CREDIT/DEBIT CARD HANDLING PROCEDURE

BALL STATE UNIVERSITY PCI COMPLIANCE COMMITTEE

Version:	V 2.4
Date of version:	06/01/2017
Created by:	PCI Compliance Committee
Approved by:	Bernard M. Hannon – VP for Business Affairs and Treasurer Philip Repp – VP for Information Technology
Confidentiality level:	University-Internal

Change history

Date	Version	Created by	Description of change
11/01/2008	1.0	Mary Cosby	Basic Document Outline
06/29/2015	2.0	PCI Compliance Committee	Updated to Reflect New Technology and Terminology
07/23/2015	2.1	Information Technology	Revised to clarify several areas. Added breach to bring in conformity with university data breach reporting, reordered several sections and revised to add clarity.
07/25/2016	2.2	PCI Compliance Committee	Updated grammatical anomalies
11/29/2016	2.3	PCI Compliance Committee	Updated language pertaining to separation of duties.
06/01/2017	2.4	PCI Compliance Committee	Reviewed and updated Committee members, terminology, and grammatical anomalies

CONTENTS

PURPOSE, SCOPE, AND APPLICATION OF THESE PROCEDURES

Ball State University accepts payments in various forms including cash, checks, and electronic funds transfers.

University departments and other units are permitted to accept credit and debit card payments only under the centralized and standardized procedure outlined in this document.

Each department or unit must be approved by the Payment Card Industry (PCI) Compliance Committee as an Approved Charging Department (as defined below) prior to accepting bank card charges. Approved departments and units may process bank card transactions through the specific methods authorized by the PCI Compliance Committee.

1 DEFINITIONS

1.1 **Acceptable Bank Card Companies:** MasterCard, Visa, Discover, and American Express. Note that the payment processor which handles CASHNet eCommerce or Certain Meetings (Moneris) does not permit the use of American Express. The list of approved bank card companies may change from time-to-time as approved by the payment processors and the PCI Compliance Committee.

1.2 **Address Verification System (AVS):** An authentication method that verifies the billing address of the cardholder when processing a transaction. Usually the billing zip code, but could also include additional billing address information.

1.3 **Approved Charging Department:** A department, organization, or unit approved by the PCI Compliance Committee to process bank card sales using approved methods of payment processing.

1.4 **Bank Card:** Either a credit card or a debit card.

1.5 **Bank Card Transactions:** Sales or credit (refund) to a customer's bank card.

1.6 **Card Security Codes (CAV2/CID/CVV2/CVC2/CVM/CVS/CVV codes):** A code of 3 or 4 extra digits (typically printed on the back of the card); is used to verify that a card is physically present when processing a transaction.

1.7 **Chargeback:** When a customer's bank reverses a charge due to potential fraud or other reasons (card charged in error, merchandise never received, etc.).

1.8 **EMV (Smart Cards) With Chip Technology:** EMV (EuroPay, MasterCard, and Visa) is a global payment system in which the cards contain microprocessor chips to prevent counterfeiting. Beginning October 1, 2015 merchants who fail to utilize EMV when a customer presents an EMV enabled bank card (such as Visa® and MasterCard® branded cards) may be liable for losses if the card turns out to be counterfeit. Merchants who have upgraded their card readers to certified EMV terminals will not generally be liable for such transactions provided they utilize the EMV and adhere to the fallback protocol when an EMV card will not function properly. EMV comes in two versions, and merchants must be able to accept both:

1.8.1 **Chip and Signature:** The cardholder must sign his/her name after the EMV card has been processed.

1.8.2 **Chip and Pin:** The cardholder must enter a unique PIN after the card has been processed in order for the transaction to be accepted. This is more secure than Chip and Signature.

1.9 **PCI Compliance Committee:** Committee of various University personnel tasked with ensuring PCI compliance. The Committee consists of the University Controller, Director of Financial Information Systems and Technology, Senior Information Systems Analyst in Financial Information Systems and Technology, Director of Cash & Investments, Assistant Director of Information Security Services, Director of Information Security Services, and the Director of Accounting. All inquiries can be directed to CREDITCARDS@BSU.EDU.

1.10 **PCI DSS:** The Payment Card Industry Data Security Standard applies to any organization which accepts, captures, stores, transmits, has access to, and/or processes payment card information either manually or through an automated system. The PCI DSS is an evolving set of comprehensive requirements designed to enhance payment account data security.

2 REQUIREMENTS

The following general requirements apply to all bank card transaction processed by or on behalf of Ball State University:

2.1. **Only Approved Charging Units May Accept Bank Card Payments:** All bank card payments to any university office or unit may be accepted only by Approved Charging Units. The PCI Compliance Committee is charged with evaluating the sale of goods and services to entities outside of the University and examining any special considerations (e.g., unrelated business income tax, accounting, legal, taxes, etc.)

2.2. **Only Approved Systems and Services May Be Used To Accept Bank Card Payments:** Bank card transaction may only be performed on systems which have been approved by the PCI Compliance Committee. The PCI Compliance Committee has selected systems approved for use which comply with the PCI DSS and other information technology security standards. Departments shall not use any other card processing system which has not been approved by the PCI Compliance Committee. Any department or unit that engages an unauthorized system will be responsible for the cost of disengaging that system.

Exceptions to these procedures may be granted by written approval of the PCI Compliance Committee.

3 ACCEPTING BANK CARD PAYMENTS

To accept bank card transactions a department must be approved as an Approved Charging Department, or special arrangements may be made for short-term processing needs:

3.1. **Establishment of Approved Charging Department:** To establish a new Approved Changing Department, the Dean, Director, or unit head will start the process by submitting the appropriate request to establish a merchant account (review the www.bsu.edu/creditcards website for current procedures on how to submit an Approved Charging Department request). Upon approval by the PCI Compliance Committee, the unit becomes an Approved Charging Department.

3.2. **Short-Term or Immediate Needs for Bank Card Processing:** Departments with an immediate or short-term need to process such transactions, the department should contact the PCI Compliance Committee at creditcards@bsu.edu to determine the best method for processing bank card transactions. Approved Charging Departments are not permitted to allow use of their equipment or process charges on behalf of other units. These requirements are described more fully below.

In either case, all bank card processing must adhere to the requirements for training, security, and general payment processing outlined below.

4 BANK CARD PROCESSING REQUIREMENTS

Prior to processing bank card transactions, it is the responsibility of the Approved Charging Department to:

4.1. **Allocate Sufficient Human Resources:** Identify the personnel needed to process bank card

transactions, ensuring adequate backups and separation of duties (as defined below).

4.2. Ensure Employees Have Completed Training: All personnel involved in bank card processing successfully complete PCI compliance training described below. Contact the PCI Compliance Committee for more information about compliance training.

4.3. Complete The Annual Bank Card Processing Self-Assessment: This form must be completed and returned to the PCI Compliance Committee prior to the end of each fiscal year. Failure to complete and return this form may result in suspension of Approved Charging Unit status.

4.4. Bank Card Security Requirements: Approved Charging Units must institute an internal card processing procedure to ensure all cardholder data is kept secure and treated as confidential information. Procedures established by the Approved Charging Units must include each of the following requirements:

4.4.1. Security Of Payment Processing Equipment: Identify a secure location for any bank card equipment and documentation and ensure only approved and trained personnel have access to such equipment.

4.4.2. Access to Bank Card Information: All access to customer bank card data and payment processing must be restricted to trained and authorized personnel. Persons who have not successfully completed training and not involved in payment processing shall not have access to bank card or confidential information involved with that transaction.

4.4.3. Separate Approval Of Each Department: Depositing transactions belonging to another merchant is a violation of the Merchant Agreement. Approved Charging Departments may not share their bank card terminal or use the bank card terminal assigned to another unit. An Approved Charging Department that deposits another department's transactions is ultimately responsible and will bear the loss from the transaction if a chargeback is granted by the bank.

4.4.4. Separation Of Duties: Appropriate separation of duties must be maintained by the Approved Charging Department. Personnel entering credit (refund) transactions are not recommended to be the same personnel entering sales transactions. If a separation of duties cannot be achieved, mitigating controls must be defined in the department's card handling procedures. All credit (refund) transactions must have documented supervisory approval. It is understood that some areas may be limited on resources and that it will not always be possible to maintain the level of segregation of duties as outlined in these procedures. While every attempt to adhere to these procedures is recommended, deviations may be acceptable only if approved by the PCI Compliance Committee. However, reconciliations must be done by an individual independent of the process regardless.

4.4.5. Workstation and User Account Security: Employees must adhere to general security requirements for workstations and user account controls. These policies and procedures can be found at the (www.bsu.edu/security/itpolicy). Regarding user accounts, each employee must have a unique login and password to access computer systems or computer programs that contain payment card information to ensure individual accountability and segregation of duties. The sharing of passwords or login information is strictly prohibited. Each individual employee is responsible for keeping their login identification and password confidential.

4.4.6. Retention of Card Data is Prohibited: Long-term retention of sensitive cardholder data (i.e., full account number, card type, card expiration date) whether electronic or on paper is prohibited. Such data must not be retained for a period exceeding two days (and must not be

stored over a weekend or holidays).

4.4.7. **Temporary Storage of Cardholder Data:** The transaction data 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. Bank card information may not be stored in a local database or in any electronic format maintained by the university.

4.4.8. **Recording of Customer Information:** Bank card regulations prohibit listing the cardholder's personal information such as phone number, driver's license, or Social Security number, on the bank card draft or sales receipt or ticket.

4.4.9. **Use Of Card Verification Codes:** Any retention of CVM/CVV/CVS (card verification codes) is strictly prohibited (i.e., paper forms which allow bank card payment must not request or include card verification codes). Any forms which solicit bank card payment must be pre-approved by the PCI Compliance Committee. It is acceptable to ask for the card verification code only when processing card transactions in real-time (i.e., via phone, or in person) however these numbers may not be written down or retained even for short-term periods as is permitted with the bank card numbers indicated above.

4.4.10. **Disclosure of Card Holder Data:** BSU employees may not disclose or acquire information concerning a cardholder's account without the cardholder's consent. No departments or employees shall sell, purchase, provide, disclose, or exchange card account information or any other transaction information to any third-party other than: to University staff for assistance in the program, to the merchant card processor, to any card associations as applicable, or as required by applicable law or regulation. Contact the PCI Compliance Committee for assistance if needed.

4.4.11. **Receipt of Bank Card Data by Fax, U.S Mail, or other similar secured means:** Departments may request sensitive cardholder information if it is transmitted to the department via secured fax or U.S. Postal Mail or other secure courier such as FedEx. If a department receives a request to pay from a cardholder through a secure method (i.e., cardholder sends an acceptable fax or U.S. Mail), departments are expected to process the transaction as soon as reasonably possible (but in no even later than two business days) before permanently redacting the sensitive cardholder data received from the cardholder as described below.

4.4.12. **Paper Records Redaction Requirements:** Paper records containing bank card numbers must have all but the last four digits redacted as soon as the transaction is processed. “Redaction” means physically removing all but the last four digits of the card number from the document such as by cutting or shredding, or another form of physical destruction. Note that it is not sufficient to mark over the top of numbers with a marker or other ink – these are insecure methods which do not provide adequate redaction.

4.4.13. **Receipt of Bank Card Data through E-Mail or Other Unsecured Means:** If departments receive sensitive cardholder information through an unsecured manner (i.e., cardholder sends requests to pay through e-mail, voicemail), that information must be destroyed immediately. The cardholder should be notified of the proper method of sending such information which must be re-submitted through a secure channel. Transactions shall be processed only when cardholder information has been received in a secured manner.

4.4.14. **Transmission of Bank Card Data Generally:** Bank card numbers shall not be transmitted in an unsecure manner, such as by e-mail 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 not show more than the last four digits of the bank card number; displaying zero digits is preferable.

4.4.15. Retention Of Records: All original transaction documentation (i.e., order number, items ordered, receipts, etc.), with sensitive cardholder data which has been redacted must be retained for not less than eighteen months. Cardholders have up to 12 months (Visa) or 18 months (MasterCard) to request copies of the original sales documentation; keeping these receipts reduces the risk of a chargeback.

4.4.16. Physical Security Of Devices/Equipment: All bank card processing equipment must be stored in a secured, locked location when not in use. Inspect all payment processing equipment for signs of tampering, alterations, or damage. Immediately cease the use of any equipment which shows signs of tampering (such as the device having been opened or modified) store the equipment in a secure location, and report the suspect device to creditcards@bsu.edu.

4.4.17. Damaged or Unneeded Equipment: Notify creditcards@bsu.edu for instructions regarding the return of damaged or unneeded equipment. The PCI Compliance Committee will work with the appropriate processing unit for proper disposal of such equipment.

4.4.18. Equipment Repair Personnel: Verify the identity of any third-party claiming to be maintenance or a repair person for payment card devices before granting them access to the device. If there are any concerns or doubts or if the identity cannot be verified, contact the vendor (if a previously established vendor) by phone and do not allow access to the device. Report any device repair or replacement to creditcards@bsu.edu.

4.4.19. Equipment Upgrades Or Replacements: Contact creditcards@bsu.edu prior to the selection, purchase, or installation any new payment processing equipment or allowing a third-party to do so. The PCI Compliance Committee will ensure equipment meets all requirements.

4.4.20. Changes to Connection Method Or Software: Any changes in the way a payment device is connected, for example moving from a phone line to an Ethernet connection, or moving from a physical payment terminal to a virtual terminal, must be approved in advance by the PCI Compliance Committee. Similarly, any changes to software such as adding or changing a third-party payment processing software package must also be approved in advance. Contact the PCI Compliance Committee at creditcards@bsu.edu for more information before making any such changes.

4.4.21. Responsibility for Losses: Bank card receipts must be treated with the same care as large sums of cash. The Approved Charging Department will be responsible for any losses. Losses resulting from poor or inadequate controls may result in other administrative actions including the possibility of removing the unit's approval to process bank card transactions until deficiencies are fully resolved, as well as other sanctions for violations as described below.

4.5. General Sales Processing Requirements: Approved Charging Units must also ensure compliance with the following general sales processing standards:

4.5.1. Timing for Charging a Bank Card: A customer may not be charged for merchandise before it is shipped. In the case of an intangible product (i.e., registration), charge the customer when confirmation is sent to the customer.

4.5.2. Exchange and Return Polices: The University is required, in good faith, to maintain a fair procedure for the exchange and return of merchandise and for resolving disputes over merchandise and/or services purchased with a bank card. The Approved Charging

Department's website, if applicable, must detail the return procedure, including identifying when transactions are considered non-refundable. Contact the PCI Compliance Committee for assistance if needed.

4.5.3. **Processing Returns and Sales Adjustments:** Returns and adjustments should be processed according to the methods as required by the bank card processor. Refund transactions may only be processed with supervisory approval and credited back to the original card using the same method as the original transaction. Check refunds may only be issued when it is not possible to refund back to the original card. If a check is given as a refund and the cardholder files a dispute, the Approved Charging Department will bear the loss from the transaction if a chargeback is granted by the bank.

4.5.4. **Cash:** Cash advances or withdrawals are prohibited.

4.5.5. **Requests For Assistance By The Payment Processor:** 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 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. Failure to respond to payment processor requests promptly may result in a default and automatic granting of a refund; the Approved Charging Department will bear the loss from the transaction if a chargeback is granted by the bank.

4.5.6. **Minimum/Maximum Purchase Amounts and Convenience Fees:** Bank card regulations prohibit assigning a minimum or maximum purchase amount or adding a surcharge to bank card transactions. A convenience fee can be added when using the CASHNet's SmartPay system. These charges are handled by a third-party merchant (Higher One), which is allowed. Contact the PCI Compliance Committee for assistance.

4.5.7. **Settlement of Bank Card Charges:** Bank card batches must be settled at least daily. Terminals can be configured for automatic daily batch settlement or for manual settlement. Please note that CASHNet eCommerce sites and Certain Registration applications are already configured to automatically settle the batch each day.

4.6. **Methods for Processing Bank Card Transactions:** There are two broad categories of bank card payment:

4.6.1. **"Card present" transactions:** This type of transaction is where a cardholder is physically present and swipes or inserts the card. This is always the preferred method of processing bank card transactions and should be used in every instance where practical. The cardholder's identity must be verified prior to processing, and the bank card receipt signed by the cardholder.

4.6.2. **"Card not present" transactions:** This type of transaction is where the cardholder is not physically present, for example phone-based orders. These transactions are permitted but are not preferred due to the higher interchange fees (assessed by the card issuer) and the greater chargeback and fraud risk.

4.7. **Additional Verification:** Bank Card processors may specify additional verification steps which will further reduce interchange fees which are charged back to departments as part of the payment processing cost. These additional verification steps should be used when possible and can be built into the card processing system. These methods include:

4.7.1. **Address Verification System (AVS):** An authentication method that verifies billing address of the cardholder when processing a transaction.

4.7.2. **Card Security Codes:** Merchant enters the card's security code of 3 or 4 extra digits (typically printed on the back of the card).

4.8. **Fees Assessed to Approved Charging Departments:** Approved Charging Departments will be charged fees associated with processing bank card transactions. These charges include transaction fees (assessed by the bank), interchange fees, equipment purchases, maintenance fees, and other fees which may be assessed from time to time by the payment processor or service providers.

5 BREACH REPORTING, MANDATORY TRAINING, AND ANNUAL REVIEW

The following sections cover procedures for reporting a suspected breach of confidential information, procedures for mandatory training, and procedures for the mandatory annual review process:

5.1. **Identifying and resolving data breaches:** In the event a suspected breach of any kind has occurred including the disclosure of bank card information to unauthorized personal, the following steps must be taken immediately:

5.1.1. If you believe criminal activity may be happening at that moment, contact the University Police Department (765-285-1111) and request immediate assistance.

5.1.2. Immediately cease the processing of bank card transactions until approved to resume operations.

5.1.3. Ensure any involved devices such as payment processing terminals, computers, etc. are turned off and disconnected from all telephone and network connections.

5.1.4. Follow the procedures for reporting a data breach, located at http://www.bsu.edu/security/itpolicy/.

5.1.5. After reporting the breach through the official channels above, send an e-mail to creditcards@bsu.edu and indicate that you have reported a breach through Office of Information Security Services.

5.2. **Employee Training:** Annual training for safe bank card handling and PCI Compliance is mandatory for:

5.2.1. Individuals who process bank card transactions.

5.2.2. Supervisors of individuals who process bank card transactions

5.2.3. Any other applicable personnel exposed to bank card data.

As new personnel assume any of the above duties, such persons must complete training prior to performing bank card-related duties. In such cases, an addendum to the Bank Card Processing Self-Assessment Form must be completed by the Approved Charging Department and submitted to the PCI Compliance Committee. Contact the PCI Compliance Committee for more information about mandatory training. Note that any employee who has been convicted of financial fraud or related illegal activities is prohibited from processing/handling bank card transactions.

5.3. **Annual Review:** All units accepting bank cards will be reviewed annually by the PCI Compliance Committee to ensure compliance with this Procedure and with PCI DSS. The information from the Bank Card Processing Self-Assessment form, from each applicable department head, will be reviewed to assist with completing the annual review. This review may include:

5.3.1. Verifying card processing procedures

5.3.2. Verifying terminal information – make/model number, connectivity, etc.

5.3.3. Verifying compliance of equipment/software.

5.3.4. Verifying names of those individuals with exposure to bank card information and their roles in the process.

5.3.5. Documenting the card processing environment, including creating equipment/network flow charts and creating payment transaction processing flow charts.

6 VIOLATIONS

Individuals who intentionally operate or accept bank card payments without approval as an Approved Charging Department or who knowingly violate these procedures are acting outside the scope of their employment and may be held personally liable for any losses, fines, fees, refunds, reverse charges, and other penalties as may be imposed by the payment processor or other entity. Additionally, violations of this procedure may result in:

6.1. Suspension of approval for accepting bank cards as a payment method.

6.2. Loss of computer or network access privileges.

6.3. Disciplinary action, suspension, termination of employment, or legal action.

FAILURE TO ADHERE TO THE PCI DSS STANDARDS MAY RESULT IN SUBSTANTIAL FINES PER INCIDENT DEPENDING ON THE BANK CARD COMPANY'S REGULATIONS AND THE SEVERITY OF THE VIOLATION.