<td>PCI DSS Self-Assessment Questionnaire</td>
</tr>
<tr>
<td>CU Learn (Security Awareness Training)</td>
<td>WCMC File Transfer Service</td>
</tr>
<tr>
<td>Lockbox Credit Card Refund Form</td>
<td>Unit Training Attestation</td>
</tr>
<tr>
<td>PCI DSS Self-Assessment Questionnaire</td>
<td></td>
</tr>
<tr>
<td>Unit Training Attestation</td>
<td></td>
</tr>
</tbody>
</table>
POLICY 3.17

Accepting Credit Cards to Conduct University Business

CONTACTS

Direct any general questions about this policy to your college or unit administrative office. If you have questions about specific issues, contact the following offices.

<table>
<thead>
<tr>
<th>Contacts, Ithaca Campus Units</th>
<th>Contact</th>
<th>Telephone</th>
<th>E-mail/Web Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Contact</td>
<td>Telephone</td>
<td>E-mail/Web Address</td>
</tr>
<tr>
<td>Policy Clarification</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>Breach, Reporting a</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td></td>
<td>Network Operations Center (NOC)/IT Security Office</td>
<td>(607) 255-9900</td>
<td><a href="mailto:security@cornell.edu">security@cornell.edu</a> <a href="http://www.cit.cornell.edu/security/depth/incident/report.cfm">www.cit.cornell.edu/security/depth/incident/report.cfm</a></td>
</tr>
<tr>
<td>Contracts with Third-Party Providers</td>
<td>Cornell Procurement Services</td>
<td>(607) 255-3804</td>
<td><a href="mailto:procurement@cornell.edu">procurement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/procurement/">www.dfa.cornell.edu/procurement/</a></td>
</tr>
<tr>
<td>Departmental Journal Credit</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>Disputed Charges and Chargebacks</td>
<td>Elavon</td>
<td>(800) 725-1245</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td></td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>Equipment Problems, Merchant Account, Merchant Discount</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>PCI Compliance, Business Practices</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a> <a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>PCI Compliance, Technical or Security</td>
<td>Network Operations Center (NOC)/IT Security Office</td>
<td>(607) 255-9900</td>
<td><a href="mailto:security@cornell.edu">security@cornell.edu</a> <a href="http://www.cit.cornell.edu/security/">www.cit.cornell.edu/security/</a></td>
</tr>
<tr>
<td>Sales Tax and Other Tax Issues</td>
<td>Tax Compliance</td>
<td>(607) 255-5195</td>
<td><a href="mailto:uco-tax@cornell.edu">uco-tax@cornell.edu</a> <a href="http://www.dfa.cornell.edu/tax/">www.dfa.cornell.edu/tax/</a></td>
</tr>
</tbody>
</table>
### POLICY 3.17

**Accepting Credit Cards to Conduct University Business**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>E-mail/Web Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Clarification</td>
<td>Cash Management</td>
<td>(607) 254-1590</td>
<td><a href="mailto:cashmanagement@cornell.edu">cashmanagement@cornell.edu</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/">www.dfa.cornell.edu/treasurer/cashoperations/cashmanagement/</a></td>
</tr>
<tr>
<td>Breach, Reporting a</td>
<td>Privacy Office</td>
<td>(212) 746-1121</td>
<td><a href="mailto:privacy@med.cornell.edu">privacy@med.cornell.edu</a></td>
</tr>
<tr>
<td></td>
<td>Information Security</td>
<td>(212) 746-7457</td>
<td><a href="mailto:support@med.cornell.edu">support@med.cornell.edu</a></td>
</tr>
<tr>
<td>Contracts with Third-Party Providers</td>
<td>Office of University Counsel</td>
<td>(212) 746-0463</td>
<td>James Kahn</td>
</tr>
<tr>
<td>PCI Compliance, Business Practices</td>
<td>Privacy Office</td>
<td>(212) 746-1121</td>
<td><a href="mailto:privacy@med.cornell.edu">privacy@med.cornell.edu</a></td>
</tr>
<tr>
<td></td>
<td>Assistant Controller, Finance</td>
<td>(646) 962-3658</td>
<td><a href="mailto:ddspears@med.cornell.edu">ddspears@med.cornell.edu</a></td>
</tr>
<tr>
<td>PCI Compliance, Technical or Security Issues</td>
<td>Information Security</td>
<td>(212) 746-7457</td>
<td><a href="mailto:support@med.cornell.edu">support@med.cornell.edu</a></td>
</tr>
<tr>
<td>Sales Tax or Unrelated Business Income Issues</td>
<td>Finance Department Compliance</td>
<td>(646) 962-3800</td>
<td><a href="mailto:ejohnson@med.cornell.edu">ejohnson@med.cornell.edu</a></td>
</tr>
<tr>
<td></td>
<td>Office</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**DEFINITIONS**

These definitions apply to terms as they are used in this policy.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquirer</strong></td>
<td>The bank or financial institution that accepts credit and or debit card payments for products or services on behalf of a merchant. The term acquirer indicates that the bank accepts or acquires transactions performed using a credit card issued by all banks within the card industry.</td>
</tr>
<tr>
<td><strong>Bank</strong></td>
<td>A financial institution that provides merchant accounts to enable a unit to accept credit card payments. Funds are deposited into an account established at this institution.</td>
</tr>
</tbody>
</table>
| **Card Verification Code or Value** | A data element on a card’s magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as the following, depending on payment card brand.  
- CAV – Card Authentication Value – JCB  
- CVC – Card Validation Code – MasterCard  
- CVV – Card Verification Value – Visa and Discover  
- CSC – Card Security Code – American Express (AMEX)  
  Also, the rightmost three-digit value printed in the signature panel area on the back of the card (for Discover, Visa, MasterCard) or the four-digit non-embossed number printed above the PAN on the face of the card (for AMEX).  
- CID – Card Identification Number – AMEX and Discover  
- CAV2 – Card Authentication Value 2 – JCB  
- CVC2 – Card Validation Code 2 – MasterCard  
- CVV2 – Card Verification Value 2 – Visa |
| **Chargeback** | The deduction of a disputed sale previously credited to a unit’s account when the unit fails to prove that the customer authorized the credit card transaction. |
| **Customer** | An individual or other entity that makes a payment to the university for goods or services. |
| **Lockbox Processing** | A method of processing credit cards at the university (see table 1, Methods of Processing Transactions, in the Procedures, Ithaca Campus Units section of this policy). |
| **Magnetic Stripe Information** | The information contained in a credit card’s magnetic stripe, including the PAN, expiration date, customer’s name, service code, and other discretionary data, such as a PIN, CVV, etc. |
| **Merchant** | A unit that accepts credit cards as a method of payment. |
| **Merchant Discount** | A percent or per-transaction fee that is deducted from the unit’s gross credit card receipts and paid to the bank. |
| **MID** | Merchant ID. An account established for a unit by a bank to credit sale amounts and debit processing fees. |
| **PAN** | Primary account number. The 16-digit account number on the front of a credit card. |
| **PCI DSS** | “Payment Card Industry Data Security Standards” – A set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a
## DEFINITIONS, continued

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS Security Awareness Training</td>
<td>An online training program, available through CU Learn for Ithaca campus units, and through myCertificates for WCMC campus units, that includes information on compliant processes (business and technical) and changes in industry standards.</td>
</tr>
<tr>
<td>PCI Security Standards Council</td>
<td>An organization for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection in the payment card industry, through education and awareness. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal identification number. A numeric password known only to the user and a system to authenticate the user to the system.</td>
</tr>
<tr>
<td>ROC</td>
<td>Report on compliance. An annual certification report issued by the PCI Security Standards Council to a third-party provider that has been validated as PCI-compliant.</td>
</tr>
<tr>
<td>Secure WebSite</td>
<td>A method of processing credit cards at the university (see table 1, Methods of Processing Transactions, in the Procedures, Ithaca Campus Units section of this policy).</td>
</tr>
<tr>
<td>Self-Assessment Questionnaire</td>
<td>One of several forms used as self-validation tools to assist merchants and service providers in evaluating their compliance with PCI DSS. For more information, contact Cash Management.</td>
</tr>
<tr>
<td>Terminal and Printer Processing</td>
<td>A method of processing credit cards at the university (see table 1, Methods of Processing Transactions, in the Procedures, Ithaca Campus Units section of this policy).</td>
</tr>
<tr>
<td>Unit</td>
<td>A college, department, program, research center, business service center, office, or other operating unit.</td>
</tr>
</tbody>
</table>
POLICY 3.17
Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, ITHACA CAMPUS UNITS

The following are the major responsibilities each party has in connection with this policy.

| Cash Management | Negotiate all contracts with credit card companies. Review requests for Merchant IDs (MIDs), and establish where appropriate. Consult with units regarding merchant accounts, merchant discounts, website security, and all other aspects of this policy. Keep current with Payment Card Industry Data Security Standards (PCI DSS) regulations and make changes to processes, as appropriate. Coordinate and account for annual PCI DSS requirements:  
  - Provide PCI security awareness training portal to units  
  - Collect, from every unit, signed and dated attestations that all appropriate individuals have completed the annual security awareness training  
    - Review unit SAQ completion status; collaboratively work with units that have an incomplete/fail status toward a successful completion of this requirement.  
  - Coordinate and review quarterly scans  
  - Confirm that units using third-party providers have submitted proper documentation  
    - Submit annually the necessary documentation to acquirer for PCI certification at the university level |
| Cornell Information Technologies (CIT) | Maintain security standards as required by this policy. Keep current with PCI DSS regulations and make changes to tools and processes, as appropriate. Consult with units on technical PCI DSS issues. Assist Cash Management in its mandatory annual training sessions. |
| Cornell Procurement Services | Consult with units regarding service contracts for third-party outsourcing of PCI-compliant credit card processing systems. When evaluating contracts on behalf of units, verify that the contract states that it will become null and void if the vendor does not maintain PCI DSS compliance. |
| Individual | Report any breaches to the Network Operations Center (NOC)/IT Security Office and Cash Management, according to the “Reporting Breaches” section of this policy. |
| Senior Finance Officer or Desigee | Attest annually to Cash Management confirming unit’s completion of the PCI security awareness training requirement annually Approve (by signing form) all applications for new MID requests |
| Unit Processing Payments | Set-up Determine if accepting credit cards will benefit the unit. Complete a merchant application form. (See Related Resources.) General Administration Maintain security standards and employ procedures as required by this policy, no matter what type of credit card processing is utilized. Provide proper unit controls regarding who may process credit card transactions (e.g., terminal passwords may be established for return |
POLICY 3.17
Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, ITHACA CAMPUS UNITS, continued

transactions).
Maintain a segregation of duties between employees who process
credit card transactions, those who reconcile daily batches, and those
who post to the general ledger.
Charge sales tax where appropriate.

Point of Sale
Get an authorization from the bank for every transaction.
Validate that the signature on the card reasonably matches the
signature of the purchaser.
Accept credit cards only for sales that are not prohibited (see the
Prohibited Credit Card Activities segment of this document).
Complete an annual PCI self-assessment questionnaire, and submit it
to Cash Management. (See Related Resources.)
Ensure that anyone responsible for and/or involved with credit card
processing (sales, reconciliation, management of these individuals,
technical support) attests to having taken the annual PCI DSS
Security Awareness Training, and being fully trained and apprised of
unit and university policies and procedures for handling credit card
transactions. Submit to Cash Management a signed and dated
attestation that this requirement was met.

After the Transaction
Balance and transmit transactions to the bank daily, if using a
terminal. Complete and submit an electronic journal as part of the
batch closing process.
Keep copies of credit card receipts and journal/register tapes. Store
them as securely as you would any confidential information. After a
retention period of six months, destroy them.
Balance the monthly credit card statement with the general ledger
within 30 calendar days of the receipt of the statement.
Respond to all disputed charges, in writing, within two business days
of the receipt of the notice.
Process refunds according to this policy.
Reconcile internal sales records to the Accounting Data Warehouse.

When a Card is not Present (e.g., Telephone Payment or Order Form)
Obtain the expiration date for use in the authorization process.
Obtain an authorization from the bank for every transaction.
Retain a copy of the confirmation.
Destroy card number after process completion.

If Using Third-Party Outsourcing
Consult with Cornell Procurement Services before signing a service
contract.
Annually submit to Cash Management a Report on Compliance
(ROC), validating PCI DSS compliance of any third-party provider.
POLICY 3.17

Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, WEILL CORNELL CAMPUS UNITS

The following are the major responsibilities each party has in connection with this policy.

<table>
<thead>
<tr>
<th>Individual</th>
<th>Record Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep copies of credit card receipts and related documents. Store them as securely as you would any confidential information.</td>
<td></td>
</tr>
<tr>
<td>Destroy records after six months.</td>
<td></td>
</tr>
<tr>
<td>Send all supporting documents to Finance promptly.</td>
<td></td>
</tr>
<tr>
<td>Disputed Charges and Refunds</td>
<td></td>
</tr>
<tr>
<td>Respond to all disputed charges, in writing, within two business days of the receipt of the notice.</td>
<td></td>
</tr>
<tr>
<td>Process refunds according to this policy.</td>
<td></td>
</tr>
</tbody>
</table>

| Privacy Officer/Assistant Controller | Attest annually that the participating departments have completed the Payment Card Industry Data Security Standards (PCI DSS) Security Awareness Training requirement. |
| Approve all applications for new merchant ID (MID) requests. |
| Submit all documentation to the Cash Management office, Ithaca campus. |

| Unit | Submit to the Assistant Controller the annual PCI-compliance certification issued by acquirer. |
| Institute proper controls regarding who may process credit card transactions. |
| Monitor adherence to this policy. |
| Maintain a segregation of duties between employees who process credit card transactions, those who reconcile daily batches, and those who post to the general ledger. |
| Complete an annual PCI self-assessment questionnaire. (See Related Resources.) |

At Point of Sale, When a Card is Presented

Check the signature on the card and compare it to that of the person paying for the service or making the donation.

Check the expiration date on the card to make certain that the card is valid.

Process the payment and obtain a confirmation (authorization number) from the bank for every transaction.

Accept credit cards only for purchases that are not prohibited (see the Prohibited Credit Card Activities segment of this document).

Post payments in a timely manner.

At Point of Sale, When Only a Card Number is Provided (Telephone Payment)

Process the payment and obtain a confirmation (authorization number) from the bank for every transaction.

Retain a copy of the confirmation.

Post payments in a timely manner.

Destroy any physical information after processing.

When a Third Party Processes a Payment

Obtain confirmation of the payment.

Process the payments.
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES

Introduction

A university unit that sells goods or services may choose to accept credit cards from its customers as a payment option. Credit cards may only be accepted for goods, services, non-degree course registration fees, and gifts to the university (see the Prohibited Credit Card Activities segment of this document).

Overall responsibility for a unit’s credit card system rests with the unit’s senior finance officer.

◆ Caution: Your unit should not accept credit cards unless there is a valid business need. When considering accepting credit cards, contact Cash Management.

◆ Note: A unit 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. Contact Tax Compliance, (or, at the Weill Cornell Medical College (WCMC), the Finance Department Compliance Office), for additional guidance.

PCI DSS Compliance

The credit card industry has developed technical and business standards that affect the way in which credit card business is conducted, called “Payment Card Industry Data Security Standards” (PCI DSS) (www.pcisecuritystandards.org).

Cornell has developed PCI-compliant procedures for every method of payment processing at Cornell. Every entity engaged in processing credit card transactions must comply with this structure. Prior to accepting credit cards, the unit must do the following:

- Identify the types of credit cards it will accept (see the Acceptable Credit Cards segment of this policy, which follows)
- Consult with Cash Management (at WCMC, the Assistant Controller in the Finance Department) to determine the most efficient and secure processing method that meets unit business needs within the centrally developed processing structure.

Acceptable Credit Cards

For Ithaca campus units, the university currently has contracts with and accepts Visa, MasterCard, Discover, American Express (AMEX), and Diners Club.

At Weill Cornell campus units, the university currently accepts Visa, MasterCard, Discover, and American Express.

◆ Caution: Units are prohibited from negotiating their own contracts with credit card companies. For more information, contact Cash Management (at WCMC, contact the Assistant Controller in the Finance Department).
POLICY 3.17
Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

Credit Card Fees
The university is charged a discount rate (fee) on all credit card transactions. The amount of the fee is determined by the accepting bank, the type of credit card, the number of transactions, and the method in which the card is processed.

At month end, these fees will be posted to the general ledger account that was identified by the unit when the merchant account was originally established.

◆ Exception: For Ithaca campus Merchant IDs (MIDs), AMEX may net the fee from each transaction.

Security and Technical Standards
All processes, procedures, or technologies must follow the security standards dictated in the credit card industry’s “Payment Card Industry Data Security Standards” (PCI DSS). Prior to implementation, the office of Cash Management (at WCMC, the Finance Department) and Cornell Information Technologies (CIT) (at WCMC, Information Technologies and Services (ITS)) must evaluate and approve any process, procedure, or technology used.

To help ensure the security of PCI-related data and assist with PCI compliance, units processing or storing credit cards may utilize the services offered by Cash Management in partnership with CIT (at WCMC, these services are offered by the Finance Department and ITS).

Units will work in conjunction with Cash Management and CIT (at WCMC, with the Finance Department and ITS) to create and maintain a PCI-compliant environment for any systems involved in credit card processing. This includes the creation of compliant network protocols, system configurations, and physical controls.

◆ Caution for Ithaca Campus Units: If the unit elects not to use Cash Management’s and CIT’s services and procedures, unit management must have advance approval from Cash Management and CIT for any planned system or procedure.

◆ Note for Ithaca Campus Units: To assist units in creating a compliant network infrastructure, CIT will maintain a PCI-compliant network that will satisfy many of the network-based PCI requirements. Units running systems that must be PCI-compliant will logically route those systems through this server to enable the server to enforce the necessary PCI rules upon the devices and any traffic to and from them.

To connect to the security server, each unit must purchase a small virtual private networking (VPN) device that will be configured by CIT to create a private network between it and the central security server (although units will be purchasing the devices, they will be configured and managed by CIT). This configuration will allow such private networks to be deployed anywhere on the Cornell campus or on the Internet. (Remote offices or traveling staff members can easily deploy the small VPN
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

device wherever they are.) Any system, from point-of-sale systems to desktop systems to Web servers, must reside behind these VPN devices. This architecture is subject to change based on evolving PCI DSS requirements and changes to the best practices of the technologies involved.

Standards for Business Processes, Paper and Electronic Processing

The standards that follow are adapted from the credit card industry’s “Payment Card Industry Data Security Standards” (PCI DSS). All units must comply with these standards, regardless of what method is used for processing credit cards.

In all cases, units must ensure that employees are kept fully trained and apprised of the unit’s procedures and practices for handling credit card transactions.

Storage and Access to Cardholder Data

- Keep storage of cardholder data to a minimum. This means only information necessary for business processing should be retained. In any event, do not store any cardholder data for longer than six months.
- Never store the following credit card data elements:
  - Full contents of any track from a magnetic stripe
  - CAV2/CVC2/CVV2/CID. These are the three-digit numbers from backs of the cards (see Card Verification Code or Value in the definitions)
  - PIN/PIN Block (Personal Identification Number)
- When designing any forms used for credit card sales, locate sensitive cardholder data (see above) together on the form, so that it can be easily removed from the form and shredded.
- Develop a disposal policy and adhere to it. Verify on a regular basis, at least quarterly, that this policy is functioning correctly.
- Destroy media properly:
  - Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
  - Render cardholder data on electronic media unrecoverable so that it cannot be reconstructed.
- Limit access to cardholder data to those individuals with a business need, as detailed in University Policy 4.12, Data Stewardship and Custodianship (for Weill Cornell campus units, as detailed in WCMC Policy 11.1 – Responsible Use of Information Technology Resources).
- Maintain a current list of those individuals with access to credit card data.
- Assign access privileges based on job classification and responsibilities.
POLICY 3.17
Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

- Review, at least quarterly, all data access controls confirming that there is a business need to allow access of each type.
- Mask the primary account number (PAN), showing only the last four digits, anywhere it is stored (this includes all portable devices, logs, backup media, A/P systems, etc.).
- Physically restrict any credit card processing areas to those individuals who have authority to be there.
- Store backups in a secure location, preferably off-site, and review the security of the storage facility at least annually, retaining documentation of that review.
- Identify and manage sensitive information contained on terminals, laptops, and other media devices using appropriate technology tools.

**Caution for Weill Cornell campus units:** Any system that stores credit card information must be encrypted using the ITS-managed encryption system described in WCMC Policy 11.6.

- Once taken out of production, wipe clean of old transactions any terminals, laptops, and other media devices that are not currently used for processing cardholder data.

Passwords, User ID, and System Access – Ithaca Campus Units

- Create passwords that are strong (containing numeric, alpha, and symbols, and at least eight characters long).
- Require passwords to be changed at least every 90 days, and not reused for at least 12 months.
- Immediately change vendor-supplied passwords upon initial sign-in.
- Do not share passwords.
- Assign users a unique ID before allowing them to access cardholder data.
- Immediately disable the user ID and access to the network when an employee leaves the unit.
- If a session has been idle for more than five minutes, require the user to re-enter the password to activate the terminal.
- Limit repeated access attempts by locking out the user ID after no more than four attempts.

Passwords, User ID, and System Access – Weill Cornell Campus Units

- Create passwords that are at least eight characters long that contain at least one uppercase and one lowercase character, and at least one number; do not contain your CWID; do not exactly match words in the dictionary; and has...
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

- not been used in the last year.
- Never share your password. ITS will never ask you for your password in person, over the phone, or via e-mail.
- Immediately change any vendor-supplied passwords upon initial sign-in.
- Assign users a unique ID before allowing access to cardholder data.
- Immediately disable the user ID and access to the network when an employee leaves the unit.
- If a session has been idle for more than five minutes, require the user to re-enter the password to activate the terminal.
- Limit repeated access attempts by locking out the user ID after six attempts.

Prohibited Credit Card Activities

Certain credit card activities are prohibited by credit card companies or policy. Prohibited activities include, but are not limited to the following:

- Tuition payment for a degree-granting program
  ◆Note: credit cards may be used to pay for non-degree courses
- The disbursement of cash from the university, including cash advances and amounts over a sale amount, except for travel advances on corporate credit cards (for more information, see university policies 3.2, 3.2.1, and 3.2.2, regarding university travel)
- Adjusting the price of goods or services based upon the method of payment (e.g., giving a discount to a customer for paying with cash)

◆Note for Ithaca campus units only: Credit cards must not be charged until the good or service is delivered.

Methods of Processing Transactions

There are five accepted methods for processing transactions: PC processing, terminal and printer, lockbox processing, secure website, and mobile card readers. For details on each of the methods, see table 1, Methods of Processing Transactions, which follows.

◆Caution: Any "smartphone" or other mobile device used for accepting credit card payments must be dedicated solely for the purpose of processing payments. It cannot be used to read or send e-mail, to browse online content not related to credit card processing, or to make use of any third-party applications that are not involved with credit card processing. Any such device must be fully PCI compliant, as must any workstation used to charge or update the device.
### Table 1
Methods of Processing Transactions

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Sending Transactions to the Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lockbox Processing</td>
<td>This is the required method for credit card orders received through the United States Postal Service. Customers are directed to send orders to a specific U.S. post office box. The bank removes materials each day, processes the credit card information, and credits accounts according to the units’ specific directions. The credit card material is returned to the unit, as a PDF file, on the same business day.</td>
<td>The bank is responsible for processing credit card receipts on a daily basis and crediting the unit account. The unit is required to design forms that allow the PAN, CVC2 et al., and expiration date to be removed easily for immediate shredding after processing by bank personnel.</td>
</tr>
</tbody>
</table>
| Mobile Card Reader          | Unit must contact Cash Management (or, at WCMC, the Finance Department) to order the necessary equipment for the following:  
  • One-time events (rental services available)  
  • Permanent solutions  
  ◆ Note: RedRover and RedRover Secure are not pre-approved networks.  
  ◆ Caution: Any "smartphone" or other mobile device used for accepting credit card payments must be dedicated solely for the purpose of processing payments. It cannot be used to read or send e-mail, to browse online content not related to credit card processing, or to make use of any third-party applications that are not involved with credit card processing. Any such device must be fully PCI compliant, as must any workstation used to charge or update the device. |                                                                                                                                                                                                                                                                     |
| PC Processing               | Unit must purchase required tool (contact Cash Management). The PC that is processing credit cards must…  
  • Be a stand-alone machine (no Web surfing or other activities permitted)  
  • Connect to the Ithaca Cornell or WCMC PCI DSS-compliant infrastructure | Transactions are sent automatically via the payment processing service.                                                                                                                                                                                                                             |
| Secure Website              | This is the required method for credit card orders received through the Internet.  
The unit requests a merchant ID and required Web tool from Cash Management (at WCMC, from the Finance Department).  
The unit establishes a website following the procedures outlined for university websites processing credit cards. The website must reside on the Ithaca-Cornell or ITS PCI-compliant infrastructure. |                                                                                                                                                                                                                                                                     |
| Terminal and Printer (includes cash registers) | The unit purchases an electronic terminal and printer (through Cash Management or, at WCMC, through the Finance Department), which are connected to analog telephone lines.  
The unit swipes the customer credit card to obtain authorization for the transaction. A receipt is printed, which the customer signs.  
Merchant receipts should be secured in a locked, limited access place.  
◆ Caution: If a terminal is IP-enabled, it must reside on the Ithaca-Cornell or ITS PCI-compliant network and related infrastructure. | The day’s receipts must be balanced and transmitted to the bank daily if there is one transaction or more.  
No transmittal is required if there are no transactions.  
No transmission equates to no sale. After 10 days, the sale is void. Each additional day of non-transmittal of data results in a higher discount fee charged to the unit. |
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

Non-Compliance  Non-compliance with PCI DSS regulations may have severe consequences to the university’s finances and reputation.

In the event of a data compromise, the university may incur large industry fines and/or be subject to a follow-up forensic examination, resulting in significant additional and ongoing costs. Also, the university is required, when there is a security breach, to notify all customers whose data was compromised and pay for free credit checks, replacement cards, etc.

Further, in the event of a breach, the PCI DSS Council or the credit card company has the right to suspend all university credit card processing until the required remediation(s) is met, crippling the university’s revenue collection stream.
**POLICY 3.17**

Accepting Credit Cards to Conduct University Business

### PROCEDURES, ITHACA CAMPUS UNITS

| Requirements for Any Individuals Involved with Credit Card Processing | 1. If you are responsible for or involved with credit card processing (sales, reconciliation, management of these individuals, technical support), complete the annual PCI DSS Security Awareness Training, in order to be fully trained and apprised of unit and university policies and procedures for handling credit card transactions.  
2. Submit an attestation that this requirement is met to Cash Management (see the Related Resources section of this policy), dated and signed by your unit’s senior finance officer. |
| Credit Card Information and E-mail | Do not use unsecured e-mail (such as Cornell’s Exchange server) to transmit cardholder information.  
◆ **Caution:** Instruct customers of this prohibition. Additionally, if a unit receives credit card information via unsecured e-mail, the unit must delete the e-mail, and **not process the transaction**, notifying the customer.  
◆ **Note:** Anyone transmitting sensitive electronic information may do so using Cornell University’s DropBox, at dropbox.cornell.edu. |
| Establishing a Merchant Account | To establish a merchant account, complete the “Application for Credit Card Merchant Accounts” (see the Related Resources section of this policy). For additional information, contact Cash Management at (607) 254-1590 or cashmanagement@cornell.edu.  
◆ **Caution:** A merchant account should not be established in your unit unless there is a valid business need. Forms that do not have full signature requirements will not be processed. When considering a merchant account, contact Cash Management. |
| Decommissioning of Computer Systems and Electronic Media Devices | When a computer system or media device that was used for credit card processing is taken out of production, it must be sanitized of all sensitive data. The hard drive of any computer system or any media device must be completely wiped and overwritten per instructions provided by the IT Security Office.  
At the very least, the media device must be erased and zeroed utilizing the United States Department of Defense 5220.22-M short wipe procedure. A media device can be re-commissioned only after it has been completely sanitized. If a media device will not be re-commissioned, it must be physically destroyed, through degaussing or dismantling. Contact the IT Security Office for specific instructions. |
PROCEDURES, ITHACA CAMPUS UNITS, continued

Protecting Sensitive Information

Terminals, laptops, and other media devices that contain confidential (Level 1) Information, (as defined in University Policy 5.10, Security of Electronic University Administrative Information), must be identified and monitored. Individuals must run Identity Finder, Spider, or a similar technology tool to locate confidential (Level 1) information.

Further, any individuals who regularly handle credit card information must protect that information as detailed in University Policy 5.10, Security of Electronic University Administrative Information.

Third-Party Outsourcing

Units that outsource storage, processing, or transmission of cardholder data to third-party service providers must obtain from them annually, a Report on Compliance (ROC), which is evidence of a successfully completed PCI DSS assessment. This documentation must be submitted to Cash Management.

In addition, units that are considering third-party outsourcing for credit card processing, or are renewing their current contracts, must consult with Cornell Procurement Services before signing a service contract. Procurement Services will review the contract for appropriate language, including a clause addressing continued compliance and specific terms regarding financial responsibility in the event of a breach.

◆Caution: Units are prohibited from engaging third-party service providers that are not PCI-compliant and have not provided ROCs.

◆Note: Units are responsible for transaction reconciliation and general ledger entries for third-party transactions.

Accepting University Procurement Cards

On your credit card sales deposit, code credit card sales made to non-procurement card users as external revenue, and credit card sales made to procurement card users as interdepartmental revenue. This entry into the general ledger is performed automatically by Cash Management, if an internal merchant account has been established. For more information, contact Cash Management.

◆Caution: Evaluate whether you should collect sales tax on external sales; do not charge sales tax on any interdepartmental sales. For more information, contact Tax Compliance at uco-tax@cornell.edu.

Transaction Reconciliation

Cash Management will post discount and other fees monthly; units will post daily sales transactions. Each unit is responsible to reconcile its internal sales records to the general ledger. The person(s) responsible for reconciliation should not have access to the sales processing system.
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, ITHACA CAMPUS UNITS, continued

Refunds

When an item or service is purchased using a credit card and a refund is necessary, the refund must be credited only to the same account from which the purchase was made, unless the original credit card account has been cancelled, in which case the refund may be issued to a different credit card. In addition, documentation of the original charge must be included with any refund transaction processed by the unit.

◆Caution: Under no circumstance is it permissible to issue a cash refund.

To process a refund, follow the procedure appropriate to the mode of processing.

◆Note: For issuing a refund using the lockbox method, use a “Lockbox Credit Card Refund Form” (see the Related Resources section of this document).

Handling a Customer Disputed Charge

The bank is obligated to advise the unit, in writing, of a disputed charge. The unit is responsible to provide the bank with written proof that the transaction was authorized by the customer. Failure to respond or provide a copy of a receipt signed by the customer or documentation of the shipping address will result in a chargeback to the unit’s account. All bank requests for information concerning a dispute must be answered within two business days of receipt.

Posting and Reconciling Transactions

It is important to record sales revenue accurately in the university financial records by completing the “Application for Credit Card Merchant Accounts” (see the Related Resources section of this document). Units post sale transactions directly into the Kuali Financial System (KFS) by submitting the Credit Card Receipt e-doc. Cash Management will continue to make the appropriate entries to record the monthly fees to each merchant ID (MID) based on the general ledger information provided by the unit.

A unit is expected to reconcile internal records of sales activity to the designated general ledger account. If there is more than one category for either internal or external sales, the designated general ledger account becomes a clearing account, and the unit must distribute sales activity and “zero” these accounts via an accounting journal entry. Please contact Cash Management for additional information.

Canceling a Merchant ID

Should a unit decide that a MID is no longer needed, the unit must contact Cash Management to cancel the MID. Likewise, the associated processing method must be properly disabled (see the Decommissioning of Computer Systems and Electronic Media Devices segment of this policy).
POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, ITHACA CAMPUS UNITS, continued

Reporting a Breach

Units must develop a local incident response procedure approved by Cash Management and train/inform all employees on procedures that must be adhered to when there is a suspected breach.

Requirements of the Individual

The most effective method to minimize the harm perpetrated in a breach situation is to take immediate action. If you suspect or have a confirmed breach of credit card information, please immediately contact Cash Management at (607) 254-1590, as well as the Network Operations Center (NOC)/IT Security Office at (607) 255-9900.

Unit Technical Requirements

- Immediately contain and limit the exposure to prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. To preserve evidence and facilitate the investigation:
  - Do not access or alter compromised systems, (i.e., do not log on at all to the machine to change passwords or run antivirus software, and do not log in as ROOT).
  - If using a wireless network, disable the wireless interface on the compromised system.
  - Do not turn the compromised machine off; instead, isolate compromised systems from the network, i.e., unplug cable.
  - Preserve logs and electronic evidence.
  - Log all actions taken.
  - Be on high alert and monitor all systems with cardholder data.
- Alert all necessary parties immediately:
  - Internal information security group and incident response team: NOC/IT Security Office.
  - Contact Cash Management who will contact the merchant bank.
- Be prepared to provide all potentially compromised accounts and related information, as requested by the processing bank, within 10 days of the breach.
- Be prepared to provide an incident report (which will be forwarded to your unit by the University Treasurer’s office, as provided by the merchant bank) within three business days of the reported compromise.

The merchant bank and the credit card agencies will consult to determine whether an independent forensic investigation will be initiated on the compromised entity.
# POLICY 3.17

## Accepting Credit Cards to Conduct University Business

<table>
<thead>
<tr>
<th>PROCEDURES, WEILL CORNELL CAMPUS UNITS</th>
</tr>
</thead>
</table>

### PCI DSS Compliance Certification

To document PCI compliance, the acquirer will issue an annual certification of PCI compliance when all PCI DSS requirements are met. This certification must be submitted each year to the Office of Cash Management, at the Ithaca Campus, no later than June 30. This activity will be coordinated by the Privacy Officer and Assistant Controller.

Training in PCI requirements is provided by the college. Training materials may be accessed at [mycertificates.med.cornell.edu](http://mycertificates.med.cornell.edu).

### Credit Card Information and E-mail

- **Caution:** Instruct customers of this prohibition. Additionally, if a unit receives credit card information via unsecured e-mail, the unit must delete the e-mail, **and not process the transaction**, notifying the customer.

- **Note:** Anyone transmitting sensitive electronic information may do so using the WCMC File Transfer Service.

  "The WCMC File Transfer Service provides a more secure way for users to exchange files that contain sensitive or confidential information compared to standard e-mail. This service can also facilitate exchange of large files that cannot be sent over e-mail. Both WCMC community members and external users can use this service by visiting [transfer.med.cornell.edu](http://transfer.med.cornell.edu)."

### Establishing a Merchant Account

To establish a merchant account, contact the Assistant Controller.

### Decommissioning of Computer Systems and Electronic Media Devices

When a computer system or media device that was used for credit card processing is taken out of production, all sensitive data must be removed. The hard drive of any computer system or any media device must be completely wiped and overwritten per instructions provided by ITS.

At the very least, the media device must be erased and zeroed utilizing the United States Department of Defense 5220.22-M short-wipe procedure. A media device can be re-commissioned only after it has been completely sanitized. If a media device will not be re-commissioned, it must be physically destroyed. Contact Environmental Health and Safety if a computer is to be destroyed.

### Protecting Sensitive Information

Terminals, laptops, and other media devices that contain confidential (Level 1) Information, (as defined in WCMC Policy 11.3 – Data Classification), must be identified and monitored.
POLICY 3.17

Accepting Credit Cards to Conduct University Business

<table>
<thead>
<tr>
<th>PROCEDURES, WEILL CORNELL CAMPUS UNITS, continued</th>
</tr>
</thead>
</table>

Further, any individuals who regularly handle credit card information must protect that information as detailed in WCMC Policy 12.2 – Physical Security.

**Third-Party Outsourcing**

Units that outsource storage, processing, or transmission of cardholder data to third-party providers must obtain from them annually, a Report on Compliance (ROC), which is evidence of a successfully completed PCI DSS assessment. This documentation must be submitted to the Assistant Controller.

In addition, units that are considering third-party outsourcing for credit card processing, or are renewing their current contracts, must consult with Office of University Counsel before signing a service contract. Office of University Counsel will review the contract for appropriate language, including a clause addressing continued compliance and specific terms regarding financial responsibility in the event of a breach.

◆ Caution: Units are prohibited from engaging third-party service providers that are not PCI-compliant and have not provided ROCs.

**Transaction Reconciliation**

Finance will post the sales transactions from the bank daily, and discount and other fees monthly. Each unit is responsible to reconcile its internal sales records. The person(s) responsible for reconciliation should not have access to the sales processing system.

**Refunds**

When an item or service is purchased using a credit card and a refund is necessary, the refund must be credited only to the same account from which the purchase was made, unless the original credit card account has been cancelled, in which case the refund may be issued to a different credit card. In addition, documentation of the original charge must be included with any refund transaction processed by the unit.

◆ Caution: Under no circumstance is it permissible to issue a cash refund.

To process a refund, follow the procedure appropriate to the mode of processing.

**Handling a Customer Disputed Charge**

The bank is obligated to advise the unit, in writing, of a disputed charge. The unit is responsible to provide the bank with written proof that the transaction was authorized by the customer. Failure to respond or provide a copy of a receipt signed by the customer or documentation of the shipping address will result in a chargeback to the unit’s account. All bank requests for information concerning a dispute must be answered within two business days of receipt.
POLICY 3.17
Accepting Credit Cards to Conduct University Business

PROCEDURES, WEILL CORNELL CAMPUS UNITS, continued

Posting and Reconciling Transactions

It is important to record sales revenue accurately in the college's financial records. Units must submit to the Assistant Controller the WCMC fund(s) where the revenue from the credit card payments will be recorded.

A unit is expected to reconcile internal records of sales activity to the designated fund.

Canceling a Merchant ID

Should a unit decide that a merchant ID (MID) is no longer needed, the unit must contact Finance to cancel the MID. Likewise, the associated processing method must be properly disabled (see the Decommissioning of Computer Systems and Electronic Media Devices segment of this policy).

Reporting a Breach

Units must notify the Privacy Office and/or ITS Security when there is a suspected breach.

Requirements of the Individual

The most effective method to minimize the harm perpetrated in a breach situation is to take immediate action. If you suspect or have a confirmed breach of credit card information, immediately contact the Privacy Office, at (212) 746-1121, as well as ITS Security at (212) 746-7457.

Also, the individual should perform the following technical tasks:

1. Do not access or alter compromised systems, (i.e., do not log on at all to the machine to change passwords or run antivirus software, and do not log in).
2. If using a wireless network, disable the wireless interface on the compromised system.
3. Do not turn the compromised machine off; instead, isolate compromised systems from the network, (i.e., unplug cable).
POLICY 3.17
Accepting Credit Cards to Conduct University Business

INDEX

Accepting Cash and Checks, University Policy 3.22 .......................................................... 4
Accepting University Gifts, University Policy 3.1.1, 4
Acquirer .......................................................... 7, 9, 11, 23
Application for Credit Card Merchant Accounts ......................................................... 4, 19, 21
Assistant Controller (WCMC) .... 6, 11, 12, 23, 24, 25
Authorization ................................................... 24
Authorization number ................................. 11
Bank ................................................... 7, 9, 11, 13, 17, 21, 22, 24
Breach .................................................. 5, 6, 18, 20, 22, 24, 25
Business practices ................................. 5, 6
Card authentication value (CAV) ................. 7
Card identification number (CID) .............. 7, 14
Card number ........................................ 9, 11
Card reader ............................................. 17
Card security code (CSC) .......................... 7
Card validation code (CVC) ......................... 7
Card verification value (CVV) ................. 7
Cardholder ............................................. 14, 19, 20, 22, 23, 24
Cardholder data ........................................ 14, 20, 22, 24
Cash .................................................. 1, 16, 17, 21, 24
Cash advance ......................................... 16
Cash Management ................................... 1, 5, 6, 8, 9, 11, 12, 13, 17, 19, 20, 21, 22, 23
Cash register ......................................... 17
Chargeback ........................................ 5, 7, 21, 24
Compromised systems ................................. 22, 25
Confidential (Level 1) information ............. 20, 23
Confidential information ......................... 9, 11
Confirmation ........................................ 9, 11
Contract .............................................. 5, 6, 9, 20, 24
Cornell Information Technologies (CIT) .... 13
Corporate card ........................................ 16
Cost Transfers on Sponsored Agreements, 
University Policy 3.20 ................................. 4
Credit card data ........................................ 14
Credit card fee ........................................ 13
Credit Card Receipt e-doc .......................... 21
Credit check ........................................... 18
CU Learn ................................................. 4, 8
Customer ............................................. 1, 7, 12, 16, 17, 18, 19, 21, 23, 24
Data Classification, WCMC Policy 11.3 4, 23
Data Stewardship and Custodianship, University Policy 4.12 ...... 4, 14
Disputed charge ...................................... 5, 9, 11, 21, 24
Donation ................................................. 11
DropBox, Cornell University ......................... 4, 19
Elavon ................................................. 5
Electronic media .................................. 14
E-mail .................................................. 14, 19, 23
Equipment ........................................... 5, 17
Finance Department (WCMC) ..................... 12, 13, 25
Finance Department Compliance Office (WCMC) 6, 12
Finance Department, WCMC ....................... 13
Financial Irregularities, University Policy 3.6 ...... 4
General ledger ....................................... 9, 11, 13, 20, 21
Gifts ...................................................... 12
Incident report ......................................... 22
Information Security (WCMC) ...................... 6, 25
Information Security, University Policy 5.10 ....... 4
Information Technologies and Services (ITS - WCMC) ........................................ 13, 14, 23, 25
Interdepartmental revenue ........................ 20
Interdepartmental sales .......................... 20
Investigation ........................................... 22
IT Security Office ..................................... 5, 9, 19, 22
Journal credit ........................................... 5
Kuali Financial System (KFS) ....................... 21
Laptop .................................................. 14, 20, 23
Laptop Encryption, WCMC Policy 11.6 ........ 4, 14
List of Validated Payment Applications, PCI Security Standards Council ................. 4
Lockbox Credit Card Refund Form ............... 21
Lockbox Credit Card Refund Form ............... 4
Lockbox processing ................................... 7, 16, 17
Magnetic stripe ....................................... 7, 14
POLICY 3.17

Accepting Credit Cards to Conduct University Business

INDEX, continued

| Media device | 8, 9, 10, 16, 17 |
| Merchant | 6, 7, 12, 13, 16, 19, 20, 21, 22, 23, 25 |
| Merchant account | 5, 6, 7, 9, 13, 17, 20, 21, 22, 23, 25 |
| Merchant ID | 5, 7, 9 |
| Merchant discount | 5, 7, 9 |
| myCertificates | 13, 17, 21, 25 |
| Network | 8, 10, 25 |
| Network Operations Center (NOC) | 5, 9, 20 |
| Non-degree course | 12, 16 |
| Office of University Counsel (WCMC) | 6, 24 |
| Outsourcing | 9, 20, 24 |
| Password | 8, 9, 14, 22 |
| Payment Card Industry (PCI) | 1, 7, 8, 12, 13, 23 |
| Payment Card Industry Data Security Standards (PCI DSS) | 1, 7, 8, 9, 12, 13, 14, 18, 20, 23, 24 |
| PC processing | 16, 17 |
| PCI | 5, 6 |
| PCI Security Standards Council | 4 |
| Personal identification number (PIN) | 7, 8, 14 |
| Physical Security, WCMC Policy 12.2 | 4, 23 |
| Point of sale | 9, 11, 13 |
| Primary account number (PAN) | 7, 14, 17 |
| Privacy Office (WCMC) | 6, 25 |
| Privacy Officer (WCMC) | 11, 23 |
| Private network | 13 |
| Processing fee | 7 |
| Procurement card | 20 |
| Procurement of Goods and Services, University Policy | 3.25 |
| Receipt | 7, 9, 11, 17, 21, 24 |
| Reconcile | 9, 11, 20, 21, 24, 25 |
| Reconciliation | 9, 19, 20, 24 |
| Record Retention | 11 |
| Refund | 11, 21, 24 |
| Registration fee | 12 |
| Remote office | 13 |
| Report on compliance (ROC) | 8, 9, 20, 24 |
| Reporting Electronic Security Incidents, University Policy | 5.4.2 |
| Responsible Use of Information Technology Resources, University Policy | 5.4.1 |
| Responsible Use of Information Technology Resources, WCMC Policy 11.1 | 4, 14 |
| Retention of University Records, University Policy | 4.7 |
| Sales Activities on Campus, University Policy 4.3.4 | 4 |
| Sales tax | 5, 6, 9, 12, 20 |
| Secure website | 8, 16, 17 |
| Security Awareness Training | 4, 8, 9 |
| Security Awareness Training | 9 |
| Security Awareness Training | 9 |
| Security Awareness Training | 11 |
| Security Awareness Training | 19 |
| Security of Electronic University Administrative Information, University Policy | 5.10 |
| Security of Information Technology Resources, University Policy | 5.4.1 |
| Security standards | 8, 9, 13 |
| Segregation of duties | 9, 11 |
| Self-assessment questionnaire | 4, 8 |
| Senior finance officer | 9, 12, 19 |
| Sensitive data | 14, 19, 23 |
| Server | 13, 19 |
| Signature | 7, 9, 11 |
| Storage | 8, 14, 20, 24 |
| Tax Compliance | 5, 12, 20 |
| Terminal | 9, 14, 16, 17 |
| Terminal and printer processing | 8, 16, 17 |
| Third-party provider | 5, 6, 8, 9, 20, 24 |
| Third-party transactions | 20 |
| Transaction Authority and Payment Approval | 4 |
| Travel advance | 16 |
| Travel, WCMC-NYC, University Policy | 3.2.1 |
| Travel, WCMC-Qatar, University Policy | 3.2.2 |
| Tuition | 16 |
| Unit training attestation | 4 |
| University Counsel | 24 |
POLICY 3.17

Accepting Credit Cards to Conduct University Business

<table>
<thead>
<tr>
<th>INDEX, continued</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Travel, University Policy 3.2.................. 4, 16</td>
</tr>
<tr>
<td>University Treasurer ............................................. 22</td>
</tr>
<tr>
<td>Unrelated business income ................................... 12</td>
</tr>
<tr>
<td>Use of Escrowed Encryption Keys, University Policy 5.3 ......................................................... 4</td>
</tr>
<tr>
<td>Vendor .................................................................... 9, 14</td>
</tr>
<tr>
<td>Virtual private networking (VPN) ............................ 13</td>
</tr>
<tr>
<td>WCMC File Transfer Service ..................................... 4, 23</td>
</tr>
<tr>
<td>Weill Cornell Medical College (WCMC) ...................... 12</td>
</tr>
<tr>
<td>Wireless network .................................................. 22, 25</td>
</tr>
</tbody>
</table>