CREDIT/DEBIT CARD MERCHANT REQUIREMENTS

Category: Financial
Responsible Office: Financial Services
Responsible Executive: Vice President for Finance & Administration
Date Established: 4/6/09
Date Last Revised: 5/2/11
Date Posted to Library: 5/2/11

Summary

Credit/debit card payments must be processed in an efficient, consistent, secure, and controlled manner in compliance with the Payment Card Industry Data Security Security Standard.

Policy

BACKGROUND

The University at Buffalo (UB) recognizes that accepting credit/debit cards as payment for goods, services, and donations has become a common practice that improves customer service, brings efficiency to the cash collection process, and is essential when business is conducted electronically. Departments may accept credit/debit card payments in electronic format, via swipe card machine, or through the mail to be processed by the appropriate business office (Financial Services, University at Buffalo Foundation (UBF), or Campus Dining & Shops (CDS)). The business office will determine the most appropriate method to be utilized based on customer service and convenience, cost (dollars and time), volume of expected activity, and impact on revenue distribution.

Situations may occur that require the ability to accept credit/debit cards on a one time basis. Contact Financial Services for suggestions on how to handle these situations.

The Payment Card Industry (including American Express, Discover, Master Card, VISA, and other major card issuers) has established important and stringent security requirements to protect credit/debit card data. These requirements are called the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS provides a single approach to safeguarding credit/debit card data for all card brands and details the security requirements for transmitting, storing, accessing, and processing cardholder data. Compliance is the entire institution’s responsibility with duties and accountability assigned at every level of the payment process.

Penalties for non-compliance include significant fines and withdrawal of payment card services by the payment card industry.

POLICY STATEMENT

University at Buffalo departments may accept credit/debit cards as an appropriate form of payment for goods, services, and donations. As a credit/debit card merchant, University departments must:

• obtain approval from the appropriate business office (Financial Services, UBF, or CDS depending on the funding source) prior to entering into any contracts or purchasing software and/or equipment to process credit/debit card payments
• provide the Financial Services Office with a PCI Compliance certificate from the vendor
• complete the “Credit Card Merchant Request” form to accept credit/debit card payments using a swipe machine
• obtain approval from the Information Security Office for all technology implementations, including payment gateways
• establish departmental procedures in accordance with the most current version of the Payment Card Industry Data Security Standard (PCI DSS) for safeguarding cardholder information and secure storage of data at all times and in all formats
• annually complete the “PCI DSS Self-Assessment Questionnaire” distributed by Financial Services to demonstrate the department’s ability to maintain compliance with the PCI DSS.

Credit/debit card data is classified as regulated private data. Credit/debit card merchants are responsible for safeguarding the confidentiality of regulated private data in accordance with the following University policies:

• Password Protection
• Protection of Regulated Private Data
• Standards for Protecting Regulated Private Data

The safeguarding and storage of cardholder information is subject to:

• periodic reviews conducted by the appropriate business office
• audit by Internal Audit
• periodic assessment and vulnerability scans conducted by the Information Security Office to assess security controls.

Departments not complying with approved safeguarding, storage, and processing procedures may lose the privilege to serve as a credit/debit card merchant.

APPLICABILITY

This Policy applies to any official or administrator with responsibilities for managing University credit/debit card transactions and those employees entrusted with handling credit/debit cards and credit/debit card information.

DEFINITIONS

Cardholder data - any personally identifiable data associated with a cardholder including but not limited to account number, expiration date, name, address, social security number, and card validation code (three or four-digit value printed on the front or back of a credit/debit card).

Credit/Debit Card Merchant - a unit that accepts credit/debit card payments.

Payment Card Industry Data Security Standard (PCI DSS) - a set of comprehensive requirements for enhancing payment account data security. The PCI DSS was developed by the founding payment brands of the PCI Security Standards Council including American Express, Discover Financial Services, MasterCard Worldwide, and VISA International to facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical
protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data and offers a single approach to safeguarding sensitive data for all card brands.

**Regulated Private Data** - includes bank credit/debit card numbers with or without PINs, social security numbers, driver license numbers, state-issued non-driver identification numbers, protected health information, passwords, and computer access protection information.

**Revenue Distribution** - process used to prioritize the allocation of revenue to departments based on the type of fee collected through the student account billing system.

**RESPONSIBILITY**

**Department or Unit Heads**
- Consult with the appropriate business office to determine whether accepting credit/debit card payments provides benefits that justify the additional cost. Benefits include assured payment, automation of payment collection, and customer service convenience. Costs include fees associated with accepting credit/debit cards and the time and effort required to comply with credit/debit card regulations.
- Submit the “Credit Card Merchant Request” form to the appropriate business office (Financial Services, UBF, or CDS depending on the funding source) to establish a credit/debit card merchant account.
- Provide the Financial Services Office with a PCI Compliance certificate from the vendor.
- Review and comply with the following University policies:
  - Password Protection Policy
  - Protection of Regulated Private Data
  - Standards for Securing Regulated Private Data
- Review and comply with the most current version of the Payment Card Industry Data Security Standard (PCI DSS).
- Annually, complete the “PCI DSS Self-Assessment Questionnaire” distributed by Financial Services.
- Notify the Information Security Office prior to implementation of any technology changes affecting transaction processing associated with the credit/debit card merchant account.
- Annually, ensure that the appropriate staff complete the UB PCI Tutorial distributed by Financial Services.

**Credit/Debit Card Handlers and Processors**
- Annually complete the UB PCI Tutorial distributed by Financial Services.
- Review and comply with the following University policies:
  - Password Protection Policy
  - Protection of Regulated Private Data
  - Standards for Securing Regulated Private Data
- Review and comply with the most current version of the Payment Card Industry Data Security Standard (PCI DSS).
Financial Services, UBF, and CDS
- Consult with departments regarding the options for the most appropriate method to accept credit/debit card payments.
- Review and approve the establishment of credit/debit card merchants.
- Administer the process of obtaining new merchant numbers.
- Conduct periodic reviews of existing merchants regarding safeguarding and storage of cardholder information.
- Provide periodic training on the secure storage and disposal of all non-eCommerce credit/debit card paper transaction records in conjunction with cash handling training.

Financial Services
- Annually, distribute the UB PCI Tutorial and the “PCI DSS Self-Assessment Questionnaire” to all departments (regardless of funding source) who accept payment via credit/debit cards.
- Monitor to ensure that all departments (regardless of funding source) complete the “PCI DSS Self-Assessment Questionnaire.”
- Contract with an authorized vendor to complete a quarterly scan for all departments (regardless of funding source) that electronically accept credit/debit card payments.
- Update the security scan vendor Web site with “PCI DSS Self-Assessment Questionnaire” answers as required by the merchant bank.

Information Security Office
- Review and approve implementation of payment gateways and technology changes associated with credit/debit card transaction processing.
- Conduct periodic reviews for compliance with the PCI DSS.

PROCEDURES
- Complete the “Credit Card Merchant Request” form; the Request must be signed by the department manager and the dean’s office.
- Submit the completed “Credit Card Merchant Request” form to the appropriate business office:
  - Financial Services – 418 Crofts Hall, North Campus
  - University at Buffalo Foundation – Center for Tomorrow, North Campus
  - Campus Dining & Shops – 146 Fargo, Ellicott Complex, North Campus
- Upon receiving approval to become a credit/debit card merchant:
  - The appropriate business office will provide the necessary equipment and training, information regarding processing procedures, and related University policies.
  - The department must follow the Payment Card Industry Data Security Standard (PCI DSS).

Contact Information

<table>
<thead>
<tr>
<th>Financial Services</th>
<th>Information Security Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>645-2660</td>
<td>645-7979</td>
</tr>
<tr>
<td>418 Crofts Hall</td>
<td>517 Capen</td>
</tr>
<tr>
<td>North Campus</td>
<td>North Campus</td>
</tr>
<tr>
<td><a href="http://ubbusiness.buffalo.edu">http://ubbusiness.buffalo.edu</a></td>
<td><a href="mailto:sec-office@buffalo.edu">sec-office@buffalo.edu</a></td>
</tr>
</tbody>
</table>

Related Information

University Documents:
- Credit Card Merchant Request Form
  http://www.business.buffalo.edu/ubbContent/Forms/fs/Merchant request form.xlsx
- Password Protection Policy
  http://www.buffalo.edu/content/www/ubit/policies/it-policies-a-to-z/ubit-password/_jcr_content/par/assetcolumn/assets/relateddownload/file.res/UB-PasswordPolicy-11-1-2013.pdf
- Protection of Regulated Private Data Policy
  http://www.buffalo.edu/content/dam/www/ubit/it-policies/RegPrivDataPolicy.pdf
- Standards for Securing Regulated Private Data
  http://www.buffalo.edu/content/dam/www/ubit/it-policies/StandardsRegPrivData.pdf
- Information Security: Data Access and Security Policy

Other Documents:
- NY State Information Security Policy
- NY State Information Security Breach and Notification Act

Related Links:
- VISA CISP merchant site:
  http://usa.visa.com/merchants/protect-your-business/index.jsp
- Payment Card Industry Security Standards Council:
  https://www.pcisecuritystandards.org/
- PCI Data Security Standard Version 3.0
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- PCI Security Standards Council Documents Library

Revision History

May 2011 - revised to include a requirement to furnish Financial Service with a PCI Compliance certificate for the vendor.
July 2014 - updates made to related information links that included a new Credit Card Merchant Request Form.

Presidential Approval

Signed by President John B. Simpson

John B. Simpson, President

4/6/09