



Payment Card Acceptance Administrative Procedure

Approved By: Brandon Gilliland, AVP for Finance and Controller
Effective Date: January 15, 2016
History: Approval Date: September 25, 2014
Revisions: December 15, 2015
Type: Administrative Procedure
Finance Policy Number: 3.11.01
Responsible Official: AVP for Finance & Controller
Director of Information Security
Related Policies: Payment Card Acceptance Administrative Policy
Departmental Deposit Administrative Policy

Administrative Procedure Statement

The purpose of this administrative procedure is to clarify the process of requesting a merchant account to accept payment cards during a sales transaction and to provide University faculty, staff and students with comprehensive procedures to ensure that proper accounting of funds is maintained and that cardholder data is kept secure throughout the transaction lifecycle.

Table of Contents

Administrative Procedure Statement	1
Table of Contents	1
Related Policies	2
Related Documents	2
Payment Card Acceptance Overview	2
Responsibilities	3
Approvals	4
Merchant Costs and Fees	5
Becoming a Merchant	5
Utilizing A Third-Party As A Merchant On Your Behalf	7

General Guidelines.....	7
Guidelines for Point of Sale Transactions	7
Guidelines for E-Commerce Transactions.....	9
Transaction Reconciliation and Accounting.....	10
Prohibited Payment Card Activities.....	10
Copy Requests and Disputed Transactions.....	11
Refunds	11
Payment Card Industry Data Security Standard Compliance	11
Risks, Sanctions & Fines Related to Non-Compliance	12
Data Retention	13
Definitions.....	13
Contacts.....	15
Policy / Procedure Violations	16
Appendix A: Address Verification System (AVS).....	17

Related Policies

Payment Card Acceptance Administrative Policy
 Departmental Deposit Administrative Policy

Related Documents

Merchant Request to Process Payment Cards Application
 Merchant Request to Change or Terminate Payment Cards Application
 Payment Card Terminal Inspection Log
 Wake Forest University Bank Card Confidentiality Agreement Form
 Wireless Terminal Deposit Form

Payment Card Acceptance Overview

Financial Services administers the payment card program at Wake Forest University and is responsible by the University’s Payment Card Acceptance Policy and the contract with the University’s sponsoring merchant bank and payment card acquirer for all payment card transactions accepted for the sale of goods and services by all University entities.

There are a variety of methods and technologies available for processing payment card transactions. Each method must be approved by the University PCI Committee before any third-party contract is signed or transactions are processed. Payment card processing can be broken down into two general methods or channels using three kinds of technologies: terminal, point of sale (POS), and e-commerce.

The two types of payment channels are ‘Card Present’ and ‘Card Not Present’. The main difference is determined by whether or not the bank-issued payment card is available to

have its chip or magnetic track read at the time of purchase or if a mobile payment service or digital wallet is utilized. Card Present processing is generally used for face-to-face transactions. The customer presents his/her payment card for payment, the card is swiped or inserted through a reader, and the customer generally signs a receipt for the merchant's records. Card Present transactions are most often handled by a payment terminal or a POS system.

Card Not Present processing is generally used for mail-order, telephone order, and e-commerce transactions. The payment card is not available to the merchant for inserting or swiping through a card reader, so the payment information must be manually keyed into the processing system. Processing payment cards in this manner can present additional challenges and risks compared to processing traditional Card Present payments. These risks must be carefully analyzed to minimize any potential for a security breach and potential loss of cardholder information. Any breach could result in not only monetary fines to the merchant, but also a loss of reputation and trust from customers.

University departments, organizations and affiliates intending to accept payment cards must establish and maintain a proper security environment to safeguard a customer's payment information at all times. Regardless of the channel or technology used, the customer trusts that the merchant department accepting his/her payment card information will protect that information as if the customer were handing over cash. Payment card information, therefore, should be treated as carefully as any other confidential information (e.g. Social Security Number). It is the responsibility of the merchant to follow these procedures to ensure transactions are processed safely and in accordance with the agreements put in place by the University and the University's payment acquirer.

University merchants can accept American Express, Discover, MasterCard and Visa. Merchants are not required to accept all card brands.

Responsibilities

Financial Services is responsible for reviewing and approving requests to set up or modify merchant accounts, accounting for payment card transactions, training merchants and ensuring merchant compliance on a routine basis.

Information Security is responsible for reviewing and approving equipment and software, responding to potential security breaches, training merchants and ensuring merchant compliance on a routine basis.

Merchants must designate individuals with the following roles: Fiscal Officer, Operations Manager, and a Dispute Resolution Contact. These roles may be fulfilled by the same individual.

- a) Fiscal Officer: responsible for submitting any requests to establish or update merchant department payment card processing services. There should only be one

- Fiscal Officer per merchant department. The Fiscal Officer is also responsible for the merchant department's compliance with all payment card processing requirements and policies and must sign off on the merchant department's compliance measures. A Fiscal Officer must be a department head or, for student organizations, the faculty/staff advisor.
- b) Operations Manager: responsible for overseeing daily card processing operations. The Operations Manager is also responsible for implementing and supervising the enforcement of all payment processing policies and requirements. This individual also ensures that individuals who process, transmit, store or dispose of cardholder data attend required training opportunities to learn about PCIDSS and related best practices regarding payment card transactions and third-party contractors fulfill contractual obligations to protect cardholder data.
 - c) Dispute Resolution Contact: responsible for responding to any requests for information regarding a disputed transaction. Information required to respond to these requests varies depending on the nature of the dispute, but generally a dispute is resolved by providing detailed information about a transaction (e.g. the signed merchant copy of the receipt).

Approvals

Before entering into any contract or purchasing equipment and software that will facilitate payment card processing activities, departments, organizations or affiliates must obtain the following approvals:

- a) Financial Services must approve all payment card processing activities at the University. This requirement applies regardless of the transaction method used (e.g., terminal, POS device or e-commerce).
- b) The University PCI Committee must approve all equipment and software implementation (including approval of authorized payment gateways) associated with the payment card processing. The University PCI Committee will ensure the equipment and software complies with PCIDSS standards and related procedures. Approved vendors and software must be confirmed as PCI compliant by the card associations and not just a third party assessor. All approved equipment must be validated as being compliant.

Third-party service providers must state through a formal contract their adherence, obligations and responsibilities in remaining compliant. These contracts will be submitted to and reviewed by Financial Services, Information Security and the Legal Department.

All applications must be approved by the school's or division's Senior Business Administrator or their proxy. Financial Services will be responsible for capturing this approval.

Approvals are granted based on the request application and supplemental materials described in the section, *Becoming a Merchant*.

Important! Under no circumstance may a department, organization or affiliate contact a payment card processor directly to obtain access to payment card privileges for University business needs.

Merchant Costs and Fees

University merchants are responsible for covering the costs related to accepting payment cards, including:

- a) Purchasing and maintaining, or renting approved equipment
- b) Purchasing and maintaining approved software applications
- c) Supply costs
- d) Transaction and processing fees (see below)
- e) Financial penalties resulting from noncompliance (see *Risks, Sanctions & Fines Related to Non-Compliance*)

Payment card processing typically involves several types of fees. These fees accumulate for each merchant account and are charged back to the responsible merchant department on a monthly basis by Financial Services.

Interchange or Discount Rate Fee: Each payment card transaction is assessed a fee known as the interchange discount rate. The fee amount is influenced by the card-issuing bank, the type of payment card used (debit vs. credit), the amount of the transaction, the amount of time between authorization and settlement, and the overall perceived risk of the transaction.

Transaction Processing Fees: Payment systems typically charge a flat rate per transaction as well as a flat monthly account fee. These fees are in addition to the interchange or discount rate fee.

Becoming a Merchant

In order to become a merchant, a department, organization or affiliate must complete the following steps before entering into any contract or purchase of software and/or equipment for processing of payment card transactions:

- a) Complete the 'Request to Process Payment Cards' application. This form captures basic information about the merchant and the types of transactions that will be occurring as well as information that will determine which Self-Assessment Questionnaire is required to ensure PCI compliance.
- b) Provide all available information about any proposed purchase of software and/or equipment to the University PCI Committee. Include contact information for the potential suppliers.

- c) Submit documented procedures for safeguarding the processing, transmittal, storage and disposal of cardholder information to the University PCI Committee via the Merchant / PCI Document Portal.

Payment card transactions must be done in person, by telephone, by mail, or via a secure University-approved internet application. Do not ever send or accept payment card information via email.

The procedures must, at a minimum, follow these requirements:

- 1) Store all materials containing cardholder account information in a restricted / secure area. In addition, these materials should be kept in a locked file cabinet, safe, or other secure storage location.
- 2) Any visitors in this secured area should always be identified, logged in and out, and escorted at all times.
- 3) Never store Sensitive Authentication Data subsequent to authorization.
- 4) Limit access to sales drafts, reports, or other sources of cardholder data to employees on a need-to-know basis.
- 5) Redact all but the last four digits of the account number if paper records containing payment card account numbers are stored.
- 6) Printed customer receipts that are distributed outside the merchant department must show only the last four digits of the payment card account number.
- 7) Do not store cardholder data in a customer database or electronic spreadsheet.
- 8) Render unreadable and cross-cut shred materials containing cardholder data prior to discarding.
- 9) Cardholder information is not to be taken or distributed for unauthorized purposes.
- 10) Visually inspect any physical card devices on a routine basis to ensure that they have not been tampered with. Inspections should be logged.

Once all of this information has been submitted, Financial Services will be able to set up the merchant account and the University PCI Committee will be able to review the technology to ensure it is compliant and that the security procedures are effective.

Important! A department, organization or affiliate must obtain its merchant account from the University's established merchant processor relationship. Merchants may NOT set up their own banking relationships for payment card processing and payment card revenue MUST be deposited into designated University bank accounts. Financial Services negotiates all banking and payment card processing relationships on behalf of the entire University, thereby taking advantage of the volume discounts and internal controls not available to individual departments, organizations or affiliates. Following the steps above will ensure these rules are followed.

Utilizing A Third-Party As A Merchant On Your Behalf

There are cases when a University department, organization or affiliate will contract with a third-party supplier that will act as the payment card merchant on behalf of the University.

In these cases, the University department, organization or affiliate must:

1. Follow the approval process outlined in the Approvals section above.
2. Provide an annual PCIDSS attestation or independent audit documentation from the supplier to Information Security. Information Security will review this documentation to ensure the supplier's continued compliance with PCIDSS.

No further procedural documentation needs to be developed by the University department, organization or affiliate. Continued compliance with the Transaction Reconciliation and Accounting section below is required, however.

General Guidelines

- 1) All faculty, staff and students involved with a merchant's payment card processing must go through a merchant processing training course before beginning any card processing. Routine refresher training will also be required.
- 2) All faculty, staff and students involved with a merchant's payment card processing in a non-cashiering function must sign the Payment Card Confidentiality Agreement and stored with the merchant.
- 3) Merchants must utilize the University centralized merchant processor (BB&T). Use of the central processor assures that the University receives the most favorable transaction pricing.
- 4) If the centralized merchant processor will not work with the merchant department's system or business process, a written request must be submitted to University PCI Committee outlining why the centralized processor will not meet the merchant's needs. The University PCI Committee will review the request, and if an exception is granted, will work with the merchant to establish service with an appropriate merchant processor.

Guidelines for Point of Sale Transactions

- 1) In order to reduce fraud, payment card companies recommend the following procedures for processing cards when the card is present (i.e. face to face transaction):
 - a) It is recommended you ask for a photo ID at the point of sale to verify the card holder is using the card.

- b) Always insert or swipe the card through the terminal/point of sale device, if applicable.
 - c) Obtain authorization for every card sale.
 - d) Ask the customer to sign the sales receipt. Merchants may choose to not require customers to sign receipts for transactions less than \$25; however, this option should only be chosen if the POS system is capable of not printing a receipt for the customer to sign.
 - e) Match the embossed number on the card to the four digits of the account number displayed on the terminal
 - f) Compare name and signature on the card to those on the transaction receipt
 - g) If you believe the card number or card sale is suspicious, make a Code 10 call Merchant Services' voice authorization center for the card being used.
- 2) If cardholder information is taken over the phone or via fax (i.e. card is not present), in order to reduce fraud, the following guidelines are recommended:
- a) Obtain cardholder name, billing address, shipping address (if different from billing address and if applicable), account number, and expiration date.
 - b) Verify the customer's billing address either electronically (by entering the ZIP code in the POS device) or by calling the credit card automated phone system (Address Verification System-AVS); see Appendix A for a list of phone numbers.
 - c) Request the Security Code (the three digit code on the back of the card in the signature panel) and validate the code at the time of authorization either electronically (through the POS device) or by calling the credit card automated phone system. This code must be destroyed once validated; it must not be stored physically or electronically.
 - d) Maintain credit card receipts and all delivery records for the retention period as specified in record retention below.
- 3) Those merchants, which utilize a fax machine for payment card orders, must operate a stand-alone fax machine connected via an analog line only. Multifunctional devices (i.e. Xerox copiers) are not allowed for receiving any payment card information. The stand-alone fax machine must be located in a secure area away from public traffic.
- 4) Transmission of sensitive cardholder data must be encrypted using at least 128 bit encryption and purged after settlement. Point of sale devices should be on an isolated VLAN.
- 5) Access to the physical location of stored credit card receipts must be in a restricted area where authorized persons can be easily identified and access to the area can be limited and restricted. Any visitors in this secured area should always be identified, logged in and out and escorted at all times.
- 6) Merchant equipment (i.e. computers or terminals) must only be used for processing card payments. Non-standard software must not be installed. Devices must have up-to-date operating system patches and antivirus protection installed. Usernames and passwords must not be shared between individuals. Passwords must be strong (e.g.

contain at least 8 characters that are a combination of letters (upper and lower case), numbers and symbols) and changed every 90 days. Contact Information Security before disposing of any merchant equipment.

Guidelines for E-Commerce Transactions

- 1) Merchants that need to accept payments over the internet must utilize the University centralized online credit card processing system (Nelnet's Commerce Manager). Use of the central service assures that the strictest controls are kept over card information and that the University is protected from liability should there be a security breach.

If a merchant can process payment card payments through the established University centralized online payment system, Financial Services will share details and guidelines for integrating the centralized payment process into the merchant's online environment. Financial Services and Information Security staff can also assist with general e-commerce questions and strategies for web site development, but cannot provide customized programming solutions. Sample code may be available depending on the web environment.

- 2) If this system is not appropriate for the type of processing needed by the merchant department, a written request must be submitted to University PCI Committee outlining why the centralized processing system will not meet the merchant's needs. The University PCI Committee will review the request, and if an exception is granted, work with the merchant to establish service with an appropriate online payment processor.

Any third party service providers must demonstrate the ability to comply with all procedure requirements outlined in this document, including the current version of PCIDSS. The merchant department establishing service is responsible for all associated costs with establishing any payment processing service.

- 3) Card processing transactions must be performed on the website of the payment gateway (i.e. the customer should enter sensitive cardholder data on a payment gateway website).
- 4) No department can store or process any payment card transaction on any University computer or network resources. All transaction data must be maintained by an approved service provider. All outside service providers must comply with the most current version of PCIDSS and be validated routinely as compliant by the card associations.

Transaction Reconciliation and Accounting

The daily net sales settle electronically into the appropriate University bank account, usually within 48 hours. It is the responsibility of the merchant to close out credit card batches daily and submit accounting information within 24 business hours of the batch close date to the University Cashier. The [Departmental Deposit Administrative Policy](#) contains more information regarding the method and timeliness of deposits, including payment card transactions.

Financial Services will contact merchants that utilize the centralized online payment system and share system instructions and reporting capabilities.

It is the merchant's responsibility, in cooperation with Financial Services, to reconcile the settlement amount in the general ledger account to the payment card receipts or payments from a third-party on a regular basis, but no less than monthly. Merchants will have two months to clear any outstanding payment card transactions that appear on the monthly bank reconciliation after which they will be written off to miscellaneous income or expensed to the merchant department.

It is also the merchant's responsibility to reconcile the payment card receipts or payments from a third-party to the system of record (e.g. events registration system, ticketing system, etc.). This will ensure that the payments received match services and goods provided.

Each merchant can view its monthly statement directly from the authorized merchant service provider. These statements provide a listing of each batch submitted for reconciliation purposes. It is the merchant's responsibility to verify that this information is correct.

Financial Services will work with merchants that do not utilize the centralized online payment system to develop specific procedures around requesting payment and reconciliation, aligned with other policies and procedures in effect.

Prohibited Payment Card Activities

Certain payment card activities are prohibited by payment card association rules or University policy. Prohibited activities include, but are not limited to:

- Tuition payment or other fees assessed and billed via Banner Accounts Receivable; these payments must be handled by Student Financial Services.
- The procurement of cash from the University, including cash advances and amounts over a sale amount (with the exception of Graylyn Conference Center).

Copy Requests and Disputed Transactions

Cardholders have the right to dispute transactions that they claim were not authorized or were done in error. Once a transaction has been disputed, the cardholder's financial institution requests a copy of the transaction from the merchant. There is a very limited amount of time for the University to respond to these requests; therefore, any merchant that receives a copy request will have two business days to produce the required transaction documentation.

If the merchant department does not respond with a rebuttal within the necessary timeframe to the request, the transaction is 'charged back' to the merchant account and the funds will be debited from the account used to record the original revenue.

Important! There is no grace period, and no appeal is possible, if the merchant misses the deadline. Therefore, it is important that all merchants must have adequate business processes in place to support the timely response of copy requests and other transaction inquiries. The Dispute Resolution contact for a merchant department merchant is responsible for responding to copy requests and disputed transactions.

Important! If the merchant chose to offer signature-less transactions to those customer transactions totaling less than \$25, there is no rebuttal process. The transaction will be charged back.

Refunds

When an item or service is purchased using a payment card and a refund is necessary, the refund must be credited to the same account from which the purchase was made. Under no circumstances is it permissible to issue a refund with cash or a check. A refund must never exceed the original payment amount.

To process a refund, the procedure appropriate to the technology used for processing (e.g. terminal, software, etc.) must be followed.

Important! If any portion of a payment is non-refundable, the merchant must declare this information to the customer before the transaction is processed and the customer must provide a means of acknowledgement (e.g. signature) that they understand and accept the terms of the payment.

Payment Card Industry Data Security Standard Compliance

A merchant must comply with the current version of the Payment Card Industry Data Security Standard (PCIDSS). The PCIDSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security

measures globally. PCIDSS provides a baseline of technical and operational requirements designed to protect cardholder data.

A merchant must undergo annual reviews called the PCIDSS Self-Assessment Questionnaire and vulnerability scanning of its processing environment by a security review team comprised of Information Security and Financial Services to ensure that all policies and procedures are being followed. Additional reviews may be required in addition to these annual reviews. As always, any business operation is subject to formal review by the Office of Internal Audit.

Any systems or processes that do not meet the current version of the requirements must be modified to meet the requirements. The merchant is responsible for the costs involved in maintaining compliance.

Important! If at any time a merchant department suspects a breach or compromise of any payment information or related data (e.g. suspected virus infection or unusual activity on a device used for processing payments), that merchant must report the event immediately to Financial Services and Information Security. Financial Services and Information Security will assess the situation and invoke the necessary incident response plan.

Important! Merchants found to be in non-compliance with processing requirements are subject to the risks, sanctions & fines related to non-compliance as found in the Payment Card Acceptance Policy.

Important! Merchants must provide an annual PCIDSS attestation or independent audit documentation from the supplier to Information Security. Information Security will review this documentation to ensure the supplier's continued compliance with PCIDSS.

Risks, Sanctions & Fines Related to Non-Compliance

Without adherence to the Payment Card Acceptance Policy and this procedure, the University would be in a position of unnecessary reputational risk and financial liability.

Merchant account holders (i.e. departments, organizations, and affiliates) who fail to comply are subject to and liable for:

- a) Any fines imposed by the payment card industry.
- b) Any additional monetary costs associated with remediation (e.g. cardholder notification, card replacement), assessment, forensic analysis, repayment of fraudulent charges or legal fees.
- c) Suspension of the merchant account.

Persons who fail to comply are subject to

- a) The loss of computer or network access privileges.
- b) Disciplinary action, including suspension and termination of employment.

- c) Legal action, as some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

Technology that does not comply is subject to immediate disconnection from the University's network.

Data Retention

Merchants must keep transaction documentation for the prior two fiscal years plus the current year transactions to support copy requests relating to disputes, refund requests and accounting audits.

Definitions

Below is a list of definitions to help the reader understand terms as they are used in this manual.

Acquirer: An organization that provides a merchant with facilities to accept card payments, accounts to the merchant for the proceeds and clears and settles the resulting obligations with card issuers.

Bank: A financial institution that provides merchant accounts to enable a merchant department to accept credit card payments. Funds are deposited into an account established at this institution.

Cardholder Data: Includes the following card attributes:

- Primary Account Number (PAN) – The payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called the Account Number.
- Cardholder Name
- Expiration Date
- Service Code

The PAN is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCIDSS requirements.

Chargeback: The deduction of a disputed sale previously credited to a merchant department's account when the merchant department fails to prove that the customer authorized the credit card transaction.

Copy Request: A request for a merchant to provide a copy of the original sales slip for a particular transaction if the cardholder is disputing the charge. Copy requests must be acted on within two days, and if ignored, can lead to chargebacks.

Customer: An individual or other entity that makes a payment to the University for goods, services, information, or gifts.

Discount Rate: A collection of fees charged by the acquirer to process the merchant's transaction. This includes interchange fee, assessment, and per item charges.

Merchant: A merchant department that accepts payment cards as a method of payment for goods, services, information, or gifts.

Merchant Account: An account established for a department, organization or affiliate by a bank to credit sale amounts and debit processing fees.

Merchant Discount: A percent or per-transaction fee that is deducted from the merchant department's gross credit card receipts and paid to the bank.

Payment Card: Either a debit card or credit card.

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

The PCIDSS is a multifaceted 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.

The regulations consist of twelve basic requirements, and corresponding sub-requirements, categorized as follows:

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Taken from *Payment Card Industry (PCI) Data Security Standard, v3.1*, April 2015; consult the current standard for any potential updates

Payment Terminal: The POS (point-of-sale) equipment used to capture, transmit, and store payment card transactions.

Rebuttal: A merchant's written reply to a chargeback that provides documentation proving that the sale was valid and that proper merchant procedures were followed.

Redact: The process of removing sensitive or classified information from a document prior to its publication.

Security Breach: Includes one or more of the following attributes:

1. Violation of an explicit or implied security policy;
2. Attempts (either failed or successful) to gain unauthorized access to a system or its data;
3. Unwanted disruption or denial of services;
4. The unauthorized use of a system for the processing or storage of data; and/or
5. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Sensitive Authentication Data: Related to cardholder data and contains the following attributes:

- Full track data (magnetic-stripe data or equivalent on a chip)
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

Sensitive Authentication Data may never be stored after authentication, even if encrypted.

Contacts

- For questions relating to payment card acceptance, merchant accounts, or accounting, contact [Financial Services](mailto:payment-cards@gg.wfu.edu) by emailing payment-cards@gg.wfu.edu.
- For questions relating to the University PCI Committee or equipment and software, contact [Information Security](mailto:infosec@wfu.edu) by emailing infosec@wfu.edu.

Policy / Procedure Violations

Policy and / or procedure violations should be reported to your supervisor, faculty administrator, human resource representative, department manager and/or the office responsible for the policy and procedure. If you prefer, you may instead contact the Audit & Compliance office (<http://compliance.wfu.edu/>) at (336) 713-4949, or make an anonymous report through the Compliance Hotline at (877) 880-7888 or <http://www.tnwinc.com/reportline> .

Appendix A: Address Verification System (AVS)

The Address Verification System (AVS) is a fraud prevention system used to verify the address of a person claiming to own a credit card. It is especially useful in Card Not Present situations (e.g. telephone, fax or e-commerce transactions). The system will check the billing address of the credit card provided by the user with the address on file at the card company or issuing bank.

If the billing address and the card address on file do not match, you will receive a response code indicating this during transaction processing. You can then choose to either deny or proceed with the transaction.

AVS Numbers for the Different Card Brands:

- VISA Merchant Verification Service: (800) 847-2750
 - Option 1, Address Verification: enter in the numeric portion of the street address, zip code, and VISA card number and it will advise you if there is a match.
 - Option 2, Issuing Bank Phone numbers: enter the VISA card number and it will provide you with the 800 number for the issuing bank if available.
- MasterCard Assist: (800) 622-7747
 - Select your language preference, then Option 2. Enter the MasterCard card number and it will provide you with the 800 number for the issuing bank if available.
- Discover Address Verification: (800) 347-7988
 - You will need your Discover Merchant number. Enter the Discover card number and address information, and it will advise you if there is a match.
- American Express Address Verifications: (800) 528-2121
 - Option 3 allows you to verify the name and address of a particular AMEX card number.