

Ball State University

Credit/Debit Card Handling Policy and Procedures

I. Background

Ball State University accepts payments in various forms including cash, checks and electronic fund transfers. University departments and other units may be allowed to accept credit and debit card payments under a centralized and standardized policy. Each department or unit must be approved as an Approved Charging Department (as defined below) prior to accepting charges by the Office of the Controller and Business Services ("Controller's Office"). If approved, departments or units may only use one of the methods of processing bank card transactions that are available for use through University Computing Services. The establishment of control measures for bank card transactions is necessary to maintain proper security over cardholder information. The Controller's Office is charged with the administration of the merchant bank card services contracts and must ensure compliance with Bank Card Merchant Rules and Regulations. University Computing Services is charged with the administration of information technology standards and security that meets the requirements of the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS is periodically revised and, therefore, the systems must be updated to ensure compliance. The University must limit the number of systems available for use to make the technical review process manageable.

II. Definitions

- a. **Acceptable Bank Card Companies:** MasterCard, Visa, Discover and American Express.
- b. **Approved Charging Department:** A department, organization or unit approved by the Controller's Office to process bank card sales.
- c. **Bank Card:** Either a credit card or a debit card.
- d. **PCI DSS:** The Payment Card Industry Data Security Standard is a regulation developed by the major bank card companies as a set of comprehensive requirements for enhancing payment account data security by instituting requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. To the extent that colleges and universities accept bank card payments for tuition, fees, goods, or other services, there is a contractual obligation to fulfill the data security standards established by the payment card industry.

III. Policy

All bank card transactions must be initiated and controlled through the Controller's Office. Since the sale of goods and services to entities outside of the University may raise special considerations (e.g., unrelated business income tax, accounting, legal, etc.) questionable sales should be reviewed by the Controller's Office and/or the Finance Office. All transactions shall only be performed on systems approved by the Controller's Office and University Computing Services. The Controller's Office and University Computing Services have selected systems for approved use based upon a careful review and analysis to ensure compliance with the PCI DSS and other information technology security standards. Departments shall not use any other card processing system. Any department or unit that engages an unauthorized system will be responsible for the cost of disengaging that system. Exceptions to this policy may be granted only upon prior written approval from the Controller's Office and University Computing Services.

IV. General Procedure

- a. The Dean, Director, or Department Head of a department or unit submits a request to the Controller's Office to establish a merchant account and upon approval by the Controller's Office becomes an Approved Charging Department.
- b. Departments must specify in writing to the Controller's Office the person or persons that will be allowed to approve a Credit (Refund) Slip. This cannot be the same person who processes sales.
- c. The employee assigned to supervise the handling of bank cards for an Approved Charging Department shall design an adequate process and procedure to ensure the following standards are maintained:
 - i. Keep secure and confidential all cardholder numbers and information.
 - ii. Bank card receipts should typically be treated with the same care as you would treat large sums of cash. The Approved Charging Department will be responsible for any losses due to poor internal or inadequate controls.
 1. Sensitive cardholder data (i.e., full account number, type, expiration or other data) cannot be stored in any way on computers or networks.
 2. Bank card numbers shall not be transmitted in an insecure manner, such as by email or through campus mail. Bank card numbers may be faxed only to a fax machine in a secure location. Printed customer receipts that are distributed outside the Approved Charging Department must show only the last four digits of the bank card number.
 3. All documentation containing card account numbers must be maintained in a "secure" environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes. Do not store bank card information in a customer database or electronic spreadsheet.

4. All documentation (i.e., order number, items ordered, etc.) regarding the transaction must be kept for not less than three (3) years. However, paper records containing bank card numbers should have all but the last four digits redacted as soon as refunds or disputes are no longer likely, but no more than 6 months.
- iii. A sales draft represents a bona fide, newly created transaction involving the merchandise and/or services itemized on the sales draft.
1. A customer cannot be charged before merchandise is shipped. In the case of an intangible product (i.e., registration) charge the customer when confirmation is sent to the customer.
 2. The University is required, in good faith, to maintain a fair policy for the exchange and return of merchandise and for resolving disputes over merchandise and/or services purchased with a bank card. If a transaction is non-returnable, non-refundable merchandise, that must be indicated in the appropriate area on the Approved Charging Department's web site with a link to your return policy.
 3. A cash advance or withdrawal from the Approved Charging Department to a cardholder, or to an employee, is not authorized.
 4. Proper credit for returns and adjustments must be done by performing the proper function as required by the bank card processor. Under no circumstances may a cardholder be paid in cash or check for any card refund or adjustment. If cash or a check is given as a refund and the cardholder files a dispute the Approved Charging Department will bear the loss of income from the transaction.
 5. The Approved Charging Department must provide Ball State University or the University's processor, upon demand, with any information, evidence, assignments or other assistance needed for any billing dispute with a cardholder or any dispute with a cardholder over the nature, quality or performance of the goods or services or in connection with any return or rejection of such goods or services. This request must be complied with in a timely manner.
 6. No employee may disclose or acquire any information concerning a cardholder's account without the cardholder's consent. An Approved Charging Department, department or employee shall not sell, purchase, provide, disclose or exchange card account information or any other transaction information to any third person other than: to University staff for assistance in the program; to the merchant card processor, to any Card Association as applicable, or as may be required by applicable law or regulation.

7. Bank card regulations prohibit assigning a minimum or maximum purchase amount, or adding a surcharge to bank card transactions.
 8. Depositing transactions belonging to another merchant is a violation of the Merchant Agreement. An Approved Charging Department that deposits another department's transactions is ultimately legally responsible for any problems resulting from the deposit. Therefore, Approved Charging Departments may not use any bank card terminal other than the one designated for and assigned with the merchant identification number for their department.
 9. Bank card regulations prohibit listing the cardholder's personal information on the bank card draft/ticket. Such information includes, but is not limited to, phone number, driver's license or Social Security number.
- iv. Restrict access to bank card data and processing to appropriate and authorized personnel.
 - v. Personnel involved in bank card handling are expected to attend card security training every two years.
 - vi. Establish appropriate segregation of duties between bank card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all bank card refunds is required.
 - vii. Perform an annual self assessment to ensure compliance with this policy and associated procedures, and report the results of this assessment to the Controller's Office.
 - viii. Notify and receive prior written approval from the Controller's Office and University Computing Services to request implementation of any technology changes affecting transactions processing associated with the merchant account.
- d. Approved Charging Departments will be required to purchase their own equipment. Supplies are furnished through the University's contract at this time.
 - e. Discount and other transaction fees are charged back to the Approved Charging Department by the Accounting Office.
 - f. **Violations of this policy and these procedures may result in the following consequences for the Approved Charging Department and/or the employees involved: discontinuance of the practice of accepting bank cards, loss of computer or network access privileges, disciplinary action, suspension, termination of employment, or legal action. The University will not be held liable for departments or individuals who are not approved merchants or who accept bank card payments without adhering to these standards. FAILURE TO ADHERE TO THE PCI DSS STANDARDS CAN RESULT IN SUBTANTIAL FINES BEGINNING AT UP TO \$25,000 FOR THE FIRST VIOLATION AND UP TO \$500,000 PER INCIDENT DEPENDING ON THE BANK CARD COMPANY'S REGULATIONS.**

If you feel that bank card records may have been compromised in any way, please immediately refer to procedures in the Suspected Information Security Breach Reporting & Incident Response Procedure for the proper steps to take to report the incident.