

## BSR-5-04 Accepting credit card as a payment option procedures and guidelines

### BSR-5-04.01 Introduction

Many departments on campus accept credit card payments either once, occasionally, or on a daily basis. It is important that we protect the privacy of this data, as well as maintain compliance with the Payment Card Industry Standards and the Graham Leach Bliley Act.

Acceptance of credit cards at The University of Akron (The University) is governed by university rule 3359-03-06 which is available at <https://www.uakron.edu/ogc/UniversityRules/university-rules-by-number.dot>. This rule authorizes coordination of this payment option through the Office of the Associate Vice President/Controller.

The following procedures and guidelines establish the method for obtaining departmental permission to accept credit cards, the fee structure, and procedures required for safeguarding credit card information obtained.

### BSR-5-04.02 Approved credit cards

The University accepts the following credit cards:

1. VISA
2. MasterCard
3. Discover

### BSR-5-04.03 Approved methods for accepting credit cards

1. Manual collection using a form (aka the "blue" card)
2. Ongoing collection using terminals
3. Collection using a web-based product (ongoing or short term)

### BSR-5-04.04 Security Guidelines

Security is a priority for credit card transactions. Handling procedures for credit card information need to incorporate secure protocols for transferring, storing, and managing this sensitive data.

1. Credit card transactions must be in person, by telephone, by mail, or by a university approved webbased storefront or application. Cashnet is the current approved provider for web-based transactions. DO NOT accept credit card information by insecure electronic methods such as email or fax. Credit card information should never be transferred from one department to another by email or fax.
2. Credit card information should never be entered and stored on any computer or computer database program in the department. Applications other than Cashnet must be approved by the IT Security Committee **PRIOR** to their use on campus. Current security and encryption protocols must be in place for all approved applications.
3. Printed receipts should show only the last four digits of the credit card number.
4. When it is necessary to record an entire credit card number on a document in order to process the transaction, that document should be sent to the Cashier's Office for storage. If a department has obtained approval to store these documents, all but the last four digits of the credit card number should

be "blacked out" on the document as soon as refunds and disputes are no longer likely, preferably within 60 days. In no case should the entire number be retained for more than 180 days.

5. Original receipts from all transactions and any original, signed documentation will be retained in a secure location for a minimum of 4 years.

**BSR-5-04.04 Security Guidelines (continued)**

6. Paper records should be stored in a locked room or cabinet when left unattended. Only authorized employees should have access to the secure area.
7. Security incidents should be immediately reported by employees to their supervisor or the Information Security Officer for a security investigation. The University of Akron incident response plan will be put in motion and a response team deployed if necessary.

**BSR-5-04.05 Manual collection of credit card information**

From time to time, there could be a situation which requires obtaining credit card information to pay for an item. When collecting information manually (not through a swipe terminal or the web), a department must:

- (a) Use a university approved form. The Cashier's Office has produced a 3x7 inch card which contains all of the information necessary to process the credit card. Individual forms may be obtained through the Cashier's Office or bulk orders (over 20 cards) should be placed with Printing Services.
- (b) Return the completed form to the Cashier's Office for processing. The charge will not be valid until it is posted by the Cashier's Office and it may be declined. The department will be responsible for contacting the individual if the charge is declined. If the charge is accepted, it will be posted to the speedtype that the department indicates like any other deposit of funds.

**BSR-5-04.06 Application process to accept credit cards**

Each department must complete a Credit Card Merchant Application to accept credit cards through a terminal or a web-based product.

1. The form will define what type of transactions will be accepted:
  - (a) A retail account with in-person terminals
  - (b) An internet account with a web-based storefront
2. Independent arrangements with card processors are prohibited by rule 3359-03-06. The University receives a negotiated discounted rate based on total volume for the entire university which must be managed through the contract bidding process. This discount will be passed on to each department.
3. The form will request the following:
  - (a) The department requesting service
  - (b) The time frame for which the credit card usage is needed
  - (c) The estimated volume
  - (d) The account code to be charged for the bank charges (with the appropriate unit approvals)

4. Cash/credit control procedures for the department which comply with the Cash/Credit Control Policy are to be in place prior to approval of the application. This includes safeguarding the equipment, storage of credit card information, and access to web-based applications.
5. Upon return of Credit Card Merchant Application and other appropriate information, the Office of Associate VP/Controller will review the information and contact the department to discuss options available based on volume, expense and frequency of need. A review of safeguards will also occur at this time.

#### **BSR-5-04.07 Fees for accepting credit cards**

1. The University is charged a fee by the credit card processor (currently Paymentech).
  - (a) This fee is based on the total dollar amount of the transaction.
  - (b) This fee must be treated as an operating cost for your activities and cannot be assessed only to those customers paying by credit card.
2. The University is charged a fee for the terminals by the credit card processor. This cost must be paid by the department using the equipment.
3. The University charges a fee for setup and maintenance costs of the web-based product.
4. All fees are outlined on the Credit Card Merchant Application. Fees will be charged to the departments by the Office of the Associate VP/Controller.

#### **BSR-5-04.08 Responsibilities and Audit**

The Associate Vice President/Controller (or designee), Office of Student Accounts/Bursar, and the Internal Audit Department reserve the right to inspect and audit any credit card information or departmental procedures at any time.

#### **BSR-5-04.09 Closing a credit card account**

If a department no longer needs to accept card credit as a payment, contact the Director of Student Accounts/Bursar for instructions.